



HAL
open science

Ni lois, ni centres : gouverner par les transactions avec les blockchains

Clément Gasull

► To cite this version:

Clément Gasull. Ni lois, ni centres : gouverner par les transactions avec les blockchains. Sociologie. Université Paris sciences et lettres, 2023. Français. NNT : 2023UPSLM034 . tel-04312126

HAL Id: tel-04312126

<https://pastel.hal.science/tel-04312126>

Submitted on 28 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



THÈSE DE DOCTORAT
DE L'UNIVERSITÉ PSL

Préparée à Mines Paris-PSL

**Ni lois, ni centres :
gouverner par les transactions avec les blockchains**

Soutenue par

Clément GASULL

Le 19 juin 2023

Ecole doctorale n° 543

**Sciences de la Décision, des
Organisations, de la Société
et de l'Échange**

Spécialité

**Sciences, technologies,
sociétés**

Composition du jury :

| | |
|---|---------------------------|
| Jeanne LAZARUS Directrice de recherche, CNRS | <i>Examinatrice</i> |
| Kevin MELLET Assistant Professor, Sciences Po | <i>Examineur</i> |
| Fabian MUNIESA Directeur de recherche, Mines Paris - PSL | <i>Directeur de thèse</i> |
| Francesca MUSIANI Chargée de recherche, CNRS | <i>Rapporteuse</i> |
| Christophe PRIEUR Professeur, Université Gustave Eiffel | <i>Président</i> |
| Antoinette ROUVROY Chercheuse FNRS, Université de Namur | <i>Examinatrice</i> |
| Yamina TADJEDDINE FOURNEYRON Professeure, Université de Lorraine | <i>Rapporteuse</i> |

Ni lois, ni centres :
gouverner par les transactions
avec les blockchains

Remerciements

Je remercie vivement Francesca Musiani et Yamina Tadjeddine-Fourneyron d'avoir accepté le rôle de rapporteuses de ce travail, ainsi que Jeanne Lazarus, Christophe Prieur et Antoinette Rouvroy d'avoir accepté de l'examiner. C'est un honneur, je me réjouis par avance de nos échanges.

Cette thèse a pu avoir lieu grâce à un financement CIFRE d'Orange. Je remercie Adam Ouurou et Kevin Mellet qui m'ont accordé leur confiance et ont joué une partition à quatre mains efficace pour commencer dans les meilleurs délais. Je remercie également Françoise Fessant, Mathieu Sannié et Emilie Sirvent-Hien pour l'accueil qu'ils m'ont réservé au sein des équipes de recherche d'Orange, et pour la qualité de nos échanges.

Je remercie Fabian Muniesa et Kevin Mellet pour la confiance qu'ils m'ont accordée tout au long de ce travail. Leurs indications étaient toujours justes et précieuses pour prolonger une piste ou ajuster la focale. Je suis profondément reconnaissant pour leur accompagnement régulier dans l'avancée de ce travail de thèse, mais aussi plus généralement pour la formation rapprochée au métier de chercheur.

Au Centre de Sociologie de l'Innovation, j'ai rencontré un laboratoire qui associe effervescence intellectuelle et générosité. Cette thèse en a largement bénéficié. Je remercie tous les permanent·e·s du Centre pour la qualité de leurs conseils et leur goût pour la discussion collective, en particulier : Madeleine Akrich, Béatrice Cointe, Clément Marquet, Morgan Meyer, Vololona Rabeharisoa, Didier Torny et Vincent-Arnaud Chappe, ainsi que Daniel Florentin. J'adresse une gratitude toute particulière à Liliana Doganova et à Alexandre Mallard pour avoir su faire des comités de suivi de thèse des espaces de discussions riches et déterminants dans la dynamique de mon travail. Merci à Fabian Muniesa et à David Pontille pour l'animation de ces si stimulants ateliers doctoraux. Liliana Doganova, Brice Laurent et Jérôme Denis m'ont propulsé sur un terrain d'enquête excitant en tant qu'accompagnateur du voyage de l'option « Affaires publiques et innovation » à Singapour. Je les remercie chaleureusement, ainsi que les élèves-ingénieurs de l'époque Lucas Colson, Lena Poirier, Hugo Mougard et Paul Pihouhé pour ces passionnants moments d'enquête. Jérôme Denis, Liliana Doganova et David Pontille ont su trouver des mots particulièrement justes à des moments déterminants dans mon rapport à la thèse ; je vous en suis particulièrement reconnaissant. Je remercie également Catherine Lucas, Florence Paterson, Frédéric Vergnaud pour leur soutien infaillible pour tout ce qui touche à l'infrastructure du travail de recherche ainsi que pour leur soutien. Enfin, je remercie le dynamique groupe de doctorant·e·s et post-doctorant·e·s pour les moments passés ensemble et la bienveillance collective : Marie Alauzen, Quentin Dufour, Alexandre Violle, Mathieu Baudrin, Nassima Abdelghafour, Émilie Perrault, Félix Talvard, Sophie Tabouret, Félix Boilève, Evan Fisher, Mathieu Rajaoba, Florian Jatou, Jean Danielou, Loïc Riom, Cornelius Heimstädt, Mathilde Pellizzari, Victoria Brun, Roman Solé-Pomies, Carole-Anne

Remerciements

Tisserand, Abdoulaye Diaw, Jean Goizauskas, Clément Foutrel, Kewan Mertens, Solène Sarnowski, Allyson Pallisser, Guillaume Louvet, Hafid Ait Sidi Hammou.

Orange m'a non seulement permis de financer cette thèse mais de la vivre au laboratoire SENSE. J'y ai trouvé une ambiance particulièrement stimulante aux côtés de chercheur·e·s multipliant les angles et les objets pour cerner le numérique sous toutes ses coutures. Je tiens à remercier les nombreux membres du laboratoire pour leur accueil, en particulier pour les commentaires et suggestions que j'ai reçus lors des deux séminaires SENSE de présentation de la thèse, en 2019 et en 2021. Pour la qualité de leurs conseils, leur curiosité, ou pour avoir su me faire dire simplement des choses ne l'étaient pas toujours, je remercie Anne Bellon, Thomas Beauvisage, Jean-Samuel Beuscart, Céline Borelle, Anca Boboc, Samuel Coavoux, Aude Danieli, Quentin Gilliotte, Théophile Megali, Anne-Sylvie Pharabod, Valérie Peugeot, Jean-Marc Raybaud, Haude Rivoal. Au sein d'Orange, j'ai également eu la chance d'échanger avec Alicia Filipiak sur les monnaies locales et complémentaires ainsi qu'avec Philippe Genestier qui coordonnait le groupe de travail sur les blockchains ; je les remercie tous les deux de leur intérêt pour mon travail, pour les sciences sociales au sein d'Orange, et pour m'avoir permis d'en présenter différentes parties au sein d'Orange.

Des analyses participant à cette thèse ont été présentées lors de différents événements. Je remercie les participant·e·s des doctorales i3 à l'Ecole des Mines en 2018 ainsi que celles et ceux de l'édition 2021, notamment Benjamin Loveluck pour nos échanges sur la communauté Ethereum. Je remercie Donald MacKenzie et Koray Caliskan pour la qualité des discussions préalables et des échanges durant la session dédiée aux blockchains en 2019, organisée au sein du réseau J de la SASE. Je remercie également Koray Caliskan pour m'avoir invité comme discutant lors de la 4S en 2021. Cette thèse a bénéficié d'une très riche discussion au laboratoire Costech à l'UTC, en février 2022. Je remercie toute l'équipe EPIN et plus particulièrement Anne Bellon et Clément Mabi pour leur invitation, et Bruno Bachimont pour la qualité et la finesse de ses impressions et conseils.

Pour faire d'une ambition de thèse un projet, j'ai bénéficié de précieux conseils et soutiens. Eve Chiapello et Francesca Musiani m'ont généreusement accordé de leur temps ; leurs aiguillages ont été déterminants. Mes remerciements vont également à Marc-Eric Bobillier-Chaumont, Julien Guibourdenche et Jacqueline Vacherand-Revel pour m'avoir initié à la recherche ethnographique. Je remercie particulièrement Marc-Eric et Julien pour avoir soutenu ma candidature de thèse au CSI ; et tout particulièrement Julien pour m'avoir suggéré, il y a dix ans, d'ouvrir un ouvrage de Bruno Latour. Je remercie également Christian Paul et Daniel Kaplan pour leurs conseils, ainsi que Joëlle Toledano et Lionel Janin pour leur invitation à participer au stimulant groupe de travail de France Stratégie sur les « jeux des blockchains » qu'ils coordonnaient.

Remerciements

Sans eux, il n'existerait ni horizon d'un monde sans centres, ni manuscrit. Pour avoir permis que le second advienne, je remercie tous les acteurs rencontrés hors ligne et ceux qui ont laissé des traces en ligne. Je remercie particulièrement Arnaud, Jean et Indy pour leur générosité et toute l'équipe de LeVote pour avoir partagé avec moi leur aventure entrepreneuriale.

Je remercie Quentin Rodriguez et Théophile Megali pour leurs relectures minutieuses de différents textes qui composent ce manuscrit. Leurs remarques comme leur présence durant ce travail ont été précieuses.

J'ai eu la chance d'être merveilleusement entouré. Pour toutes les agréables bulles d'air qui ont été essentielles à ce travail, je remercie notamment Quentin, Théophile, Anne, Haude, Céline, Adrien, Laura, Camille, Quentin, Mickael, Léa, Jean-Baptiste, Pauline, Émilie, Justine, Laure, Mikael, Hélène, Philippe et Pierre. Merci également à mes parents Pascale et Pierre et mon frère Nicolas qui ont toujours été encourageants.

Enfin, je remercie ma compagne, Amélie, qui a su trouver les mots et les gestes, quelles que soient les circonstances et tout au long de ce travail. Sa compréhension de cet exercice solitaire, sa patience et sa tendresse ont été capitaux durant ces années. Je lui en suis infiniment reconnaissant.

Table des matières

| | |
|---|-----------|
| Remerciements..... | 6 |
| Acronymes..... | 18 |
| Introduction générale..... | 21 |
| 1. Problème et objet..... | 21 |
| <i>Faits sociaux et interventions sur les réseaux.....</i> | <i>21</i> |
| <i>Problématisation des réseaux comme producteurs de faits.....</i> | <i>23</i> |
| <i>Technologie de gouvernance.....</i> | <i>26</i> |
| <i>Imaginaires de l'autonomie : entités souveraines et ordre autonome.....</i> | <i>33</i> |
| 2. Démarche et enquête..... | 36 |
| <i>Point de départ : blockchain-mania et crypto-bashing institutionnels.....</i> | <i>36</i> |
| <i>Ethereum : objet d'enquête à l'articulation entre blockchain et crypto-monnaies.....</i> | <i>39</i> |
| <i>Démarche d'enquête : explorer les réseaux de développement d'Ethereum.....</i> | <i>42</i> |
| <i>Une dynamique d'innovation distribuée en co-construction.....</i> | <i>45</i> |
| 3. Espaces transactionnels sans hétéronomie..... | 47 |
| <i>Réseaux économiques conçus comme espaces transactionnels.....</i> | <i>48</i> |
| <i>Hétérotopies numériques en train de se faire.....</i> | <i>50</i> |
| <i>Transactions comme opérations de production d'un « monde commun ».....</i> | <i>52</i> |
| <i>Espaces et conditions de forme sur les transactions.....</i> | <i>54</i> |
| 4. Sur la piste de l'ingénierie des transactions..... | 56 |
| <i>Changer la réalité en neutralisant les inscripteurs des relations sociales.....</i> | <i>56</i> |
| <i>Alignement à partir de l'inscription matérielle.....</i> | <i>58</i> |
| <i>Précautions de langages.....</i> | <i>61</i> |
| 5. Composition du manuscrit..... | 62 |
| <i>Indications générales.....</i> | <i>62</i> |
| <i>Chapitre 1. Mystique du protocole : calculer sans connaître.....</i> | <i>63</i> |
| <i>Chapitre 2. Les modes des jetons : instituer par les smart contracts.....</i> | <i>64</i> |
| <i>Chapitre 3. Technologie de plateformes, modalisations de la gouvernance.....</i> | <i>65</i> |
| <i>Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire.....</i> | <i>67</i> |
| <i>Annexe 1 – Épisodes de terrain hors ligne.....</i> | <i>68</i> |
| <i>Annexe 2 – Meetups.....</i> | <i>68</i> |
| <i>Annexe 3 – Ethereum par un bord.....</i> | <i>68</i> |
| Chapitre 1. Mystique du protocole : calculer sans connaître..... | 70 |
| Introduction. De Bitcoin à la blockchain : l'informatique faite théorie du contrôle..... | 70 |
| <i>Blockchain et le social « sans confiance » dans les institutions.....</i> | <i>71</i> |
| <i>Analyse de la gouvernance : la mystique du protocole.....</i> | <i>74</i> |
| <i>Du problème institutionnel au problème du contrôle des relations numériques.....</i> | <i>76</i> |

| | |
|---|------------|
| Plan du chapitre..... | 79 |
| 1. Bitcoin : gouverner des relations sans sujets de connaissance..... | 81 |
| 1.1. Problématisation des institutions comme systèmes corruptibles..... | 81 |
| <i>Bitcoin dans une généalogie du problème des « autorités » sur Internet.....</i> | <i>82</i> |
| <i>Le problème des autorités (et) de la valeur.....</i> | <i>87</i> |
| <i>La solution : un protocole « autonome » de la cité pour une confiance inter-individus....</i> | <i>89</i> |
| 1.2. Instaurer la rupture épistémique : l'autorité déléguée à un réseau d'entités passivées..... | 93 |
| <i>Le protocole : agenceur du registre, passiviseur des mineurs.....</i> | <i>94</i> |
| <i>Le problème des généraux byzantins : faire calculer un réseau ouvert de calculateurs faillibles.....</i> | <i>97</i> |
| <i>Un système impérativement fiable.....</i> | <i>99</i> |
| <i>Des autorités sans intentionnalité ni périmètre.....</i> | <i>101</i> |
| <i>La transaction, matière première d'un processus de validation rémunérateur.....</i> | <i>103</i> |
| 1.3. Le protocole : technique de neutralisation du pouvoir de gouvernants sur des gouvernés..... | 106 |
| <i>Conjurer tout pouvoir sur les transactions.....</i> | <i>106</i> |
| <i>L'exercice du pouvoir comme domination de gouvernants sur des gouvernés.....</i> | <i>108</i> |
| <i>Les intérêts, dans l'analyse (de Lukes) et dans la neutralisation (par Bitcoin) du pouvoir.....</i> | <i>110</i> |
| <i>L'agentivité et la structuration par les intérêts individuels.....</i> | <i>112</i> |
| <i>Capacité et « pouvoir de » : la limite matérielle de la puissance de calcul.....</i> | <i>114</i> |
| Conclusion intermédiaire. Gouverner par le calcul distribué : inscrire sans connaître..... | 116 |
| 2. Ethereum : libérer le calcul par le gouvernement des inscriptions..... | 121 |
| 2.1. Les transactions : inscriptions contrôlables plutôt que données circulantes..... | 121 |
| <i>Smart contracts : les relations numériques comme contrats autonomes.....</i> | <i>122</i> |
| <i>Problématisation du Web : un espace de données détachées des individus et agissantes.....</i> | <i>126</i> |
| <i>Contrôler le travail des données par les transactions.....</i> | <i>131</i> |
| 2.2. En filiation avec Bitcoin : un mécanisme de pouvoir inscrire..... | 133 |
| <i>Des transactions monétaires aux transactions contractuelles : Bitcoin, du système au modèle.....</i> | <i>134</i> |
| <i>Bitcoin : architecture et véhicule de problématisation des institutions comme systèmes.....</i> | <i>137</i> |
| <i>Le protocole : mécanisme de pouvoir inscrire.....</i> | <i>138</i> |
| <i>Le point de vue de la technologie de pouvoir.....</i> | <i>141</i> |
| 2.3. Ethereum dans un art de gouverner par le calcul informatique..... | 145 |
| <i>Sécuriser le calcul par la décentralisation.....</i> | <i>145</i> |
| <i>Ethereum : dispositif de sécurité pour le Web.....</i> | <i>150</i> |
| <i>La centralisation du calcul dans la problématisation politique de l'informatisation.....</i> | <i>154</i> |
| Conclusion du chapitre..... | 159 |
| Chapitre 2. Les modes des jetons : instituer par les smart contracts..... | 163 |
| Introduction : l'institutionnalisation des cryptoactifs et le problème de leurs significations..... | 163 |
| <i>Les cryptoactifs et l'argent : institutions, significations.....</i> | <i>165</i> |
| <i>Institutionnalisation des cryptoactifs : enquête sur les significations des jetons.....</i> | <i>169</i> |
| <i>Plan du chapitre.....</i> | <i>170</i> |

| | |
|---|------------|
| 1. Les jetons : anatomie sémiotique de la conception du Web décentralisé..... | 173 |
| 1.1. Les jetons utilitaires : imaginaire d'autonomisation des plateformes du Web..... | 174 |
| <i>Début 2018 : foisonnement de DApps.....</i> | <i>174</i> |
| <i>Les smart contracts, plateformes dépouillées.....</i> | <i>177</i> |
| <i>La plateforme garnie : les jetons utilitaires.....</i> | <i>183</i> |
| 1.2. Les jetons, ingénierie de relations entrepreneuriales..... | 186 |
| <i>Cas Digix : le financement par l'émission de jetons de gouvernance.....</i> | <i>187</i> |
| <i>Cas Bluzelle : le financement par l'émission de jetons utilitaires.....</i> | <i>191</i> |
| <i>Les jetons : dispositifs d' enrôlement et opérations de capitalisation.....</i> | <i>193</i> |
| 1.3. Gestation d'un agencement marchand : quelques plans de coupe..... | 196 |
| <i>Le whitepaper : dispositif de valorisation et de capitalisation.....</i> | <i>197</i> |
| <i>ICO mania : valorisation des jetons et commerce de l'influence.....</i> | <i>199</i> |
| <i>Intéresser d'abord, monnayer l' enrôlement ensuite.....</i> | <i>202</i> |
| <i>Les IEO, ou la fusion des valorisations marchandes et entrepreneuriales.....</i> | <i>206</i> |
| 2. La conception institutionnelle des jetons..... | 209 |
| 2.1. Un processus de conception institutionnel..... | 210 |
| <i>Pratiques de conception : standardisation et réseaux de proximités.....</i> | <i>210</i> |
| <i>Les argents de la conception de DApps : ethers et bitcoin articulés au dollar étatsunien.....</i> | <i>214</i> |
| <i>Institutionnalisation d'objets technologiques plutôt que technologie institutionnelle.....</i> | <i>217</i> |
| 2.2. Meetups de ConsenSys, sites de problématisation des jetons et des smart contracts..... | 220 |
| <i>Rencontre avec une entreprise en mutation.....</i> | <i>220</i> |
| <i>Les meetups : fil rouge d'enquête sur un « écosystème ».....</i> | <i>223</i> |
| <i>Problématisation des ICO : qualités du marché des jetons plutôt que l'ampleur de ses significations.....</i> | <i>228</i> |
| 2.3. Incertitudes et significations : jetons utilitaires et security tokens..... | 231 |
| <i>Problématisation de la finance institutionnelle.....</i> | <i>232</i> |
| <i>D'une incertitude réglementaire à une innovation technologique.....</i> | <i>235</i> |
| <i>Regarder les relations comme un concepteur de jetons.....</i> | <i>236</i> |
| <i>La complexité des relations « intégrée » dans les jetons.....</i> | <i>240</i> |
| <i>Parcours de conception : les security tokens et les émetteurs de titres faits concepteurs de jetons.....</i> | <i>243</i> |
| Conclusion du chapitre..... | 248 |

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance.....252

| | |
|--|------------|
| Introduction. D'organisations économiques à la gouvernance par les transactions..... | 252 |
| <i>Modalisations de la gouvernance par l'infrastructure : formation et formulation des transactions.....</i> | <i>253</i> |
| <i>Technologie de plateformes.....</i> | <i>254</i> |
| <i>Prescriptions : un utilisateur générique d'Ethereum, des utilisateurs spécifiques de plateformes.....</i> | <i>256</i> |
| <i>Plan du chapitre.....</i> | <i>257</i> |
| 1. Technologiser une infrastructure, transformer l'économie numérique par les transactions..... | 259 |
| <i>Avec Hughes : suivre l'activité d'un « system builder » pour analyser l' « infrastructuring ».....</i> | <i>259</i> |

| | |
|--|-----|
| 1.1. Étendre un écosystème de formulateurs par le développement infrastructurel..... | 262 |
| <i>B2C et B2B : un travail infrastructurel transverse.....</i> | 262 |
| <i>Le cas de la DeFi : les entreprises comme potentielles utilisatrices de services B2C.....</i> | 264 |
| <i>D'un écosystème B2C à faire exister par la conception de briques infrastructurelles....</i> | 266 |
| <i>... à la technologisation de l'infrastructure : briques logicielles intégrées en « full stack »</i> | |
| <i>B2B.....</i> | 269 |
| 1.2. La preuve est dans le script : tactiques d'enrôlement des grandes entreprises..... | 271 |
| <i>Portrait : des cartes graphiques au conseil.....</i> | 272 |
| <i>Prouver que les entreprises sont inscrites comme utilisatrices imaginées.....</i> | 274 |
| <i>Développer l'écosystème par l'infrastructure : transformer les briques en produits.....</i> | 277 |
| 1.3. Faire converger des organisations économiques par l'infrastructure..... | 279 |
| <i>Vision : une économie unifiée par une infrastructure universelle.....</i> | 280 |
| <i>Compétition des « solutions blockchain ».....</i> | 282 |
| <i>Construire une « full stack » en intégrant les briques en produits.....</i> | 286 |
| Conclusion de la section : conception d'une convergence infrastructurelle de l'économie numérique..... | 290 |

2. L'écosystème en action : les transactions, opérations duales des plateformes.....293

| | |
|---|-----|
| 2.1. L'écosystème, réseau de concepteurs de plateformes..... | 293 |
| <i>Polysémie de « plateforme » : support d'un écosystème et objets de conception.....</i> | 294 |
| <i>Figure du concepteur de DApps : travailleur autonome en « organisation décentralisée »</i> | |
| | 296 |
| <i>L'écosystème : espace de convergences entre utilisations B2C et B2B.....</i> | 301 |
| 2.2. Cadrage par une technologie de plateformes : l'utilisateur-citoyen, cas LeVote..... | 305 |
| <i>Deux utilisateurs imaginés : un utilisateur-autonome et un citoyen-imaginé.....</i> | 306 |
| 2.2.1. <i>La plateforme comme cadrage des relations numériques : le cas du vote.....</i> | 307 |
| 2.2.2. <i>Le cadrage par la plateforme à l'épreuve du monde : l'intéressement des Élus.....</i> | 314 |
| Le rôle d'Orange et de LeVote : assistance technique à la formulation de scrutins par les Élus..... | 314 |
| Prototype et inclusion des Maires dans le processus de formulation des votes..... | 317 |
| 2.3. Débordements du cadrage, négociations de la formation et de la formulation..... | 321 |
| 2.3.1. <i>Réformer les transactions : coût et politique de la totalisation.....</i> | 322 |
| Mutualiser pour diminuer les coûts de formation des transactions..... | 322 |
| Politique du serveur mutualisateur : un intermédiaire entre Ethereum et l'utilisateur-citoyen..... | 324 |
| 2.3.2. <i>(Re)formuler des transactions, (re)constituer un corps électoral.....</i> | 327 |
| Partir de l'utilisateur (plutôt que du jeton)..... | 328 |
| Enrôler l'utilisateur en formulant le vote « simplement »..... | 330 |
| Développer l'application comme un lien durable entre Élus et administrés..... | 331 |
| Conclusion de la section : la plateforme, dispositif de gouvernance modalisable..... | 333 |

Conclusion du chapitre.....338

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire.....341

Introduction : l'autonomie de l'infrastructure comme objet plutôt que principe.....341

| | |
|--|-----|
| <i>Les smart contracts, des « lois ».....</i> | 341 |
| <i>L'autonomie des blockchains, acquise par principe ?.....</i> | 343 |
| <i>L'autonomie, résultat d'alliances temporairement stabilisées.....</i> | 344 |

| | |
|--|------------|
| <i>La communauté : groupe problématisant la construction de l'infrastructure.....</i> | 346 |
| <i>Terrain mobilisé dans ce chapitre.....</i> | 348 |
| <i>Argument du chapitre et annonce du plan.....</i> | 349 |
| 1. L'autonomie à l'épreuve de la construction de l'infrastructure..... | 351 |
| 1.1. L'instauration d'Ethereum entre mystique du protocole et fonctions imaginées..... | 352 |
| « Décentralisation » : mystique et instauration des blockchains..... | 352 |
| a. La mystique comme prisme de problématisation..... | 354 |
| Les fermes de minage : décentralisation de l'infrastructure matérielle..... | 354 |
| Protocole et logiciels « clients » : décentralisation de la conception logicielle..... | 356 |
| b. Au-delà de la mystique : l'infrastructure au prisme de sa fonction imaginée..... | 358 |
| 1.2. Constitution de la communauté et développement de l'écosystème..... | 362 |
| <i>Deux points de vue sur la communauté Ethereum.....</i> | 362 |
| <i>Un groupe constitué à l'épreuve du développement de l'écosystème.....</i> | 365 |
| <i>Un groupe fragile à l'épreuve du développement de l'écosystème.....</i> | 368 |
| 1.3. L'autonomie, une fonction infrastructurelle..... | 372 |
| <i>TheDAO, un « hack » ?.....</i> | 373 |
| <i>Clivage : prendre en compte l'écosystème dans l'action collective ?.....</i> | 374 |
| <i>Références épistémiques pour l'action collective.....</i> | 377 |
| <i>L'autonomie de l'infrastructure : un concept défini en situation.....</i> | 379 |
| 2. Gouverner le développement de l'écosystème au prisme de la mystique..... | 381 |
| 2.1. Actions collectives sur et par l'infrastructure..... | 381 |
| <i>Grammaire de l'action collective : le cas de la controverse TheDAO.....</i> | 382 |
| <i>Délibération : nécessité et théorisation vernaculaire.....</i> | 386 |
| 2.2. Le financement des « biens publics » : cas de problématisation de l'action collective.. | 389 |
| <i>Financer les « biens publics » de l'écosystème : un problème de gouvernement.....</i> | 390 |
| <i>« Biens publics » et communauté de joueurs rationnels.....</i> | 392 |
| <i>Le financement par les organisations : suspect par hypothèse.....</i> | 395 |
| 2.3. Mécanismes : le gouvernement automatique et participatif..... | 399 |
| <i>Le financement idéal : automatiser origine et allocation de l'argent.....</i> | 399 |
| <i>Des mécanismes indépendants des significations des transactions.....</i> | 401 |
| <i>L'allocation délibérée : « décider sur la chaîne » des biens publics à financer.....</i> | 404 |
| 2.4. La mystique du protocole appliquée à la décision collective..... | 406 |
| <i>Qualification des « biens publics » par le vote.....</i> | 407 |
| <i>À quoi bon voter pour un « bien public » ?.....</i> | 408 |
| <i>L'impossibilité d'éviter les « attaques » par « collusion ».....</i> | 409 |
| <i>La nature « ploutocratique » du vote.....</i> | 411 |
| <i>Le vote comme prédiction, ou la création d'identités ad hoc.....</i> | 412 |
| Conclusion du chapitre. L'infrastructure, processus constitutionnel..... | 415 |
| Conclusion générale..... | 418 |
| 1. Décentralisé : imaginaire de l'autonomie..... | 418 |
| 1.1. Imaginaire d'un monde sans centres..... | 418 |
| 1.2. La quête d'une souveraineté scripturale..... | 420 |
| 2. Décentraliser : institution d'une gouvernance par les transactions..... | 422 |

| | |
|---|------------|
| 2.1. Gouvernance par les transactions : quelques traits..... | 422 |
| 2.2. Autonomie instituée..... | 425 |
| 3. Perspectives..... | 427 |
| Bibliographie..... | 430 |
| Sources..... | 450 |
| Annexes..... | 461 |
| Annexe 1 – Épisodes de terrain hors ligne..... | 461 |
| Annexe 2 – Meetups..... | 464 |
| Annexe 3 – Ethereum par un bord..... | 468 |
| 1. L'utilisateur : un portefeuille responsable..... | 470 |
| 1.a. Accéder à MEW : l'utilisateur « responsable » de sa « sécurité »..... | 471 |
| 1.b. Créer un « wallet » : s'équiper des « keys » pour gérer ses « Ethers » et ses « Tokens »..... | 472 |
| 1.c. Interagir avec d'autres : générer une « transaction » et l'envoyer dans le « network »..... | 474 |
| 2. Ethereum : un « réseau » dans lequel on entre par des « nodes »..... | 476 |
| 2.a « Network » et « gas price » : paramétrer les transactions..... | 476 |
| 2.b. Trajectoire des « transactions »..... | 478 |
| 2.c. « Nodes » omniscients : valideurs ou « mineurs »..... | 480 |
| 3. Les formes des nodes, pivots entre l'utilisateur et la <i>blockchain</i> | 484 |
| 3.a. Être node soi-même..... | 484 |
| 3.b. Ce qu'il se passe en ligne, ce qu'il se passe hors ligne..... | 486 |
| 3.c. De la diversité des points d'entrées d'Ethereum. Des nodes « techniques » aux positions « économiques » : individus, startups et plateformes d'échanges..... | 487 |
| Figures de l'Annexe 3..... | 490 |

Index des tableaux

| | |
|--|-----|
| Tableau 1 : Correspondance entre désignations utilisées pour décrire Bitcoin..... | 101 |
| Tableau 2 : Flux et type d'informations entre acteurs impliqués dans un contrat fizzy..... | 124 |
| Tableau 3 : Correspondance entre le langage de Foucault et l'analyse d'Ethereum..... | 145 |
| Tableau 4 : Visions des fondateurs de DApps rencontrés à Singapour en février 2018..... | 176 |
| Tableau 5 : Émission des jetons BLZ et effets attendus pour la firme..... | 192 |
| Tableau 6 : Récapitulatif des usages imaginés des jetons, cas Bluzelle et Digix..... | 194 |
| Tableau 7 : Correspondance entre catégories d'orateurs et de spectateurs attendus entre juin 2018 et mars 2020, selon la numérotation de l'Annexe 2..... | 227 |
| Tableau 8 : L'importance de la DeFi face aux deux publics..... | 265 |
| Tableau 9 : Pas d'applications décentralisées sans outils d'infrastructure et de développement..... | 267 |
| Tableau 10 : À chaque public une modalité de gouvernance de l'économie..... | 271 |
| Tableau 11 : L'universalité de l'inscription comme fondement d'une nouvelle économie numérique | 280 |
| Tableau 12 : À chaque public sa problématisation du contrôle sur les relations..... | 281 |
| Tableau 13 : Verbatims issus d'un entretien avec Geoffrey (novembre 2018) : contractualisation avec deux Communes clientes..... | 318 |
| Tableau 14 : Récapitulatif des principes de connaissance et d'intervention sur Ethereum et sur Ethereum Classic..... | 379 |
| Tableau 15 : Types d'actions collectives dans la controverse TheDAO..... | 383 |

Index des figures

| | |
|--|-----|
| Figure 1 : Diagramme dessiné par Robert Metcalfe pour une présentation d'Ethernet en juin 1976 à la National Computer Conference (Metcalfe 2020)..... | 56 |
| Figure 2 : Illustration de la métaphore du « Problème des Généraux Byzantins » proposée dans un article promouvant et vulgarisant le fonctionnement des cryptomonnaies (crédit : DeCoste 2019).. | 99 |
| Figure 3 : Image reproduite depuis Clement (2019). Titre d'origine : « <i>High Level workflow of the interactions between the fizzy app and its Smart Contract</i> »..... | 123 |
| Figure 4 : Reproduction de la représentation des trois axes de la (dé)centralisation selon Buterin (2017a)..... | 147 |
| Figure 5 : Impression écran d'une partie de la page web ethereum.org en mai 2020..... | 151 |
| Figure 6 : Page d'accueil du site coinmarketcap.com, octobre 2021..... | 165 |
| Figure 7 : Nombre de nouvelles DApp par mois (StateOfTheDApp 2020) – mes ajouts en rouge. | 175 |
| Figure 8 : Articulation de la promesse de service à l' « Internet décentralisé » (Bains 2018)..... | 180 |
| Figure 9 : « Cycle de vie du produit » (Eufemio et al. 2016)..... | 182 |
| Figure 10 : Extrait de Bains (2018 : 20) – mes ajouts en rouge..... | 185 |
| Figure 11 : Hiérarchie des pouvoirs de décision dans DigixDAO..... | 189 |
| Figure 12 : Tweet de John McAfee faisant la publicité d'un service de rédaction de <i>whitepapers</i> | 201 |
| Figure 13 : Exemple d'avalanche de questions à l'ouverture du chat – mes rajouts en rouge (concentration des messages) et gris (anonymisation)..... | 205 |
| Figure 14 : Photo prise lors de l'introduction du meetup #10 (mai 2019) à ConsenSys, rue Vauvilliers, Paris 1 ^{er} arrondissement..... | 224 |
| Figure 15 : Photo d'un mur des locaux de ConsenSys France couvert de citations, prise lors du meetup #10 (mai 2019)..... | 225 |
| Figure 16 : Photographie de la représentation de la « convergence » entre B2B et B2C (meetup #18, mars 2020)..... | 282 |
| Figure 17 : Indicateurs <i>marketing</i> qui assimilent utilisations B2C et B2C..... | 287 |
| Figure 18 : Représentation de la « <i>full stack</i> » durant le meetup #16 (septembre 2019)..... | 288 |
| Figure 19 : Diapositive d'Agueda présentant les différents modèles organisationnels dans Laloux (2016)..... | 297 |
| Figure 20 : Présentation de l'application LeVote par Geoffrey à VivaTech 2019..... | 316 |

| | |
|---|-----|
| Figure 21 : « <i>Users are features!</i> », Bastien, sep. 2019..... | 329 |
| Figure 22 : « <i>The design dilemma</i> », Bastien, sep. 2019..... | 329 |
| Figure 23 : « <i>Get into user’s head!</i> », Bastien, sep. 2019..... | 329 |
| Figure 24 : Enquête sur l’utilisateur, Bastien, sep. 2019..... | 329 |
| Figure 25 : Photo d’une diapositive de BS intégrant une photo du premier cercle d’enthousiastes présents à la Miami Bitcoin Conference, parmi lesquels V. Buterin, C. Hoskinson, J. Lubin, G. Wood..... | 369 |
| Figure 26 : Tweet de BS dénonçant la réécriture de l’annonce publique d’Ethereum..... | 370 |
| Figure 27 : Résultat affiché du vote (CarbonVote 2022)..... | 385 |
| Figure 28 : Graphique critique de CarbonVote, produit par un opposant à la bifurcation (Idle 2016) | 386 |
| Figure 29 : Vitalik Buterin pose le problème de financement des « <i>public goods</i> » comme un problème de gouvernement..... | 391 |
| Figure 30 : Vitalik Buterin explique le problème de la rémunération des « <i>public goods builders</i> » | 393 |
| Figure 31 : Page d’accueil du site MyEtherWallet.com..... | 472 |
| Figure 32 : <i>Paper wallet</i> | 473 |
| Figure 33 : Paramétrage du <i>gas price</i> et du <i>network</i> | 477 |
| Figure 34 : Confirmation de changement de <i>network</i> | 477 |
| Figure 35 : Représentation de la trajectoire des <i>transactions</i> par MEW..... | 479 |

Acronymes

| | |
|--------|--|
| ACPR | Autorité de contrôle prudentiel et de résolution |
| ADAN | Association pour le Développement des Actifs Numériques |
| AMAFI | Association française des marchés financiers |
| AMF | Autorité des marchés financiers |
| API | <i>Application Programming Interface</i> |
| ASIC | <i>Application Specific Integrated Circuit</i> (minage) |
| B2B | <i>Business to Business</i> |
| B2C | <i>Business to Customer</i> |
| BS | Bob Summerwill (protagoniste du Chapitre 4) |
| DAO | <i>Decentralized Autonomous Organization</i> (organisation autonome décentralisée) |
| DApp | <i>Decentralized Application</i> (application décentralisée) |
| DeFi | <i>Decentralized Finance</i> (finance décentralisée) |
| DevCon | Developer Conference |
| DLT | <i>Distributed Ledger Technology</i> (technologie de registre distribué) |
| DRM | <i>Digital Rights Management</i> |
| EEA | Ethereum Enterprise Alliance |
| EF | Ethereum Foundation |

Acronymes

| | |
|----------|--|
| EIP | <i>Ethereum Improvement Proposals</i> |
| ERC | <i>Ethereum Request for Comments</i> |
| ESMA | European Securities and Markets Authority |
| ETH NVTV | Ethereum Network Value / Token Value (indicateur financier) |
| EthCC | Ethereum Community Conference |
| EvN | Evan Van Ness (protagoniste du Chapitre 4) |
| GIF | Graphics Interchange Format (format de fichiers) |
| HTTP | HyperText Transfer Protocol (protocole pour le WWW) |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICO | <i>Initial Coin Offering</i> , offre initiale en jetons |
| IETF | Internet Engineering Task Force |
| IPO | <i>Initial Public Offering</i> (introduction en bourse) |
| IEO | <i>Initial Exchange Offering</i> (ICO par un exchange) |
| KPI | <i>Key Performance Indicator</i> (indicateur clé de performance) |
| MEFF | Ministère de l'Économie et des Finances en France |
| MEW | MyEtherWallet (service de <i>wallet</i> en ligne) |
| MOOC | <i>Massive Open Online Course</i> (cours en ligne ouvert à tous) |
| MVP | <i>Minimum Viable Product</i> (littéralement Produit Minimum Viable) |

Acronymes

| | |
|-------|---|
| NFT | <i>Non Fungible Token</i> (jeton non fongible) |
| PACTE | Loi Pour la Croissance et la Transformation des Entreprises |
| PDF | Portable Document Format (format de fichiers) |
| PRV | <i>Power: A Radical View</i> (titre d'ouvrages de Steven Lukes) |
| PSAN | Prestataires en Actifs Numériques (catégorie d'acteurs en droit français) |
| SEC | U.S. Securities and Exchange Commission |
| SSII | Société de Service en Ingénierie Informatique |
| ST | <i>Security Token</i> (jeton représentant un titre financier) |
| STO | <i>Security Token Offering</i> (offre d'émission de titres financiers) |
| STS | <i>Science & Technology Studies</i> |
| TBN | The Bounties Network |
| TDN | The Dauriel Network |
| URL | <i>Uniform Resource Locator</i> (communément « adresse Web ») |
| VB | Vitalik Buterin (inventeur d'Ethereum) |
| W3C | World Wide Web Consortium |
| WWW | World Wide Web (protocole du Web) |

Introduction générale

Échanger et s'associer souverainement était le principe d'institution d'un ordre en société qui rassemblait, au tournant des années 2020, des développeurs, des entrepreneurs, des investisseurs, des militants, des administrations et des entreprises. Tous participaient à un projet technologique appelé Ethereum. Ensemble, ils faisaient advenir ce principe de souveraineté individuelle par la conception d'espaces relationnels. L'ordre qu'ils imaginaient devait être insensible aux prises du reste du monde. Dans la présente thèse, j'analyse la dynamique d'innovation autour d'Ethereum comme instauration de ce principe d'institution d'un ordre en société par le développement de logiciels, d'infrastructures, de cryptomonnaies, de modèles d'affaires, de dispositifs d'investissements et de coordination.

Cette introduction commence par esquisser le problème que se posaient les acteurs de ce processus d'innovation (comment échanger et s'associer souverainement par des réseaux numériques ?) et comment je l'analyse (l'imagination d'une « technologie de gouvernance »). Je présente mon enquête dans une seconde section, en décrivant les sites et les méthodes de manière réflexive. Une troisième section articule les objets rencontrés durant l'enquête (des réseaux économiques) au problème posé à la première section (technologie de gouvernance) par le concept d'« espace transactionnel ». Une quatrième section présente la démarche analytique : suivre la dynamique de la conception des espaces transactionnels. Enfin, les chapitres sont annoncés.

1. Problème et objet

Faits sociaux et interventions sur les réseaux

Internet et les technologies de réseaux numériques forment un pan toujours plus large de nos relations. Les courriels et les innovations du Web comme les pages personnelles, les portails, les blogs, les forums, les wikis, les sites commerciaux, et plus récemment les réseaux sociaux ou les applications pour smartphones forment des relations avec nos

Introduction générale

proches, nos collègues, des inconnus¹, des administrations, des entreprises, des gouvernements. Les significations de ces relations du point de vue des utilisateurs de ces technologies foisonnent sans être spécifiques aux media eux-mêmes. Ils prolongent des relations sociales hors ligne et font advenir de nouvelles formes de coopération, de partage, d'échanges. Les réseaux sociaux sont, par exemple, autant des outils de communication utilisés pour passer des appels ou envoyer des messages écrits que des outils d'organisation pour des associations, des syndicats, des mouvements politiques, ou des espaces publicitaires et des vitrines commerciales. Dans le même temps, ces usages font controverse : risques en termes de vie privée et d'espionnage à grande échelle, menace sur la liberté d'expression et sur la sécurité des communications, contournement des droits d'auteurs, manipulation des opinions publiques, transformation des identités individuelles, bouleversement des économies et des chaînes de valeur, ou encore poids de la consommation énergétique.

Le problème du contrôle des relations numériques comme intervention sur des données numériques est au cœur des controverses portant sur les développements contemporains d'Internet et des technologies de réseaux. Ces interventions peuvent être directes ou indirectes. Activistes, lanceurs d'alertes et militants sont souvent à l'origine de ces controverses quand ils mettent en visibilité les rôles d'acteurs institutionnels en capacité d'influencer, de modifier, d'empêcher, d'orienter, en un mot de contrôler les relations en intervenant sur les données. Les révélations d'Edward Snowden, en dévoilant les accords secrets liant de nombreuses entreprises du numérique et le gouvernement américain, illustrent l'intervention directe de ces acteurs institutionnels ; en l'occurrence, utiliser des communications privées à des fins de surveillance. Mais le contrôle est également exercé de manière indirecte. Différents champs de recherche abordent l'ampleur de ces modalités. La sociologie du numérique et les études en communication pointent notamment les conditions d'utilisation secondaire des relations faites données, montrant les rôles d'acteurs variés dans leurs usages, en termes de politique de modération ou de contrôle d'accès à des

1 J'utilise le masculin générique dans tout ce manuscrit, car la très large majorité des acteurs rencontrés étaient des hommes.

Introduction générale

plateformes, mais aussi en pointant le lien entre innovation et objectifs politiques ou commerciaux, comme des stratégies de présentation des contenus, ou l'élaboration de formats spécifiques².

Ce problème était celui des protagonistes au cœur de ce travail. Ils concevaient des technologies de réseaux comme remparts à toute possibilité d'intervention sur des relations numériques. Ces innovateurs étaient des développeurs, des individus regroupés en associations, des entrepreneurs, des investisseurs, des représentants d'institutions ou d'entreprises publiques et privées. Les relations qu'ils cherchaient à protéger étaient des échanges d'objets physiques ou numériques (kilo watt heures, argent, capacité de stockage de données en ligne, biens immobiliers, titres financiers, données personnelles, spiritueux ou conteneurs, pour ne citer que quelques exemples), sinon des expressions dans des processus de décision (typiquement, des votes). Au centre de leur attention figurait une technologie le plus souvent désignée par « chaîne de blocs » (*blockchain*), parfois par « technologie de registres distribués » (*distributed ledger technology*, DLT). Ils voyaient dans cette technologie en cours de développement une manière de faire d'échanges d'information numérique des faits sociaux inaltérables.

Problématisation des réseaux comme producteurs de faits

Constituer des faits sociaux inaltérables était une problématisation des réseaux formant les échanges ou les décisions. Prenons deux exemples. En 2016, l'opérateur de télécommunications français Orange et la banque centrale de Singapour étudiaient le « potentiel » de la *blockchain* ou DLT. Le premier voyait dans cette technologie une opportunité pour bâtir un service de vote en ligne. Le second construisait un prototype d'argent de banque centrale dont la distribution serait plus « efficace » et « ouverte » que sa version contemporaine. Votes et échanges monétaires étaient imaginés dans des formes techniques similaires : des communications qui pourraient être numérisées, ou dont la

2 Dans le développement de l'économie numérique par exemple, la sociologie du numérique montre que ces données sont « extraites » des usages pour alimenter les modèles d'affaires des acteurs les plus influents du Web de dispositifs comme les algorithmes (Cardon 2013) ou les cookies (Mellet & Beauvisage 2020), ou que leur pervasivité échappe aux acteurs qui en font usage et impactent en retour les vies des utilisateurs (Ebeling 2018).

Introduction générale

numérisation pourrait être améliorée.

L'un des griefs essentiels formulé à l'encontre du vote électronique est l'opacité de son fonctionnement, qui conduit à dépendre d'un tiers qui a les moyens de manipuler les résultats sans que les électeurs puissent le détecter. L'espoir suscité par la technologie blockchain en matière de vote est précisément associé à sa capacité à réaliser un consensus entre de multiples tiers, sans qu'aucun ne soit à lui seul en mesure de fausser le système à son profit. C'est donc un enjeu de confiance, essentiel à l'implication de chacun dans le processus participatif et démocratique, auquel la blockchain peut contribuer. (document interne projet VoteChain d'Orange, 2016)

DLT is at the centre of a massive push for innovation across the financial services industry. While DLT is by no means a one-size-fits-all solution, it has the potential to drastically alter the way we do business and interact with one another. The technology is also known as the "Internet of Value", as it increases the efficiency, security and transparency of transactional activities. (rapport public publié par Deloitte et la Monetary Authority of Singapore, 2016)

Orange problématisait le processus participatif et démocratique comme un « système » de vote aujourd'hui opaque dont les résultats pouvaient être faussés au profit d'un acteur, c'est-à-dire à l'insu des électeurs. Le projet Ubin, lancé à l'initiative de la banque centrale de Singapour en association avec les banques commerciales opérant à Singapour, problématisait les systèmes et circuits des paiements inter-bancaires manquant d'efficacité, de sécurité, de transparence. Dans ces deux cas, le processus qui traduisait l'action d'utilisateurs de réseaux (citoyens qui expriment leurs voix, banques qui transfèrent de l'argent) en faits (la participation effective à un scrutin, la juste modification des comptes d'un réseau bancaire) était suspecté de compromission (possibilité de manipulation, problème d'efficacité et de sécurité).

Ces problématisations assimilaient des formes institutionnelles (processus démocratiques, administration de l'argent) à des réseaux informatiques défailants. La blockchain était vue comme une solution de substitution. Les innovateurs opéraient successivement deux « déplacements » ou « délégations » (Latour 1992 ; Akrih & Latour 1992). D'une part, un processus institutionnel était délégué à un réseau informatique (par exemple, le vote comme « système ») ; d'autre part, ce dernier était problématisé et ses qualités étaient déléguées à

Introduction générale

un autre réseau objet de l'innovation. Les qualités de ces réseaux innovants, aussi bien techniques qu'institutionnelles, étaient associées à leur architecture technique. À l'architecture contemporaine des réseaux informatiques dans lesquels un fournisseur de services joue le rôle du « serveur » et l'utilisateur celui du « client » (de ce serveur), la blockchain opposait une architecture « distribuée » ou « décentralisée ». Ces « serveurs » sont les machines qui inscrivent nos interactions numériques sur le *World Wide Web* et plus généralement dans une large part des applications d'Internet et des réseaux IP. Cette architecture semble naturelle tant elle structure nos relations numériques. Pourtant, ce sont ces serveurs qui, aux yeux des protagonistes au cœur de ce travail, étaient susceptibles de défaillances ou de compromissions techniques ou institutionnelles. L'architecture blockchain, au contraire, distribuait ce rôle de « serveur », quels que soient les objets substitués.

Le vocabulaire mobilisé par les acteurs témoignait de l'intrication des registres techniques et politiques associés à l'architecture informatique des réseaux informatiques. La notion vernaculaire « intermédiaire » désignait par exemple autant des médiateurs techniques que des acteurs suspectés d'agir sur le processus de constitution de faits. Il s'agit d'une version « institutionnelle » de la notion informatique « serveur ». « Intermédiaire » désignait tout acteur qui participait à former une relation sous forme numérique ; aussi bien ceux qui participaient normalement à la constitution des faits (assesseurs, présidents de bureaux de vote, personnel administratif, responsables politiques dans le cas du vote, ou banques, gestionnaires de systèmes d'information, banque centrale dans le cas de la monnaie inter-bancaire) que ceux qui cherchaient à compromettre cette constitution normale des faits (en fraudant, en rusant, en s'infiltrant de quelque manière que ce soit dans le processus institutionnel). Les réseaux de substitution « blockchain » étaient dits « sans intermédiaire » : ils étaient imaginés comme émancipateurs de toute intervention, que ces intervenants participassent aux institutions ou qu'ils leur étaient extérieurs, de manière à exclure toute possibilité de défaillance volontaire ou involontaire. Produire des faits inaltérables signifiait exclure toute intervention possible dans la traduction de relations numériques valant réalités collectives.

Introduction générale

Pour les protagonistes au cœur de ce travail, les « intermédiaires » ou les « serveurs » gouvernaient la production de faits sociaux de manière problématique : propres à leurs intérêts, qui étaient par nature impossibles à connaître. En réponse, ils proposaient de ré-architecturer les réseaux produisant des faits sociaux (échanges et décisions) de manière à prévenir toute forme d'intervention. Les « intermédiaires » ou les « serveurs » étaient vus comme des points de passages obligés, au sens de la notion élaborée par la sociologie de la traduction pour analyser le développement des sciences et des techniques (Callon 1984, Latour 1987, Latour 1992, Akrich et al. 2006, Muniesa 2015) : des entités agissant pour constituer les utilisateurs (comme des citoyens ou des banques) en collectif (d'une collectivité, d'un système inter-bancaire). Ce sont ces entités dont il fallût s'émanciper, en redéfinissant la manière de produire des faits sociaux dans une forme numérique.

Technologie de gouvernance

Cette thèse analyse la blockchain comme une technologie de gouvernance : un ensemble de connaissances, de pratiques, de modes de raisonnements assemblés dans la conception de dispositifs techniques ayant pour objet d'instituer des manières de gouverner. Prendre cet ensemble pour objet d'analyse consistait à approcher deux dimensions politiques des dispositifs construits comme « applications » de la « technologie » la blockchain. Premièrement, ces dispositifs avaient des effets politiques, du fait de leur relation à leur environnement et des présupposés éthiques et moraux de leurs concepteurs. Ces artefacts avaient des politiques qui se comprennent notamment en analysant les effets d'autorisation ou d'exclusion qu'ils produisent (Winner 1980) ; par exemple, le vote numérique excluait certaines catégories d'électeurs, d'assesseurs, et des formes d'intervention sur le processus électoral. Ces effets politiques étaient articulés aux présupposés éthiques et moraux prescrits par leurs concepteurs quand ils imaginaient un utilisateur de ces dispositifs (Akrich 1989) ; par exemple, Orange imaginait un votant qui doutait de la fiabilité de processus électoraux ou un assesseur fraudeur. Deuxièmement, ces dispositifs étaient conçus pour instaurer un ordre en société. Le développement des technologies au cœur de ce travail était alimenté de réflexions et de controverses prenant explicitement pour objet la

Introduction générale

bonne organisation sociale, vis-à-vis d'institutions ou de dispositifs techniques que les concepteurs critiquaient, mais aussi entre les concepteurs. La notion de technologie participe à analyser cette dimension : la systématisation d'un modèle technique construit au croisement de connaissances et de pratiques techniques, entrepreneuriales, financières, informatiques.

« Technologie de gouvernance » cherche à articuler ce que les concepteurs dénonçaient (le gouvernement par les intermédiaires des interactions numériques), l'horizon qu'ils opposaient, et comment ils faisaient advenir cet horizon en pratique ; en promouvant une technologie, en s'associant, en écrivant du code, et en investissant. Cette notion se distingue de celle proposée, dans les mêmes termes, par des économistes de la nouvelle économie institutionnelle qui naturalisent la dimension ordonnatrice de la technologie au prisme de leur théorie économique. En effet ils voient dans la blockchain une technologie susceptible d'être elle-même une institution de marché, c'est-à-dire de produire les formes de « gouvernance » suffisantes pour faire advenir ce qu'ils nomment, à la suite de Friedrich Hayek, une « catallaxie » ou économie auto-organisée (voir par exemple Allen et al. 2018a, 2018b, Davidson et al. 2016a, 2016b, 2018, MacDonald et al. 2016). Leur approche consiste à analyser la technologie comme mise en œuvre de théories économiques, plutôt que comme outil d'analyse de la normativité de cette technologie. Selon le juriste Alain Supiot, ce type d'analyse est conforme à la doctrine *Law and economics*³ qui prend le droit et les institutions comme instruments de mise en œuvre de théories (et du calcul) économiques plutôt que comme objets d'analyses par la théorie économique⁴. L'analyse proposée ici s'intéresse plutôt aux connaissances, aux pratiques, aux modes de raisonnements qui président, sont construits et assemblés dans la conception de technologies susceptibles d'être vues comme instruments pour gouverner. Ce travail vise à caractériser ce processus d'innovation comme une manière de faire advenir un certain

3 Doctrine à laquelle participe l'économie néo-institutionnelle, mais également la théorie des jeux ou la *New Comparative Analysis* consistant à évaluer les performances des systèmes juridiques nationaux, au vu des calculs d'utilité individuelle.

4 Supiot distingue les approches économiques qui font du droit un instrument de mise en œuvre de théories économiques de celles qui mobilisent une théorie économique pour analyser la normativité du droit. Le juriste cite des représentants de la sociologie des conventions et de l'école de la régulation : Laurent Thevenot, François Eymard-Duvernay, Olivier Favereau et Michel Aglietta.

Introduction générale

ordre, et non à témoigner d'un nouveau perfectionnement de l'organisation des marchés dans des formes techniques.

La notion de « gouvernance » est préférée à « gouvernement » pour des raisons empiriques et analytiques. « Gouvernement » suggère une distinction hiérarchique entre des gouvernés et des gouvernants formant un corps social. Or, empiriquement, la verticalité de ce rapport est exclue *a priori* par les concepteurs qui imaginaient au contraire des relations horizontales, formées par un dispositif technique sur lequel aucun acteur ne puisse intervenir ; en particulier, un dispositif qui instaure l'absence de gouvernants mis en position institutionnelle d'exercer un pouvoir légitime. Analytiquement, cette distinction s'inscrit, d'une part, à la suite de travaux du champ dit de la « gouvernance d'Internet » qui remarque que « gouvernement » est associé à l'exercice d'un pouvoir exercé sur un territoire et une population, à des principes hiérarchiques, ou encore dans les termes de Max Weber à l'existence d'une institution exerçant le monopole de la violence légitime (Rossi et al. 2022). D'autre part, cette distinction s'inspire de travaux d'Alain Supiot, alors titulaire de la chaire « État social et mondialisation : analyse juridique des solidarités », dédiés au passage du gouvernement par les lois à la gouvernance par les nombres (Supiot 2013, 2015). Le juriste voit dans ce passage la substitution du nombre à la loi comme fondement légitime de la norme en société, une tendance qui se renforce d'autant plus dans les sociétés occidentales⁵.

La gouvernance d'Internet est un domaine de recherche qui pose la singularité des questions de gouvernance propres à Internet, due notamment à la diversité des instruments d'exercice du pouvoir et des acteurs qui participent à l'élaboration, à la maintenance ou à la mobilisation de ces instruments : des textes juridiques énoncés par les institutions politiques locales jusqu'à supra-nationales, mais aussi les contrats entre acteurs privés, les standards techniques, les formats de données, les logiciels ou encore l'infrastructure matérielle. Ces travaux foisonnent par les disciplines autant que les méthodes. Ils montrent que, bien souvent, les controverses portant sur des objets qui semblent purement techniques se

5 Le juriste contraste cette tendance, par exemple, avec la tradition de gouvernement en Chine, mêlant légalisme et ritualisme.

Introduction générale

révèlent être tout autant politiques. Ils identifient une pluralité d'acteurs, des institutions formelles comme l'ICANN, le W3C ou l'IETF à des processus de décision plus informels (Van Eeten & Mueller 2012, Musiani et al. 2016, Musiani 2022). Parmi ces derniers, l'architecture technique des infrastructures réseaux est devenu un objet d'étude central pour comprendre la politique exercée au travers d'Internet, par exemple en matière d'innovation de services Internet (Musiani 2013), de communications numériques (Ermoshina & Musiani 2019) ou, plus immédiatement lié à l'objet du présent travail, la gouvernance de Bitcoin (De Filippi & Loveluck 2016 ; Musiani et al. 2018).

Ce travail s'inscrit à la suite de ces études, en particulier de celles attentives aux formes de l'architecture technique comme gouvernance (voir notamment Musiani 2013, 2015). Ces dernières ont mis en évidence les redistributions de rôles d'un large spectre d'acteurs dans les architectures décentralisées, distribuées ou encore pair-à-pair, par contraste avec celles dites « centralisées », c'est-à-dire impliquant un fournisseur de service jouant seul le rôle de « serveur » et l'utilisateur le rôle de « client ». Les infrastructures blockchain prolongent cette histoire des technologies de réseaux décentralisées⁶, mais posent de nouvelles questions propres à leurs fonctions. Ces dispositifs pair-à-pair échangent des « contenus » : (flux) vidéos, images, communications textuelles, requêtes d'indexation des contenus eux-mêmes. Or, les blockchains ont pour fonction principale de former et d'enregistrer de relations d'échanges ou d'associations, conçues comme des références inaltérables, dissociant ainsi traces d'un contenu et contenu lui-même. Du point de vue de l'information comme « contenu », la blockchain s'intéresse plus aux « méta-données » qu'aux « données ». Alors que les études précédentes observaient des « contenus » qui « circulent » dans des réseaux (souvent par bouts, produisant la « *privacy by design* »), les blockchains enregistrent de manière immuable les traces de relations dans le temps et dans l'espace. Certains auteurs voient les blockchains comme les témoins technologiques de l'importance contemporaine donnée à la traçabilité dans de nombreux domaines, qu'ils proposent d'étudier comme « infrastructures de traçabilité » (voir par exemple Power 2019).

6 On retrouve aussi bien une architecture technique de type décentralisée que nombre de critiques opposées aux architectures centralisées déjà identifiées dans les réseaux pair-à-pair, notamment : contrôle excessif des fournisseurs de services, « opacité » de ce contrôle du point de vue de l'utilisateur, vulnérabilité aux « points de dépendance uniques » du réseau (*single points of failure*).

Introduction générale

Ordonner les relations pour faire société : les architectures de réseaux distribuées étaient ici conçues pour garantir un ordre nécessaire à des relations de pair-à-pair. Cette fonction « ordonnatrice » par l'architecture se distingue des « droits » (à la vie privée, d'accès à des contenus, de propriété intellectuelle) formés par l'architecture dans les études des architectures distribuées précédemment citées. Alors que les échanges de contenus sont conçus comme connexions bilatérales et éphémères entre un fournisseur et un utilisateur, la reconnaissance d'une relation entre pairs suppose que la relation soit totalisée dans une forme durable : une relation de propriété sur un objet échangé (comme un montant en argent dans le cas du projet Ubin) ou d'association entre pairs (l'expression d'un vote dans le cas du projet d'Orange) ne prend son sens que ramenée à un tout perenne (qui garantit que l'argent est bien transféré, ou que le vote est bien pris en compte). C'est cette totalisation qui posait problème aux protagonistes : la capacité de formation de relations d'échange ou d'association était mise à l'épreuve de la matérialité des dispositifs qui totalisaient ces relations. Ces dispositifs permettaient les « interventions » quelles qu'elles soient : d'institutions « légitimes » mais capables d'agir selon leurs propres « intérêts », tout autant que de acteurs réussissant à modifier les relations en rusant. L'innovation de ces protagonistes totalisait les relations par une architecture de réseaux distribuée produisant des références, enregistrements ou « traces » de relations reconnues des membres d'un groupe qui les mobilisaient, individuellement ou collectivement, pour bâtir des organisations des échanges (économies) et s'organiser (associations).

Autrement dit, l'architecture informatique devait former des relations d'échanges et d'associations entre pairs libérés de toute forme d'hétéronomie : sans norme posée en surplomb et limitant la toute puissance subjective pour former ces relations. La matérialité du calcul par l'architecture distribuée le rendait « autonome », au sens où le résultat de calcul comme « trace » deviendrait émancipé de toute norme extérieure aux individus libres de former des relations décidées souverainement. Substituer le calcul à toute forme de norme extérieure aux individus (en particulier, à la loi) est typique de ce qu'Alain Supiot appelle la « gouvernance par les nombres ». Le juriste voit une généralisation du calcul comme fondement de la légitimité des normes, à différentes échelles : entreprises, État,

Introduction générale

communautés et relations internationales. Ces normes sont intériorisées par les individus, à la manière de lois biologiques ou du programme d'un ordinateur. Elles se distinguent notamment de la loi, construite comme référence extérieure de production d'un ordre en société depuis l'Antiquité grecque⁷ (Supiot 2013). L'originalité du calcul produit par ces architectures distribuées (blockchain) est d'être utilisé comme institution autonome : l'opération de calcul étant produite collectivement (entre nœuds du réseau), elle donne une force normative à ses significations décidées indépendamment par les utilisateurs (formulation des relations d'échange et de décisions). Les premiers sont les garants des pactes des seconds. Ce calcul n'autonomise pas une forme juridique : à la différence de la gouvernance par les nombres décrite par Supiot, le calcul ne donne pas force normative au droit en le relativisant comme une norme sur un marché plus large, mais à des relations bilatérales entre individus souverains, réduites à des traces vues comme faits.

La notion de « technologie » mobilisée dans « technologie de gouvernance » emprunte à un autre penseur du gouvernement, lui aussi titulaire d'une chaire au Collège de France. Dans son cours *Securité, Territoire, Population* (1977-1978), Michel Foucault propose une généalogie de la gouvernementalité, c'est-à-dire l'analyse historique des institutions, procédures, analyses et réflexions, calculs et tactiques qui ont conduit à ce qu'aujourd'hui soit exercé une forme de pouvoir dit « gouvernement » prééminent sur tous les autres (dont la souveraineté et la discipline), prenant la population pour cible principale (Foucault 2004a). Cette forme de pouvoir a amené, d'une part, le développement de divers savoirs et prend aujourd'hui pour forme majeure l'économie politique, et, d'autre part, le développement d'une série d'appareils spécifiques de gouvernement qu'il appelle les « dispositifs de sécurité ». Ces dispositifs sont des « technologies de pouvoir », au même titre que la « technologie disciplinaire ». La pensée de Foucault est intéressante pour

⁷ Dans ce cours, le juriste propose une histoire des manières de penser l'institution de la société. Il rappelle que la loi apparaît en Grèce, quand une Cité cherche à se gouverner elle-même. Avec l'idée d'institution d'une référence normative comme œuvre humaine (par opposition aux lois de la nature ou des dieux), la loi civile se trouve privée de garant et par là soumise aux risques de relativité et de contradiction permanente des gouvernants eux-mêmes (à l'exercice de leur pouvoir). La démocratie est inventée comme cité qui se gouverne elle-même et qui applique à tous les mêmes lois (isonomie). À Rome, avec la République, la loi devient une technique de gouvernement autonome du régime politique : l'ordre juridique s'impose aux gouvernants (il autonomise la forme juridique et investit les gouvernés de droits opposables) et est instrument de leur pouvoir (la loi civile donne force normative à la volonté humaine et peut être modelée et transformée par elle).

Introduction générale

analyser les manières de gouverner dans une continuité historique⁸ : l'exercice d'un « art de gouverner » est objet de réflexions, d'ajustements en termes de savoirs, de formes institutionnelles et d'objets. Il emprunte à différentes technologies de pouvoir, les combine en fonction de circonstances historiques. Cet art suit une « ligne de pente », il est « infléchi » : c'est ce type de transformations que théorisent, par l'architecture informatique, les innovateurs des blockchains. Les technologies pair-à-pair sont mobilisées pour instituer des nouvelles manières de gouverner par Internet ; la blockchain pourrait être vue comme un ensemble d'instruments de gouvernance qui s'inscrivent dans une histoire de la « gouvernançalité ».

La notion de « technologie » mobilisée ici puise également dans les travaux en anthropologie des sciences et des techniques intéressés par l'écriture pour analyser les spécificités de la gouvernance propre aux dispositifs blockchains sans écraser la diversité des différents régimes de gouvernance qu'ils produisent en pratique. Par exemple, Jack Goody désigne l'écriture comme « technologie intellectuelle » (Goody 1979). Selon Goody, écrire n'est pas une simple transcription de pensées orales, mais produit des formes de raisonnement spécifiques : on ne réfléchit pas de la même manière à l'écrit et à l'oral. Pour autant, toutes les formes d'écriture ne produisent pas les mêmes manières de penser. Autre exemple : David Pontille montre que la signature collective d'une œuvre scientifique n'est pas un simple signalement de la participation de différents individus, mais est révélateur d'« agencements scientifiques ». La signature collective est une « technologie d'attribution », qui s'exprime selon des régimes spécifiques aux disciplines qui codent avec la signature les contributions qui relèvent de l'individuel et du collectif, de l'accessoire et du décisif, du scientifique et du technique (Pontille 2016).

Ainsi équipée, la notion de « technologie » dans « technologie de gouvernance » vise à articuler une analyse de la blockchain comme un type de gouvernance spécifique à la

8 Ce travail retient de Foucault le travail de conceptualisation du gouvernement comme un « art » continu dans le temps plutôt que sa conception du pouvoir, considérée par nature comme exercé par des gouvernants aussi bien dans *Sécurité, Territoire, Population* que dans *La Naissance de la biopolitique* (Foucault 2004b). Cette critique est formulée par Supiot qui reproche à Foucault de rabattre l'exercice du pouvoir sur le gouvernement avec la notion de « bio-pouvoir », un geste que ce dernier associe à la modernité occidentale et qui exclut, notamment, le gouvernement par des acteurs privés qu'englobe plus facilement la notion de « gouvernance ».

Introduction générale

diversité de ses régimes. Différents traits de la gouvernance par les dispositifs blockchain ont été esquissés plus haut : en termes de production de faits inaltérables, d'évitement de l'« intervention » sur les relations, ou d'institution d'une garantie reconnue par un même corps social. Ils indiquent la systématisation d'une forme d'agencement socio-technique comme instrument de gouvernance des relations d'échange et d'association. Toutefois, différents régimes étaient propres à la manière de constituer les corps sociaux auxquels un dispositif blockchain aurait servi de référence. Les deux cas donnés en illustration plus haut montrent que les dispositifs blockchain sont candidats pour gouverner autant des relations entre banques qu'un processus démocratique. Avec le cas de la banque centrale de Singapour, le corps concerné par la formation de relations d'échanges est constitué d'institutions financières connues à l'avance qui échangent entre elles et qui sont les seules à pouvoir lire l'enregistrement de leurs transactions dans l'infrastructure. Cette dernière fonctionnait comme un intranet, dont les membres étaient cooptés en fonction de leur statut d'opérateur bancaire. Au contraire, Orange visait l'ensemble d'un corps social dont les contours ne pouvaient pas être précisés *a priori* et préférait une infrastructure dite « publique », accessible par tout Internaute, et dont l'administration était réputée indépendante de l'entreprise.

Imaginaires de l'autonomie : entités souveraines et ordre autonome

Comment faire tenir un ordre garantissant à la fois la souveraineté des entités le peuplant et sa propre autonomie ? Quelles visions du monde président et sont élaborées dans la construction de cette technologie de gouvernance ? Quelle conception du rapport de l'individu au tout cet ordre suppose-t-il ? Quelle rationalité gouvernementale résulte d'un ordre selon lequel les relations sociales sont gouvernées comme des faits réduits à des écritures à la main d'individus souverains ?

Cette thèse étudie ces questions en s'appuyant sur une enquête auprès de concepteurs en train d'imaginer cet ordre autonome par des développements technologiques, entrepreneuriaux, financiers et associatifs. Cette enquête est présentée dans la section suivante. Les « applications », comme Ubin ou LeVote, étaient à l'époque expérimentales,

Introduction générale

aussi bien techniquement, socialement qu'économiquement ou financièrement. Les concepteurs eux-mêmes étaient leurs propres utilisateurs. Des entreprises proposaient des « *Proof of concept* », pendant que des développeurs, entrepreneurs, utilisateurs, et investisseurs imaginaient un Web où les échanges et les associations seraient émancipés des grands noms du numérique au profit d'un « *crypto space* » tout juste en train d'émerger. L'imagination qu'ils déployaient dans ce processus d'innovation parle autant du monde qu'ils cherchaient à faire advenir que d'eux-mêmes dans le monde. En particulier, ce processus d'innovation faisait apparaître des alliances entre acteurs souvent opposés *a priori* dans le débat public comme dans l'arène scientifique, par exemple entre promoteurs de « cryptomonnaies » et de « blockchain ». Ces convergences peuvent utilement être comprises en termes d'imaginaires partagés.

L'enquête montre que l'ordre qu'ils imaginaient n'avait rien de spontané. Il était au contraire objet d'une ingénierie complexe par la diversité des savoirs mobilisés (notamment entrepreneuriaux, financiers, de sciences des réseaux informatiques, ou de théorie des jeux) autant que par l'éclatement géographique et la diversité de ses acteurs. Toutefois, les travaux associant la blockchain à un ordre spontané (notamment d'économistes cités plus haut) permis par la blockchain identifient bien une partie de l'imaginaire qui était à l'œuvre : la perspective, guidant ce processus d'innovation, d'infrastructures faisant se rencontrer des fournisseurs-offreurs de services et des utilisateurs-consommateurs avec le minimum de « coûts de transaction », selon le vocabulaire des économistes Ronald Coase et Oliver Williamson. Cet horizon formule en termes entrepreneuriaux l'imaginaire cybernétique : un univers peuplé de particules contractantes, agissant avec d'autres en « rétroaction » en fonction de la maximisation de leur utilité individuelle⁹. Il rejoint celui que décrit Alain Supiot avec la gouvernance par les nombres, fondé sur le modèle de l'ordinateur plutôt que sur l'horloge qui apparaît dès l'apparition de la version moderne du gouvernement par les lois, de Thomas Hobbes à l'organisation tayloriste du travail.

9 Les références cybernétiques sont explicites dans les analyses des économistes néo-institutionnalistes, jusque dans les développements technologiques que proposent ces mêmes auteurs (voir par exemple Davidson et al. 2016a, 2016b, 2018). Une des coautrices était aussi une actrice du développement des blockchains, proposant d'étudier le « potentiel de la technologie blockchain dans la mise en place d'un nouveau système de valeur qui soutiendra mieux la dynamique du partage social » (Pazaitis & De Filippi 2018), en participant à la conception d'une application appelée « *Backfeed* », littéralement « rétroaction ».

Introduction générale

Mais cet imaginaire n'est pas statique : il participe activement à faire advenir l'horizon qu'il dessine. Ce travail propose d'analyser la dynamique d'innovation, notamment les efforts produits en pratique pour que cet ordre advienne. Les analyses statiques se limitent à la description de « ce que la blockchain pourrait faire » ou à son « potentiel », c'est-à-dire à dessiner l'horizon d'un univers entrepreneurial sans hétéronomie peuplé d'entités souveraines. L'analyse dynamique vise à comprendre l'imaginaire qui guide ces efforts pour faire en pratique advenir l'ordre décrit dans les analyses statiques : étudier en même temps la promotion de technologies et les formes politiques imaginées susceptibles de faire advenir cet ordre. Cette partie de l'analyse prend au sérieux ce qui fait voir aux concepteurs du « potentiel » dans cette technologie : la production d'un ordre qui soit insensible aux prises du reste du monde, c'est-à-dire qui règle le problème de la matérialité des dispositifs permettant les « interventions » sur la formation des relations.

Le concept d'« imaginaire sociotechnique » développé par Sheila Jasanoff vient utilement équiper cette démarche. Ce concept est bâti sur une comparaison entre le développement et la régulation du nucléaire aux États-Unis et en Corée du Sud, deux pays dans lesquels la technologie est imaginée en lien avec le rapport au pouvoir politique (Jasanoff & Kim 2009). Pourtant, les significations de ces imaginaires diffèrent entre les deux pays dans les pratiques scientifiques, technologiques et politiques : il se formule en termes de confinement d'une part, de développement de l'autre. Ces formulations ont des effets en retour, notamment dans la manière de gérer les incidents sur les infrastructures nucléaires ou dans le développement du mouvement anti-nucléaires.

Avec la blockchain, deux formulations conjointes de l'autonomie et du développement des réseaux pair-à-pair sont formulées ensemble. La première formulation « statique » projette des individus qui échangent et s'associent souverainement, dans la lignée des utopies d'Internet et de l'imaginaire cybernétique. La seconde formulation vise à faire de la première une réalité. Elle traduit l'imaginaire à l'œuvre dans la première formulation au problème de la matérialité des traces des échanges et des associations : la rationalité d'un monde peuplé d'entités contractantes, rétro-agissant dans le monde en fonction de leur calcul d'intérêt, sert de fondement à l'établissement à la production des traces des relations.

Introduction générale

Cette deuxième formulation fait des réseaux pair-à-pair une technologie instituante. Alors que la première formulation indique ce qui « doit être » dans un monde imaginé et en construction, la seconde indique « comment instituer ce qui doit être » : les relations de pair-à-pair entre utilisateurs et fournisseurs de services Web doivent être protégées des techniques de pouvoir, les « interventions » des « intermédiaires » sur les serveurs. Sous cet angle, les significations d'un imaginaire sociotechnique s'articulent et se distinguent par les entités qu'elles mettent en relation pour produire l' « autonomie ». La seconde formulation met en relation des entités produisant des traces qui se substituent aux institutions qui empêchent matériellement le développement de la première formulation de cet imaginaire. Ces deux formulations ne se distinguent donc pas ici en termes de zones géographiques, économies et États où le lien entre pouvoir politique et technologie est formulé localement, mais en termes d'objets qui devaient être rendus autonomes : l'individu pour la première formulation, l'espace peuplé de ces individus pour la seconde.

La section suivante présente l'enquête. La troisième section articule les deux formulations des imaginaires de l'autonomie et des réseaux de pair-à-pair avec la notion d' « espaces transactionnels ». La quatrième section précise la méthode pour analyser la construction de ces espaces : suivre les traductions sociotechniques qui forment en cascade les « transactions », objets qui ont du sens autant pour les utilisateurs et producteurs de services imaginés comme souverains (première formulation de l'imaginaire) que pour les entités chargées de faire advenir l'espace autonome dans lequel les premiers agissent souverainement (deuxième formulation).

2. Démarche et enquête

Point de départ : blockchain-mania et crypto-bashing institutionnels

Orange Vallée, division dédiée à l'innovation au sein d'Orange, a pour mission d'imaginer et de développer les services numériques de demain, à destination des particuliers, professionnels et entreprises. Le projet VoteChain¹⁰, sous la

10 « VoteChain » est le premier nom qui avait été donné au projet ensuite commercialisé sous le nom

Introduction générale

responsabilité de Monsieur X, a pour objectif d'évaluer le potentiel produit et business de la technologie blockchain au service du vote en ligne, et de développer une offre opérationnelle en en tirant le meilleur parti. (document interne projet VoteChain d'Orange, 2016¹¹)

A group of banks in Singapore, with the support of MAS, Singapore's central bank and financial regulatory authority, have also been developing a payment system prototype using DLT in which bank users can exchange currency with one another without lengthy processing times, expensive processing fees, or intermediaries. R3 – a consortium specialising in DLT – has partnered with the group on the initiative, known as Project Ubin. (rapport public Project Ubin Phase 1 de la banque centrale de Singapour, 2016)

Dès 2016, votes et transactions monétaires inter-bancaires étaient imaginés dans des formes techniques similaires : des communications qui pourraient être numérisées ou dont la numérisation pourrait être améliorée. Ces « cas d'usages » étaient imaginés à une époque où la blockchain mettait le monde des affaires en ébullition. Des anticipations de transformations sociales profondes semblaient à portée d'investissements. En 2015, on voyait une technologie « derrière » ou « sous-jacente à » Bitcoin qui serait capable de changer l'économie et le monde, aussi bien en une de *The Economist* (2015) que dans la littérature pour entreprises et décideurs politiques (Swan 2015). Dans le même temps, des investisseurs de tous poils investissaient dans des startups, lesquelles voyaient dans la monnaie numérique Bitcoin une architecture informatique susceptible de devenir une « technologie » terreau de nouveaux usages. Les frères Tapscott, influents investisseurs de la Silicon Valley, publiaient en 2018 un livre qui analysait la blockchain comme une révolution en cours de « la monnaie, des affaires et du monde » (Tapscott & Tapscott 2016). De grandes sociétés de conseil dédiaient des équipes entières au développement d'offres spécifiques et expérimentales, industrie par industrie, appelées « *proofs of concept* »¹². Ces différents acteurs se retrouvaient aux côtés de régulateurs dans des arènes comme l'organisation internationale de lobbying *World Economic Forum*¹³. La blockchain

« LeVote ».

11 Le responsable en question a été anonymisé.

12 Ces « preuves de concept » tentaient généralement, à partir d'un prototype réalisé avec un client, de généraliser « ce que le « potentiel » de la technologie blockchain. Voir par exemple la proposition d'Accenture (2017) de « réingénierie de la chaîne de valeur des médias ».

13 Voir par exemple Ulieru (2016) pour le *World Economic Forum*.

Introduction générale

était alors en tête de l'ordre du jour de dirigeants politiques et économiques en raison du possible « impact » sur l'économie dont la technologie était alors auréolée.

A cette époque, dans la presse généraliste et spécialisée, une opposition s'installait entre une « technologie blockchain » aux perspectives économiques prometteuses et des cryptomonnaies inquiétantes¹⁴. La plupart des gouvernements, institutions financières et grandes entreprises attribuaient aux cryptomonnaies une charge morale négative : elles favoriseraient le blanchiment d'argent ou le développement du terrorisme, elles reposeraient sur des schémas de Ponzi ou joueraient une excitation passagère pour des produits dont les valorisations dépassaient l'entendement, à la manière de la tulipomanie du XVIIe siècle. Dans le même temps, ces mêmes institutions présentaient la technologie blockchain comme l'héritière et double angélique des cryptomonnaies. Entre 2016 et 2018, la blockchain gravissait irrésistiblement la cartographie de référence développée par la société de conseil et de recherche sur les technologies Gartner¹⁵. La blockchain y apparaissait comme une de ces technologies investies d'attentes importantes à une époque donnée, aux côtés du « cloud », des imprimantes 3D ou plus récemment, de l'« intelligence artificielle ». Présentes jusque dans la version de 2015 de la « *hype cycle* » des (projets de) technologies qui excitent les appétits d'investisseurs et bouleverse les agendas technologiques des grandes entreprises, les « cryptomonnaies » en disparaissent en 2016 alors que la « blockchain » y faisait son entrée la même année (Gartner 2015, 2016). En 2017 et 2018, Gartner positionnait la blockchain à la charnière entre un « pic des attentes exagérées » et un « gouffre des désillusions » (Gartner 2017, 2018).

« La blockchain » participait alors d'un régime des « promesses technoscientifiques », selon la définition qu'en ont donné des travaux d'études sociales des sciences et des techniques (Joly 2015). À l'image des nanotechnologies, la blockchain véhiculait des promesses d'un avenir meilleur : rendre le vote plus démocratique avec Orange, ou la finance plus

14 Des analyses du discours médiatique se sont intéressées à la valorisation de la blockchain contre les cryptomonnaies et à leur participation à l'« adoption » de la technologie (Chow-White et al. 2020, Perdana et al. 2021).

15 Cette courbe représente ce qu'il est commun d'appeler des « *buzzwords* » dans les milieux de recherche et développement, d'investissement, et de recherche dans les technologies. Elle théorise le devenir d'une technologie depuis son apparition fulgurante jusqu'à un hypothétique « plateau de productivité ».

Introduction générale

transparente avec la banque centrale de Singapour. Elle représentait alors un gisement d'espoirs pour différentes industries ou administrations. La diversité des acteurs participant à ce processus (États, régulateurs nationaux et internationaux, entreprises, startups, centres de recherche, communautés de développement informatique) était caractéristique de ces formes d'innovations contemporaines par les promesses technoscientifiques (Joly et al. 2010 : 22-23). L'activité de certains était d'ailleurs directement orientée vers la crédibilisation de ces promesses ; c'est par exemple le cas des sociétés U et Deloitte, conseils respectifs d'Orange et de la banque centrale de Singapour, autrices des rapports dont sont issues les citations ci-dessus qui vantaient aussi bien les perspectives de nouveaux services pour leurs clients que leur propre expertise pour cette technologie émergente. Cette crédibilisation passait également par l'arène scientifique¹⁶.

Ethereum : objet d'enquête à l'articulation entre blockchain et cryptomonnaies

Je commençais à scruter les écrits de la presse spécialisée en finance et en technologie mentionnant la notion de « blockchain » en 2016 ; j'étais intrigué par les mentions de cette nouvelle technologie dans mon espace professionnel. « Blockchain » préoccupait la société de conseil qui m'employait. Cette société voyait dans l'émergence de cette technologie une opportunité pour bâtir une nouvelle offre de missions dans l'air du temps. La blockchain s'imposait comme une candidate parfaite pour figurer dans le catalogue de missions familièrement appelées « le *new* » aux côtés de technologies comme la « robotique » (laquelle deviendra quelques années plus tard « intelligence artificielle »). La blockchain préoccupait également la direction financière de la grande banque au sein de laquelle je travaillais comme « consultant en organisation »¹⁷. Mon intérêt pour cette technologie part

16 Des revues et des centres de recherches prenaient explicitement la blockchain comme un objet technologique prometteur, en lien avec les préoccupations industrielles. Par exemple, Ellul (2021) est chercheur au « Centre for Distributed Ledger Technologies » de l'Université de Malte, dont le gouvernement s'est déclaré terre d'accueil des projets de cryptomonnaies ; il qualifie la santé de cet objet en termes de développement entrepreneurial, de prix des cryptomonnaies, ou de position sur la courbe de Gartner, dans « The Journal of The British Blockchain Association ». Autre exemple : Treiblmaier (2019) propose dans la revue « Frontiers in Blockchain » des recommandations pour « une recherche sur la blockchain plus rigoureuse », qui soit « mieux » articulée aux réalités industrielles.

17 J'ai commencé à travailler en mission de conseil pour cette banque en 2013 lors d'un stage de fin d'études

Introduction générale

ainsi d'une curiosité politique : « blockchain » me paraissait être un label auquel étaient associées des politiques qui me paraissaient contradictoires. D'une part, les cryptomonnaies et Bitcoin étaient vues comme solutions techniques pour un monde sans banques, lesquelles étaient désignées par leurs promoteurs comme discriminatrices dans l'accès aux services financiers et garantes de politiques monétaires anti-démocratiques (voir par ex. Favier & Takkal Bataille 2018). D'autre part et comme suggéré ci-dessus, « la blockchain » était un réservoir de promesses qui agitaient le monde des affaires en général, et les grandes banques en particulier. Ces dernières voyaient dans Bitcoin une invention qui pourrait être réemployée pour de nouveaux usages au service de leurs activités commerciales et administratives, à l'image du prototype bâti par la banque centrale de Singapour qui vise, à l'anti-thèse de Bitcoin, à renforcer le système financier.

C'est à cette époque et par articles de presse interposés que je rencontre Ethereum. Mais ce n'est qu'à l'été 2018, quelques mois après le début de l'enquête, que j'ai choisi de centrer mon étude sur ce projet technologique imaginé en 2013 et lancé matériellement en 2015. Cet objet me semblait intéressant pour explorer la contradiction apparente entre politique des cryptomonnaies et politique de la blockchain. D'une part, Ethereum était l'infrastructure d'une cryptomonnaie appelée « ether »¹⁸. Son cours, établi sur des places d'échanges communément appelées *exchanges* (ressemblant à des bourses alors non régulées) était, comme celui du bitcoin, tendanciellement croissant. La presse voyait dans ce réseau pair-à-pair un « potentiel » pour des usages infinis d'un genre nouveau : « décentralisés » et « autonomes » vis-à-vis des offreurs de services qui structuraient le Web de la fin des années 2010. Mais dans le même temps, Ethereum commençait à être vu comme un logiciel pour des infrastructures privées d'entreprises industrielles ou de services.

en école d'ingénieurs. Après une mission d'assistance à la mise en œuvre des dernières réglementations prudentielles et comptables exigeant des banques européennes de mettre en place des outils et des processus permettant de calculer des « ratios de liquidité », mes activités ont été étendues à un rôle de conseil et de *management* attaché à différents projets du directeur de l'entité de la banque en question qui contractait avec la société qui m'employait.

18 Je reprends la convention syntaxique des acteurs qui désignent en général le nom d'une cryptomonnaie avec une lettre majuscule sans article (Bitcoin, Ethereum) et l'unité de compte de cette cryptomonnaie avec une lettre minuscule et un article défini (le bitcoin, l'ether).

Introduction générale

Le cas de la banque d'investissement JP Morgan illustre la position centrale d'Ethereum, entre « cryptomonnaies » et « blockchain ». En 2017, son *Chief Operating Officer* (CEO) Jamie Dimon prenait position contre Bitcoin : il qualifiait la cryptomonnaie d' « arnaque » destinée aux dealers de drogue, aux assassins et aux personnes vivant en Corée du Nord (Monaghan 2017). La même année, la banque participait à fonder l' « *Ethereum Enterprise Alliance* », un consortium d'entreprises qui se donnait pour objectif de développer un logiciel blockchain à destination d'entreprises, à partir du code de la cryptomonnaie Ethereum. Cette initiative était la seconde pour JP Morgan qui avait déjà participé à fonder un consortium du même type en 2014 (Irrera 2017a, 2017b). Ce dernier, appelé R3, se donnait comme objectif de bâtir une solution logicielle indépendante d'autres initiatives liées aux cryptomonnaies. Chacun de ces consortia cherchait à développer un logiciel blockchain candidat à devenir un standard *open source* pour l'industrie¹⁹.

L'hybridité d'Ethereum, à la fois cryptomonnaie (infrastructure publique) et blockchain (logiciel pour infrastructures privées), m'offrait une possibilité d'explorer la tension qui me préoccupait autour d'un même nom. Il me semblait important, dès le départ de l'enquête, de prendre « blockchain » et « cryptomonnaies » comme des catégories vernaculaires, ni tout à fait homogènes, ni mutuellement excluantes. Il s'agissait par là d'interroger, par l'enquête, les positions publiques d'acteurs comme JP Morgan qui présentaient le développement technologique comme un processus chronologiquement linéaire d'un point de vue technique mais en rupture d'un point de vue politique : selon eux, Bitcoin pouvait évoluer, vidé des inspirations idéologiques et militantes, qui ont été qualifiées en termes de crypto-anarchisme et de cyber-libertarianisme (voir par exemple Golumbia 2016, Brunton 2019). Le développement d'Ethereum était au contraire foisonnant et articulait ce qui pouvait discursivement ressembler à deux « sphères » indépendantes mais qui co-construisaient des formes de gouvernance des relations aux inspirations (modes de pensées, visions du monde et formes de rationalité) circulant par l'innovation technologique et entrepreneuriale.

19 Aux côtés d'institutions financières, ces consortia étaient principalement composés d'entreprises technologiques (comme Microsoft ou IBM) et de cabinets de conseils et d'audit (comme Accenture ou KPMG). Ces dernières finançaient les activités de développement technologique du consortium et participaient à leur gouvernance. R3 se donnait pour objectif de développer un logiciel indépendant de tout autre projet blockchain. L'Ethereum Enterprise Alliance se donnait pour objectif de développer une version d'Ethereum pour entreprises.

Démarche d'enquête : explorer les réseaux de développement d'Ethereum

J'ai approché différents acteurs en différents lieux pour privilégier l'analyse de « comment » les concepteurs problématisaient des réseaux et des manières de gouverner, plutôt que celle du « ce » qu'ils problématisent (diverses relations d'échange et de décision). D'une part, « ce » qu'ils problématisaient était le point de départ de ma curiosité pour ces objets : Bitcoin et la banque centrale de Singapour problématisent tous deux le système financier, mais dans des termes (*a priori*) radicalement opposés. D'autre part, il me semblait important d'interroger la séparation affichée entre développement des « cryptomonnaies » et des « blockchains ». Rien n'indiquait qu'il aurait été pertinent d'analyser « ce » qu'ils problématisaient comme des « options » (Joly et al. 2010 : 30) ou des « solutions alternatives » (Joly 2015 : 4) véhiculant chacune des « promesses » en compétition. Au contraire, l'enquête montre que le processus d'innovation associait des startups, investisseurs et grandes entreprises qui collaboraient. Les études sociales des techniques, héritières des études sociales des sciences, se sont opposées aux analyses linéaires des processus d'innovation dès les années 1980. Le cas du développement du néon comme nouvelle technique d'éclairage (Bijker 1992) montre bien que l'analyse du développement technologique suppose de s'intéresser à la pluralité des acteurs en présence pour analyser en même temps les processus de conception et de mise sur le marché ainsi que la qualité ou la signification sociale associée à une technique.

Mon enquête a commencé par une phase exploratoire, à Singapour, en février 2018. Singapour était alors un des épïcêtres mondiaux du développement de la blockchain. La cité-Etat regroupait les bureaux asiatiques de différentes sociétés nationales et multinationales participant à des consortia, ainsi qu'un ensemble d'acteurs qui formaient un « écosystème » : entrepreneurs, investisseurs publics et privés, fondations de développement de logiciel. Toujours consultant à l'époque, j'ai été invité par Liliana Doganova et Brice Laurent, chercheurs au Centre de Sociologie de l'Innovation et responsables de l'option « Affaires publiques et innovation » du cursus ingénieur-civil, à me joindre au voyage à vocation de recherche et d'enseignement qu'ils organisaient à

Introduction générale

Singapour avec Jérôme Denis, également chercheur au CSI. Ce voyage m'a permis de rencontrer différents acteurs qui participaient au processus d'innovation de « la blockchain », dans un temps et un espace limités. Je préparais ce voyage en multipliant les demandes d'entretiens tous azimuts avec pour seul critère : acteur qui associe (ou se fait associer dans la presse en ligne) « blockchain » à son activité. J'ai conduit²⁰ 18 entretiens qui peuvent schématiquement être distingués entre, d'une part, des entrepreneurs (startups) et, d'autre part, des acteurs institutionnels. Ces derniers occupaient différentes positions dans de grandes entreprises ou administrations directement aux prises avec la construction de prototypes blockchain²¹. Les rencontres avec les premiers ont fait apparaître deux régularités : huit sur les dix entrepreneurs travaillaient en lien direct avec Ethereum ; et parmi ces huit personnes, le responsable local de la société ConsenSys entretenait des relations personnelles avec chacun des sept autres, ainsi qu'avec des acteurs institutionnels, comme les représentants de la banque centrale de Singapour.

ConsenSys était au cœur du développement d'Ethereum et de la « technologie blockchain », en 2018 et durant les années suivantes. Cette société a été fondée en 2015 par Joseph Lubin, un entrepreneur qui a construit une fortune personnelle en investissant dans Bitcoin et les cryptomonnaies au début des années 2010 après une carrière dans les services financiers débutée dans les années 1990. À partir de juin 2018, à Paris, j'ai suivi les activités de cette société qui se disait alors « *startup venture studio* » : à la fois fonds d'investissement, incubateur, organisateur de réseaux entrepreneuriaux. J'ai participé à 20 événements publics qu'elle a organisés jusqu'en mars 2020, seule ou en association avec des partenaires comme l'association de promotion d'Ethereum en France (appelée Asseth puis Ethereum France à partir de décembre 2019)²². Ces événements appelés « meetups » (à partir du nom

20 Une majorité de ces entretiens ont été conduits avec Liliana Doganova et les étudiants Lucas Colson, Hugo Mougard, Paul Pihouhé et Lena Poirier, étudiants à l'École des Mines de Paris.

21 Les acteurs « institutionnels » interviewés étaient : le responsable de l'innovation à la bourse de Singapour, des cadres d'une société de production d'électricité, un chercheur d'une grande société de développement informatique, un cadre d'une société de conseil, les responsables d'un incubateur de startups soutenu par l'État, l'employé d'un consortium blockchain, les responsables d'une institution de régulation nationale.

22 À partir de ce moment-là et avec la pandémie de Covid, les événements de ConsenSys sont devenus plus rares, puis n'ont plus été maintenus avec la fermeture du bureau de Paris. Certains événements, plus rares, et ligne et à visée très directement promotionnelle, ont été assurés par des employés de bureau principalement aux États-Unis et en Asie.

Introduction générale

de la plateforme Web meetup.com via laquelle les événements été publicisés) regroupaient l' « écosystème » parisien, essentiellement constitué d'entrepreneurs et de curieux cherchant à se documenter sur les actualités d'Ethereum et les produits proposés par ConsenSys, et parfois de représentants de l'État et d'experts employés par des institutions publiques ou privées. Ces meetups ont constitué le fil conducteur de mon enquête. Ils m'ont servi de point focal pour analyser le développement d'Ethereum de manière historiquement et spatialement située, à partir de l'activité de ConsenSys.

Le suivi de l'activité de ConsenSys a déplacé ma préoccupation initiale pour la dissonance entre (politique des) cryptomonnaies et (celle de la) blockchain vers une distinction empirique entre types de réseaux économiques imaginés dans le développement et l'utilisation d'Ethereum. À l'image de sa position centrale dans les relations entre entrepreneurs à Singapour, ConsenSys participait activement à fédérer un « écosystème » à Paris, composé d'acteurs participant à deux types d'utilisations d'Ethereum. Les acteurs distinguaient en effet les utilisations « B2C » (*Business to Customer*) et « B2B » (*Business to Business*). L'utilisation B2C était principalement celle des startups²³ qui faisaient d'Ethereum une « plateforme de développement d'applications décentralisées », selon la formulation de son fondateur Vitalik Buterin (Buterin 2014a). L'utilisation « B2B » était au contraire celle d'entreprises et d'institutions qui cherchaient à faire de la blockchain une solution pour rendre leurs échanges plus efficaces, sûrs ou transparents (à l'image de la banque centrale de Singapour). ConsenSys était présent sur les deux fronts et les articulait, sans les opposer, au travers de deux types d'activités. D'une part, ConsenSys participait au développement de l'utilisation B2C en jouant un rôle d'incubateur et de fonds d'investissement dans des startups amenées soit à proposer des services commerciaux, sinon des logiciels *open source* destinés à équiper d'autres startups. D'autre part, ConsenSys vendait son expertise technologique et entrepreneuriale aux grandes entreprises et institutions via des prestations de conseil. Ce faisant, ConsenSys était un opérateur de transfert technologique et entrepreneurial de l'utilisation B2C à l'utilisation B2B.

23 Y compris au sein d'Orange, le cas du vote était développé par une startup en « intrapreneuriat ».

Une dynamique d'innovation distribuée en co-construction

Ces deux types de réseaux économiques s'imaginaient et se concevaient ensemble. J'ai étendu mon enquête à une ethnographie multi-sites, multipliant les points de vue pour prendre la mesure des connexions entre ces deux dynamiques d'innovation sans les réduire à une opposition donnée à l'avance, soit entre logiciel blockchain et utilisation B2B d'une part, et infrastructure publique et applications B2C d'autre part, sinon entre institutions d'une part, et startups d'autre part. En complément des meetups, j'ai participé aux Assemblées Générales de l'association Ethereum France et à l'événement majeur qu'elle organisait (*Ethereum Community Conference*), à des conférences technologiques publiques prenant Ethereum comme un des objets centraux (*Peer to Peer Festival*) ou dans lesquelles des entrepreneurs présentaient leurs utilisations de la blockchain et d'Ethereum (par ex. VivaTech), mais aussi privées (par ex. d'un séminaire organisé par IBM), ainsi qu'à des réunions régulières d'un groupe d'intérêts des entreprises du secteur financier, et les prises de paroles d'un député français, tous relayant l'engouement pour la blockchain de cercles industriels et de recherche jusqu'à l'Assemblée Nationale. J'ai également participé, en début d'enquête, à différents événements de la communauté Bitcoin en France pour comprendre la signification de l'héritage revendiqué par les concepteurs d'Ethereum. Enfin, j'ai rencontré des acteurs participant à la construction d'un projet appelé NXT, semblable à Ethereum à certains égards, ainsi que des représentants d'entreprises utilisant des solutions logicielles alternatives à Ethereum. Tous ces matériaux n'ont pas été directement mobilisés dans cette thèse ; ils sont résumés en Annexe 1. Ces observations « en présentiel » ont été complétées par des observations d'arènes de discussion en ligne et par des entretiens avec différents acteurs rencontrés hors ligne.

Cette démarche vise à analyser une dynamique distribuée entre participants à la « co-production » d'artefacts techniques et de formes économiques et organisationnelles. Analytiquement et à la suite de travaux en *Science & Technology Studies*, elle se distingue notamment de travaux qui voient une logique interne et autonome dans le développement des techniques. Parmi ces travaux, différents auteurs ont cherché des mécanismes ou des lois qui seraient intrinsèques à l'objet technique lui-même, indépendamment du monde qui

Introduction générale

le maintient en existence, de manière à construire une « science des techniques » : les techniques se perfectionneraient, à la manière d'organismes biologiques, en rétroaction à leur environnement (Lafitte 1932), ou encore, les objets techniques auraient une cohérence propre à des « lignées phylogénétiques » dont la « concrétisation » serait inscrite dans leurs « êtres » depuis leur « genèse » (Simondon 1958). Au contraire de ces approches qui distinguent différentes formes de rationalités (technique, économique, politique), d'autres auteurs ont vu le développement technologie comme un système autonome, colonisant le monde social en exerçant une forme de domination critiquable car réduisant la vie sociale à une rationalité instrumentale propre au développement technique. L'appareil industriel de production et de distribution est par exemple décrit, dans son ensemble, comme « totalitaire » car déterminant les attitudes, aptitudes, aspirations et les besoins individuels selon les besoins sociaux, définis selon des formes de contrôle et de cohésion sociale toujours plus efficaces et agréables (Marcuse 1968).

Mais encore, cette démarche visait à rendre compte des convergences, transferts, échanges entre différents groupes d'acteurs qui, pris individuellement, liaient à leur manière effets politiques et développements technologiques. Nous avons par exemple vu que pour le dirigeant de JP Morgan, Bitcoin allait avec un ensemble de pratiques répréhensibles alors que la blockchain allait avec des relations entre firmes plus efficaces. Symétriquement, les promoteurs de Bitcoin niaient l'existence d'une technologie blockchain qu'ils réduisaient à une « technologie Bitcoin » qui avait pour fonction de rendre la monnaie « acéphale » (Favier & Takkal Bataille 2018). Mais plus généralement, ils se retrouvaient sur l'assimilation de formes institutionnelles à des réseaux informationnels, comme l'indiquent les deux cas en tête de cette introduction. Leur manière d'agir sur le monde *via* la technique en évitant les points de passages obligés dans des réseaux fait converger une préoccupation d'ingénieur à la fois technique, sociale, politique et économique : les systèmes d'informations ne devaient pas comporter de défaillance. Vue comme un réseau informatique, toute défaillance technique de la monnaie signifiait défaillance économique et financière, et vice-versa ; toute défaillance technique du processus démocratique vu comme réseau signifiait défaillance démocratique, et vice-versa.

3. Espaces transactionnels sans hétéronomie

Ces différents réseaux économiques imaginés étaient peuplés d'individus ou d'entreprises qui échangeaient et s'associaient souverainement. Ces entités étaient des portefeuilles ou « *wallets* » capables de contracter avec d'autres selon leur seul calcul d'intérêt, protégées de toute forme d'« intervention ». Cette protection signifiait absence de prise du reste du monde. Dans le cas des utilisations B2B comme B2C, la toute puissance de la contractualisation exigeait absence d'hétéronomie, c'est-à-dire absence de norme qui serait venue peser sur la capacité de chacun à agir selon son propre intérêt. En un mot, rendre les entités souveraines passait par la construction d'un espace spécifique, autonome, qui produisît les conditions d'échanges et d'associations imaginées pour ces réseaux économiques : un espace qui ne pouvait être gouverné par personne, mais qui liait les entités par les engagements qu'elles avaient formulés au travers de leurs portefeuilles.

Face à un monde incertain qui laisse la place aux « interventions » humaines, ces espaces opposaient l'absence de norme, sinon celles issues de la contractualisation volontaire. Ces espaces pensés pour éviter toute hétéronomie supposaient en pratique une norme collective qui relevait de la vérité plutôt que de la justice. Elle consistait à voir les échanges et associations totalisés dans cet espace comme des faits en raison de la manière dont les relations étaient inscrites. Pour devenir des faits, les relations avaient une condition de forme : être formulées dans un langage calculable par le réseau lui-même. Cette section met en perspective les deux types de réseaux économiques présentés à la section précédente. Dans les deux cas, ces réseaux étaient imaginés comme espaces articulant l'autonomie individuelle au tout par des conditions de formes propres aux relations elles-mêmes.

« Transaction » était cette condition de forme en langage vernaculaire. Elle était utilisée comme terme technique (au sens d'opération informatique) aussi bien que comme terme fonctionnel (la relation d'échange ou d'association formée par des acteurs peuplant ces espaces) par tous les acteurs impliqués dans le développement des cryptomonnaies et de la blockchain. Elle plaçait au niveau d'opérations l'assimilation entre formes institutionnelles et réseaux informationnels problématisés ; elle était imaginée pour se passer, par

Introduction générale

construction, des points de passages obligés des réseaux informationnels problématisés (par ex. la monnaie, le vote).

Cette notion était héritée des vocabulaires de l'économie et de la comptabilité, mais aussi de la science informatique et des systèmes d'information. Le premier héritage apparaissait le plus immédiatement dans la formulation des usages : les réseaux économiques B2B et B2C étaient des espaces où on transigeait. Ces espaces, pensés en termes économiques, appelaient un deuxième héritage pour advenir matériellement. L'informatique donnait à « transaction » le sens d'une bribe d'informations qui pouvait instantanément et librement circuler pour être reconnue de toutes les entités de l'espace tout en étant durable et à la seule main d'individus se reconnaissant mutuellement comme souverains, et ainsi être totalisée en « fait ».

Réseaux économiques conçus comme espaces transactionnels

Les réseaux économiques étaient imaginés comme des espaces *ad hoc* peuplés d'acteurs économiques qui formaient des transactions. La littérature comme les acteurs distinguaient ces espaces en fonction de leur degré d' « ouverture ». On dit les réseaux B2C « blockchains publiques » ou « ouvertes » car tout individu est en capacité (matérielle, légale) d'entrer dans cet espace, c'est-à-dire former des transactions avec les autres participants. Ces derniers sont opposés aux réseaux B2B dits « blockchains privées » ou « fermées » dans lesquels seuls les acteurs autorisés par les « propriétaires » de l'infrastructure peuvent transiger.

Les acteurs des réseaux B2B étaient souvent à la fois administrateurs et utilisateurs. Ils organisaient leur propre sélection ; personne, en dehors de ces derniers, ne pouvait accéder à ces espaces, c'est-à-dire lire les transactions ou former des transactions avec ces derniers. Dans le même temps, ces espaces étaient conçus pour qu'aucun des acteurs les peuplant puisse devenir un point de passage obligé de la formation de transactions, libellés en termes comptables (en argent, ou objets économiques ou financiers échangés par les acteurs peuplant ces espaces). Ils problématisaient des réseaux reliant différents participants,

Introduction générale

entreprises ou administrations, certains étant susceptibles de jouer un rôle central dans la formation de transactions. Cette prééminence était vue comme un risque de contrôle pesant sur la stabilité, la sécurité, l'efficacité du système. En réponse, ces espaces impliquaient les participants dans la définition et l'application collective de règles selon lesquelles les transactions étaient formées. Ces infrastructures étaient des registres à la disposition de leurs membres et indépendants de chacun ; à la manière d'intranets, ces réseaux faisaient de la blockchain une technologie de formation de transactions spécifiques à des coalitions d'entreprises ou d'administrations.

Au contraire, les utilisations B2C existaient sur une infrastructure accessible *via* Internet. Sans autre précision et couramment, « Ethereum » désigne cette infrastructure. L'espace des points de passage obligés problématisés était, dans ce cas, le Web dans sa totalité (dit « Web 2.0 »). Cette infrastructure ne sélectionnait ni ses utilisateurs ni ses administrateurs par leur identité légale ; elle était pensée comme « ouverte » à tout Internaute. Les transactions y étaient la plupart du temps formulées en « jetons ». Ces jetons étaient formés par des algorithmes dits « *smart contracts* », développés par des entreprises (« *Businesses* », le « B » dans B2C). Chaque jeton était imaginé comme tissu de relations économiques, financières, démocratiques ou réputationnelles entre des utilisateurs (« *Customers* »). Ces jetons ont participé à la popularisation des cryptomonnaies dont les cours, les profits et les promesses technologiques, financières et politiques explosaient entre 2016 et 2018. Ils catalysaient l'engouement de l'époque pour le dépassement des « applications monétaires » de la blockchain associées, notamment, à Bitcoin. Ces différents jetons se comptaient en dizaines de milliers ; la diversité des réseaux de substitution imaginés avec ces jetons était impressionnante²⁴. Certains jetons permettaient d'utiliser des applications Web qui ressemblaient en tout points à des sites de e-commerce traditionnels, d'autres servent de droit de vote pour des scrutins associant des Internautes,

24 En 2017 et 2018, Ethereum devenait populaire avec la multiplication de jetons dits « utilitaires » et d' « *Initial Coin Offering* » (ICO). D'autres types de jetons étaient également imaginés, comme des jetons de « gouvernance » imaginés comme des droits de votes permettant à des groupes d'individus de prendre des décisions dans des « *Decentralized Autonomous Organizations* » (DAO) ou « *Decentralized Autonomous Corporations* » (DAC). À la même période émergeaient d'autres types de jetons appelés *stablecoins*, mais aussi des *security tokens*, ou encore des *collectibles*, devenus populaires en 2021 sous l'appellation « *Non Fungible Tokens* » (NFT).

Introduction générale

certaines représentaient des titres de propriété d'œuvres numériques ou de sociétés anonymes. L'espace constitué par ces jetons était imaginé comme un nouveau Web (« Web 3.0 »²⁵) en général et plus tardivement au sein de ce nouveau Web, comme une « finance décentralisée »²⁶.

Hétérotopies numériques en train de se faire

L'objectif de faire d'épargner ces espaces de toute forme d'hétéronomie passait par une séparation relative du reste de l'espace public ; ils étaient conçus en opposition avec d'autres espaces, sans en être tout à fait isolés. La notion d'hétérotopie (Foucault 2004c) est utile pour les penser. Michel Foucault distingue l'utopie, emplacement sans lieu réel, de l'hétérotopie, « contre-emplacement » qui est une utopie effectivement réalisée. L'hétérotopie est localisable, elle parle d'une culture donnée comme un « miroir » ; elle est un lieu de contestation de l'espace dans lequel nous vivons : le jardin, la bibliothèque, le cimetière, la maison close ou le musée sont tous des espaces à la fois délimités et ouverts sur l'ensemble d'une société à laquelle ils opposent des normes relationnelles. Dans ce texte de 1967, Foucault indique, de manière troublante par rapport à l'objet de ce travail : « on sait l'importance des problèmes de l'emplacement dans la technique contemporaine : stockage de l'information ou des résultats partiels d'un calcul dans la mémoire d'une machine » (ibid : 13). Au problème de l'emplacement des données sur lesquels il est possible d'intervenir, les concepteurs des réseaux B2C comme B2B répondent avec des hétérotopies numériques en train de se faire : ils concevaient des espaces délimités qui communiquent avec le reste du monde tout en s'en démarquant par des règles spécifiques, culturellement situées.

25 Web3 est une expression apparue sous la plume du cofondateur d'Ethereum Gavin Wood en 2014 pour désigner un projet de refondation du Web. Après le passage du Web 1.0 au Web 2.0 marqué par de nouvelles formes de participation en ligne, le Web 3.0 serait un espace d'interactions numériques libres de l'incursion des gouvernements ou de grandes organisations.

26 La finance décentralisée désigne des services financiers accessibles *via* Internet indépendamment de toutes les institutions financières traditionnelles comme les banques (centrales et commerciales), les assureurs, les gestionnaires d'actifs ou les bourses d'échanges. Web3 et finance décentralisée ont en commun de projeter un monde débarrassé d'acteurs qualifiés d' « intermédiaires » ou « points de passages obligés » de certains réseaux.

Introduction générale

Des traits culturels étaient lisibles dans chacune des catégories d'espaces B2B et B2C. Les réseaux B2B étaient les « miroirs » d'une organisation des échanges commerciaux et monétaires à l'échelle de la planète qui était retranscrite dans les comptabilités de grandes entreprises et administrations. Les réseaux B2B prolongeaient cette structuration comptable des échanges en les rassemblant dans un même espace. Plutôt qu'une comptabilité éclatée entre différents acteurs qui n'avaient chacun qu'une vue partielle des échanges passés avec leurs partenaires, faisant de chacune d'elle un « intermédiaire », les réseaux B2B rassemblaient dans un même espace l'image comptable des échanges d'une filière industrielle ou financière. Ils donnaient ainsi une vue instantanée et partagée par tous les acteurs de l'état des échanges. Les réseaux B2C étaient quant à eux les « miroirs » d'une politique des échanges sur Internet à la main de grandes entreprises du numérique, et plus généralement d'une utilisation commerciale et asymétrique des réseaux par des acteurs influents. Ces réseaux opposaient une normativité des échanges inspirée des balbutiements d'Internet promouvant l'anonymat des relations sur Internet, la nature pair-à-pair des échanges sur le Web (à l'image du fonctionnement de l'infrastructure d'Internet, distribuée, par opposition aux télécommunications par « circuits ») qui devaient être protégées de toute forme d'intervention des États et d'entreprises. Ces impératifs ont éloquemment été formulés en termes d' « espace » par John Perry Barlow dans sa fameuse « Déclaration d'Indépendance du Cyberespace » (Barlow 1996).

En dépit de ces différences, ces deux types de réseaux projettent un monde peuplé d'acteurs indépendants en règle générale, sinon liés aux autres par des relations purement bilatérales et « horizontales » ne dépendant d'aucun garant, juge ou arbitre. Dans le cas des réseaux B2B, ces relations étaient convenues entre partenaires commerciaux ; la comptabilité formait les relations en même temps qu'elle en attestait. Dans le cas des réseaux B2C, ces relations étaient formées dans les termes d'entreprises (« *Businesses* ») qui développaient des services fonctionnant par jetons dont les transferts entre utilisateurs (« *Customers* ») étaient indépendants des premiers. Les positions d'acteurs institutionnels comme Orange ou la Société Générale dans les réseaux B2C témoignent de la porosité entre ces deux manières de concevoir la gouvernance par les réseaux commerciaux et financiers. Ces entreprises

Introduction générale

n'étaient pourtant pas attendues dans l'espace des utilisations B2C d'Ethereum *a priori*, et plus généralement de ce que les acteurs appellent la « sphère crypto » (*crypto-sphere*) qui inclut Ethereum, Bitcoin et les autres cryptomonnaies. Elles proposaient des services B2C qui prenaient Ethereum pour une infrastructure neutre en donnant aux transactions les valeurs de « transparence », d' « ouverture » ou encore de « sécurité » par conception (« *by design* »), aussi bien dans le cas du vote pour Orange que dans celui des transferts d'actifs financiers dans le cas de la filiale SG Forge de la Société Générale.

Transactions comme opérations de production d'un « monde commun »

Caractériser un espace social (délimité par rapport au reste du monde) par la forme des négociations entre individus est au cœur de l'analyse d'une sociologie dite « de la transaction » ou « sociologie transactionnelle »²⁷. Cette tradition prend les « transactions sociales » pour objets d'enquête, selon une « posture méthodologique qui oriente le regard du sociologue vers les tensions, les conflits, les négociations et les compromis, formels ou informels » (Blanc 2009 : 25) : la transaction est pour eux un « projecteur qui permet de voir certaines choses quand il est allumé, alors qu'elles échappent au regard quand il est éteint » (Blanc 2009 : 30). Cette approche permettrait de voir « l'innovation sociale » dans un « espace de transactions », au sein d'une famille aussi bien que d'une ville, comme lutte avec les « normes en vigueur » et en « marge des institutions ». Elle cherche par là à se distinguer de la transaction mobilisée par la sociologie des organisations qui la comprend selon eux comme un concept économique utile pour analyser les relations entre, d'une part, l'organisation vue comme « un isolat structuré et jouissant d'une indépendance vis-à-vis de son contexte », et, d'autre part, le reste du monde (Blanc 2009 : 31-4).

Pour ces sociologues comme pour les concepteurs d'Ethereum, la transaction est « innovation ». Pour les premiers, la transaction est un objet d'analyse, et pour les seconds, un objet d'ingénierie. La transaction est le résultat de négociations qui s'affranchissent des

²⁷ Cette approche est née à Louvain dans les années 1960 et s'est développée comme alternative au structuralisme de Pierre Bourdieu et de Louis Althusser et aux sociologies des mouvements sociaux d'Alain Touraine et des organisations de Michel Crozier (Blanc 2009 : 26).

Introduction générale

règles du monde, des « normes en vigueur » pour les premiers, des contraintes pesant sur la manière de former les échanges et les associations dans le monde contemporain pour les seconds. Mais encore, la préférence de ces sociologues pour le mot « transaction » à « interaction » indique que les individus et le monde dans lequel ils vivent sont transformés par ces négociations. Ils indiquent que le concept de « transaction » contourne le problème de la connaissance du monde et de ses normes, qu'elles soient sociales, juridiques ou naturelles. De manière similaire et dans leur perspective de transformation de ce monde, les concepteurs d'Ethereum voient les transactions comme une manière de former des relations en évitant les garants, références, institutions ou « intermédiaires » représentant des normes dont ils cherchent à s'affranchir.

En effet, pour ces sociologues, « transaction » articule le rapport individuel à un « monde commun » dans les termes au philosophe pragmatiste John Dewey duquel ils retiennent une pensée du rapport entre « organisme » et « environnement ». Pour souligner que l'interaction ne transforme pas seulement la relation entre deux entités mais aussi les entités elles-mêmes, Dewey préfère lui-même la notion de « transaction » (Foucart 2013 : 75) par laquelle il propose de ne comprendre une relation qu'en situation (Steiner 2010 : 204). Pour Dewey, la transaction est un concept essentiel pour élaborer toute théorie de la connaissance qui articule « choses-connues » et « hommes-connaissant »²⁸. Les sociologues de la transaction voient chez Dewey une inspiration épistémologique pour penser la résolution des conflits en société : en attribuant un nom à ces situations problématiques, les acteurs engagent une transaction entre le « nommant » et le « nommé ». Dans ces processus transactionnels, les acteurs créent un « monde commun » sans lequel la compréhension mutuelle est impossible (Foucart 2013 : 77-8). Ce monde commun est le résultat de l'expérience en situation comprise comme une « transaction continue » qui devient l'objet d'étude sociologique plutôt que le sujet individuel. Ainsi, ils incluent les changements dont les acteurs sont eux-mêmes les objets dans le processus d'expérience collective (Foucart 2013 : 79-80).

28 Cette intuition s'appuie sur une lecture des derniers développements de la science physique au début du XX^e siècle, qui ne suppose pas de différence radicale entre observé, observant et observateur (Dewey & Bentley 1946 : 505).

Espaces et conditions de forme sur les transactions

Symétriquement, ces « mondes communs » imposaient des conditions de forme à ces « actions au travers » des espaces transactionnels, de type B2B comme B2C. Ces normes sur les transactions étaient la contrepartie pour maintenir ces espaces « autres » selon Foucault, protégés du reste du monde. Le cas des réseaux B2B était de ce point de vue plus immédiat : les transactions devaient être formulées selon les règles comptables convenues par des partenaires d'une même filière industrielle ou commerciale selon des règles convenues collectivement et en avance. Dans les réseaux B2C, les transactions en jetons étaient formulées selon toute l'amplitude que permet la programmation informatique par différentes entreprises, pouvant signifier des titres financiers avec la Société Générale jusqu'à l'expression de votes avec le cas d'Orange. Mais quelles que soient ces significations, les transactions rémunéraient les acteurs qui maintenaient cet espace séparé du reste du monde. Cette rémunération passait par la cryptomonnaie « ether », matière première d'exécution des « *smart contracts* ».

Il est intéressant de remarquer que la notion d' « ether » apparaît chez Dewey dans sa discussion de l'action en lien avec l'environnement. L'importance que le philosophe accorde à l'environnement vient de sa lecture des développements de la science physique qui lui est contemporaine. Au début du XX^e siècle, la physique ne suppose plus de différence radicale entre observé, observant et observateur (Dewey & Bentley 1946 : 505), un changement de paradigme qui donne naissance à la mécanique quantique. Ce nouveau regard des physiciens sur la matière fait suite aux travaux de James Clerk Maxwell à la fin du XIX^e siècle portant sur une nouvelle théorie électromagnétique. Cette théorie repose sur une remise en question de la description physique dans le langage de la mécanique newtonienne en termes de forces, d'action et de réaction, qui suppose de considérer des parties isolées de la matière (Dewey & Bentley 1946 : 508). Une telle théorie générale de la physique en termes d' « interactions » oublie certains éléments du monde physique, mais en appelle également de nouveaux, réels ou instrumentaux, pour son maintien. L'ether est un artefact intellectuel de ce type : pour que la théorie électromagnétique puisse être conçue dans les termes de la théorie newtonienne, l'existence d'un matériau nommé ether a été

Introduction générale

postulé (mais jamais démontré expérimentalement) par les physiciens.

Or, la cryptomonnaie ether sert précisément d'artefact (informatique et non théorique) qui fait tenir l'espace transactionnel des utilisations B2C imaginé comme monde de relations pair-à-pair entre individus souverains. Ces relations n'étaient pas imaginées comme de simples interactions dans le vide ; elles devaient être inscrites dans un espace, faites transactions, par cet artefact. Il est intéressant de remarquer que le nom Ethereum est inspiré, au moins poétiquement, de l'artefact en physique. Interrogé sur l'origine du nom « Ethereum » dès les premiers mois suivants la publication de ce qui était alors un projet embryonnaire, l'inventeur d'Ethereum Vitalik Buterin expliquait qu'il avait choisi « Ethereum » dans une liste Wikipedia d'éléments utilisés en science-fiction, un de ses genres littéraires favoris. « Ethereum » lui aurait convenu esthétiquement, mais aussi car « *it had the word 'ether', referring to the hypothetical invisible medium that permeates the universe and allows light to travel* » (Buterin 2014b).

La notion d'« ether » apparaît également dans les réseaux d'Internet avec Ethernet, standard technologique qui a joué un rôle important dans son développement. Ces réseaux sont également conçus pour être « horizontaux » et « ouverts »²⁹, et ils conditionnent les actions possibles entre les entités qui le peuplent par leurs formes. Quelques décennies avant Ethereum, le concept d'« ether » était utilisé par l'inventeur d'Ethernet Robert Metcalfe³⁰. Au milieu des années 1970, son employeur au centre de recherche de Xerox lui demandait de construire un réseau qui n'eût pas besoin d'être reconfiguré lors de l'installation ou de la désinstallation de machines, ordinateurs et imprimantes ; autrement dit, qui permettrait à des entités de communiquer en faisant l'économie d'interventions du reste du monde. Metcalfe imaginait alors un réseau conçu comme un espace ouvert à toutes les machines, évitant la « configuration » systématique d'un technicien. L'environnement au sens de Dewey devait limiter les termes de la transaction entre imprimantes mais permettre que les machines se comprennent. Le mot Ethernet apparaît pour la première fois dans le mémo que Metcalfe remit à son employeur en 1976, en référence à « l'idée d'utiliser un câble

29 Bien que ce ne soit pas le cas à ses débuts : voir Abbate (1999) et Flichy (2001).

30 Plus tard, le nom de Metcalfe est associé à Ethernet ; il est par exemple devenu responsable de la section « *From The Ether* » de la revue spécialisée en systèmes d'information *InfoWorld*.

Introduction générale

coaxial comme ether » (Kirsner 1998). Cette métaphore permet à Metcalfe d'expliquer et de représenter picturalement son invention comme un espace, comme sur la Figure 1 produite par Metcalfe pour présenter Ethernet en juin 1976 à la *National Computer Conference*.

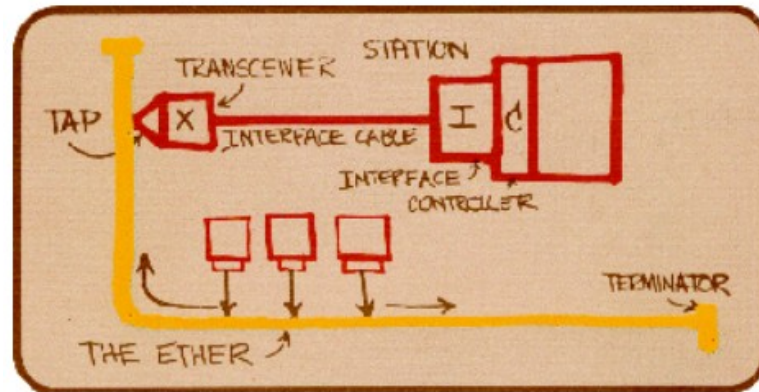


Figure 1 : Diagramme dessiné par Robert Metcalfe pour une présentation d'Ethernet en juin 1976 à la *National Computer Conference* (Metcalfe 2020)

4. Sur la piste de l'ingénierie des transactions

Le trait important de ces espaces était d'inscrire des relations en « faits » indépendamment des significations formulées par les utilisateurs (comme un vote ou un transfert d'argent). En pratique, cette décorrélation entre forme scripturale et significations était au cœur de l'ingénierie politique de ces infrastructures. Elle consistait à neutraliser les possibilités matérielles d'intervention et de recours sur les transactions. Dans le même temps, elle prescrivait les formes possibles que pouvaient prendre les transactions, donc cadrant les significations, au travers de différents dispositifs qui étaient nécessaires pour traduire successivement la formulation d'une relation par un utilisateur « portefeuille » en inscription par les inscripteurs.

Changer la réalité en neutralisant les inscripteurs des relations sociales

La problématisation des réseaux informationnels visait la fragilité des formes scripturales

Introduction générale

des relations. Par exemple dans le cas d'un vote, le dépouillement d'un scrutin est une suite d'opérations scripturales : noter le nombre de voix obtenues par des candidats dans chaque bureau, mais aussi le nombre d'enveloppes, croiser les chiffres des bureaux de votes, publier les résultats. Ces inscriptions en chaîne forment, ensemble, une élection. Voter est une action individuelle qui prend son sens dans une procédure collective qui existe matériellement comme une série d'inscriptions, et dont le résultat est valable pour tous les membres d'un corps politique. L'action collective se comprend comme produit d'actions individuelles calculées par un réseau scriptural. De la même manière : demander un virement bancaire, vérifier que l'argent sur le compte émetteur est disponible, effectuer le transfert de fonds sont des opérations d'inscription. Là aussi, exécuter un virement est une action individuelle qui prend son sens dans une procédure collective qui existe matériellement comme une série d'inscriptions, et dont le résultat est valable pour tous les acteurs d'un système bancaire.

Dans ces deux cas, des inscripteurs donnent un sens collectif à des actions individuelles : ce sont eux qui produisent le « monde commun » dans lequel insérer un bout de papier dans une urne ou cliquer sur une application bancaire ont des significations spécifiques. Mais, selon les concepteurs d'Ethereum, ce type de processus scriptural en série rendait les interactions fragiles en raison du pouvoir d'intervention d'inscripteurs particuliers à différentes étapes, notamment capables de contrôler l'identité pour autoriser ou non une interaction (par exemple, ouverture l'ouverture d'un compte en banque ou l'accès à un scrutin), modifier l'inscription d'une interaction passée (par exemple, modifier un vote ou le solde d'un compte), ou en faisant circuler les inscriptions d'interactions numériques passées (par exemple, divulguer les votes de certains électeurs).

L'écriture participe à instaurer une réalité dont la signification est spécifique à ses formes et à son contenu. « L'apport de Smith est important en ce qu'il souligne le rôle des documents et des technologies d'écriture au sens large dans l'instauration de versions spécifiques de la réalité », souligne Jérôme Denis dans un chapitre intitulé *La construction scripturale de la réalité* (Denis 2018 : 83-97). Dès les années 1970, la sociologue Dorothy Smith place les formes scripturales au cœur de son analyse politique des organisations (Smith 1974) : les

Introduction générale

« *accounts* », au sens de comptes-rendus que nous produisons pour constituer nos actions quotidiennes en phénomènes intelligibles, sont de nature scripturale. Le regard que Smith porte sur les organisations en sociologue résonne avec celui que les concepteurs d'Ethereum portent sur les réseaux informationnels qu'ils cherchent à remplacer. La sociologue montre que le social est composé d'écrits, des faits scripturaux eux-mêmes résultats de pratiques organisées par des organisations qui les orientent. Les concepteurs d'Ethereum ingénieraient des réseaux permettant aux utilisateurs d'instaurer des réalités qui « rendent compte » de leurs relations numériques différemment : sans qu'un « intermédiaire » ou qu'une « autorité » ait la capacité matérielle d'intervenir.

Ce travail d'ingénierie consistait à articuler formulation des relations et leur inscription en rendant les deux actions indépendantes l'une de l'autre. Ces inscripteurs, connus comme « *miners* », parfois « *stakers* », accumulaient matériellement les relations formulées par les utilisateurs, dans des « blocs », mis à la « chaîne ». Imaginons les aveugles : ils reconnaissaient la conformité de forme des transactions au toucher, sans voir leurs significations. Ils communiquaient entre eux à l'oral, pour s'assurer que chacun ait bien toutes les transactions inscrites de son côté. Ainsi, aucun acteur (humain ou non-humain) ne pouvait être en capacité d'intervenir discrétionnairement sur les relations numériques. L'inscripteur aveugle ne pouvait pas « défaillir » ou profiter de sa position, simplement exécuter l'ordre d'inscription en fonction d'une incitation monétaire. Il devait authentifier une interaction sans porter le moindre « intérêt » à sa signification. L'activité d'inscription était conçue comme une activité purement économique, dont les gains et pertes pouvaient être calculés à l'avance par ces inscripteurs quelle que soit la relation. Elle portait une rationalité scripturale : la nécessaire immuabilité des inscriptions était le résultat d'une rupture entre la forme graphique d'une interaction et sa signification (qui ne devait être lisible que par les parties prenantes de l'interaction inscrite).

Alignement à partir de l'inscription matérielle

En corollaire des conclusions de Smith, changer la manière d'inscrire les relations numériques transforme également leurs significations. Pour convenir aux conditions de

Introduction générale

forme des inscripteurs, les transactions étaient modelées par une série de dispositifs pour que les transactions soient vues comme une relation par l'utilisateur et comme un gain monétaire par l'inscripteur. Les utilisateurs devaient être identifiés, généralement sous la forme de portefeuilles (*wallets*), l'inscripteur avait un logiciel « client ». Entre les deux, une chaîne d'acteurs (algorithmes, nœuds de réseau, protocoles, cryptographie, contrats intelligents ou « *smart contracts* » etc.) transformaient en cascade les relations pour qu'elles soient traduites (inscrites) en « transactions ». Ces différents objets techniques n'étaient pas seulement des « intermédiaires », c'est-à-dire des moyens pour atteindre une fin, mais des « médiateurs », à la fois fin et moyens, qui autorisaient, obligeaient, interdisaient des formes d'action (Latour 2007 : 44).

Ainsi, changer la manière d'inscrire supposait un vaste travail de ré-ingénierie des relations numériques. Ce travail était réinvention d'un « alignement » jusque-là provisoirement stabilisé entre acteurs en présence (Latour 1990 : 129) : utilisateurs, fournisseurs de services numériques, mais aussi inscripteurs et tous les médiateurs « techniques » impliqués dans les traductions successives qui faisaient qu'une relation devienne « transaction ». Ces maillons « techniques » de l'alignement étaient des réceptacles de projets, de visions, de formes politiques et sociales pensées dans leur conception ; elles étaient aussi objets de négociations, productrices de formes politiques et sociales contingentes à leur développement et à leur circulation (Latour 1992 : 160-3).

La notion de « technologie » dans « technologie blockchain » signale la systématisation de cet alignement, de l'identification des utilisateurs comme portefeuilles à la manière d'inscrire les relations par un réseau d'inscripteurs aveugles. L'ensemble peut se comprendre comme un « programme d'inscriptions », à partir des concepts « programme d'actions » et « inscription ». Les concepteurs définissent un « programme d'actions » visant à empêcher un « anti-programme » qui est postulé : la possibilité de défaillance volontaire ou involontaire de l'intégrité des inscriptions en bases de données chez les fournisseurs de services du Web (qu'elle soit fraude, panne, intervention légitime ou illégitime) dans le cas du réseau B2C, ou chez un des partenaires dans le cas des réseaux B2B.

Introduction générale

En retour, cette nouvelle manière d'inscrire les relations changeait les entités mises en relations elles-mêmes. C'est ce que suggère la notion de « transaction » (cf. section précédente), mais aussi ce que nous apprennent les travaux de Jack Goody : la manière d'écrire change le contenu de ce qui est formulé. L'anthropologue montre en effet que les modes de raisonnements sont associés à la formulation du raisonnement³¹ (Goody 1979) : les formes écrites, à la différence de l'oralité, rendent le langage durable et produisent des formes de raisonnement qui leur sont propres. Goody a notamment développé cet argument en prenant le cas des listes et des tableaux. Ces artefacts graphiques engendrent des formes d'actions spécifiques : ils instaurent des raisonnements en termes de limitation, de simplification, de classification, d'opposition entre éléments écrits. L'écriture est une « technologie cognitive » qui participe à constituer le raisonnement. Dans la même veine, Elisabeth Eisenstein attribue à l'innovation scripturale qu'est l'imprimerie un rôle central dans le développement de nouvelles théories scientifiques : en transportant des comptes-rendus d'observations sur le bureau de savants, il devenait possible d'accumuler des énoncés dans un même espace, donc de douter ou de répondre à des conclusions produites ailleurs (Eisenstein 1991).

Ainsi, l'« immuabilité » caractéristique d'une activité d'écriture était ici radicalisée en objet d'ingénierie premier qui conduit à une ingénierie totale des relations, antidote nécessaire au contrôle d'intermédiaires sur les relations : l'immuabilité devait être absolue pour que les transactions constituent des faits. L'immuabilité résultait d'un agencement particulier des inscripteurs, dont l'« intérêt » devait être purement utilitariste, assimilé au résultat d'un calcul de pertes et de gains en monnaie. Ce faisant, l'impératif premier d'immuabilité supposait des hypothèses sur les entités peuplant les espaces.

Cette forme d'écriture particulière supposait de penser les échanges et les décisions sur le Web comme transactions. Les relations d'échanges et d'associations étaient formulées en langage informatique (interfaces Web et « smart contracts ») par les « *Businesses* » du réseau B2C, ou par les entreprises partenaires dans les réseaux B2B. Ces formulations

31 L'anthropologue montre que la raison, que nombre de ses pairs tendent à réifier et à situer dans les cerveaux, émerge et évolue avec les transformations des pratiques d'écritures.

Introduction générale

traduisaient des modèles d'affaires et des usages spécifiques, souvent directement inspirés de l'expérience des concepteurs eux-mêmes. Dans le même temps, ces formulations étaient équipées de standards informatiques et de pratiques de développement partagées que ces acteurs faisaient évoluer dans un processus de développement *open source* au sein d'une « communauté » de développeurs et d'un « écosystème » entrepreneurial. Ces deux ensembles rassemblaient, de manière distribuée et souvent en ligne, des contributeurs participant à l'élaboration de réseaux B2C et B2B. L'analyse de ces pratiques partagées permet de pointer non seulement les différences mais aussi les convergences dans les formes sociales imaginées malgré les différences d'acteurs impliqués dans la construction de ces réseaux économiques.

Précautions de langages

« Programme », « réseau », ou encore « intermédiaire » sont des concepts qui appartiennent à la fois au langage vernaculaire et au vocabulaire analytique de la sociologie de la traduction que je mobilise dans cette thèse pour rendre compte d'un travail d'ingénierie à la fois technique et social (Akrich 1989 ; Latour 1992 ; Akrich & Latour 1992). La notion de « programme d'action », par exemple, est utile pour rendre compte du projet des concepteurs et des formes qu'il prend en pratique, plutôt que comme simple outil descriptif : les acteurs ne revendiquent pas, littéralement, construire un « programme » qui transforme les manières d'inscrire en bases de données ; ils parlent plutôt d'une technologie et de réseaux qui sont autonomes et décentralisés permettant de bâtir un Web 3.0 ou une finance décentralisée. L'objectif de ce travail est d'intégrer la signification des concepts forgés par les acteurs à l'analyse pour comprendre les visions du monde engagées dans la conception technologique, et les relations que cette dernière fait advenir.

Cette précaution vise à éviter deux écueils. Le premier consisterait à chercher une correspondance entre un vocabulaire analytique et un langage vernaculaire qui semblent proches, au risque de tordre à la fois le sens du vocabulaire analytique et la richesse des matériaux d'enquête. Ce type d'attitude tendrait à faire de l'analyse une description bancale car restituée par des mots à la signification rendue ambiguë, sinon à transférer la charge

Introduction générale

politique des mots des acteurs au vocabulaire analytique, et vice-versa³². Le second écueil serait de ne pas interroger la signification des concepts mobilisés par les acteurs alors que ces derniers les chargent politiquement. Ce travail cherche à les approcher comme éléments d'enquête, c'est-à-dire à prendre cette charge comme une donnée : considérer les acteurs comme des théoriciens et praticiens du social qui s'équipent, notamment, d'un vocabulaire spécifique. Les concepteurs sont des analystes du social, une position qu'ils revendiquent en l'ingénierant dans des perspectives explicitement politiques. Il s'agit d'analyser leur travail comme une ingénierie sociale de second ordre (Muniesa 2019 : 198), et pour cela, de prendre leur vocabulaire comme éléments de cette ingénierie. Un des enjeux importants de ce travail est donc de soigner la distinction entre vocabulaire analytique et mots du terrain, une précaution qui dépasse le vocabulaire de la sociologie de la traduction.

5. Composition du manuscrit

Indications générales

Chaque chapitre suit l'approche développée dans cette Introduction. Chaque chapitre est constitué de deux sections. Elles traitent le problème posé en introduction de chaque chapitre en faisant varier les angles analytiques ou les matériaux empiriques. Sauf quand ils sont nommés avec leurs noms et prénoms, les protagonistes rencontrés lors d'épisodes d'enquêtes sont systématiquement anonymisés dans le manuscrit et simplement désignés avec un prénom.

Le Chapitre 4 s'appuie sur des résultats proposés dans les chapitres précédents. Les trois premiers chapitres sont plus indépendants. Toutefois, l'ordre proposé tient compte de différents éléments : introduction progressive d'entités (en particulier techniques), développement historique de l'objet, et progression de l'enquête.

Trois Annexes complètent le manuscrit.

³² Ce type de critique a été adressé à la sociologie de la traduction par des auteurs qui dénoncent une inspiration connexionniste aux conséquences politiques impensées (voir par exemple Mirowski 2017) ou posant d'emblée des limites à l'analyse (Quéré 1989).

Chapitre 1. Mystique du protocole : calculer sans connaître

J'analyse Ethereum dans les termes de la technologie de gouvernance en me concentrant sur la filiation technologique entre Bitcoin et Ethereum : de quelles qualités politiques prêtées à Bitcoin hérite Ethereum ? Une vaste littérature prête à la blockchain une qualité politique tirée de Bitcoin : des relations numériques se passant de confiance dans toute forme d'institution. Je me situe à la suite de travaux labellisés STS qui ont directement pris en charge la question de la gouvernance avec Bitcoin en proposant de l'analyser comme une théorie du contrôle inscrite dans le protocole du réseau.

La première section est consacrée à Bitcoin, vu comme un artefact qui a une politique (Winner 1980) imaginée. Dans un premier temps, j'analyse la problématisation de Bitcoin à partir de verbalisations de promoteurs (livres, prises de paroles publiques, entretien) que je prends comme moments de réflexivité. Ils donnent accès à la manière dont ils pensent la politique : des relations inter-individuelles formées par un système « autonome ». Dans un second temps, j'analyse l'autonomie de Bitcoin en suivant les traductions (Akrich et al. 2006) opérées par le protocole de consensus, agenceur des acteurs en présence. Elle met en évidence que la politique de Bitcoin tient à une opération de rupture épistémique : le réseau est « sécurisé » par le protocole dans la mesure où les relations des utilisateurs ne sont pas connues des participants du réseau qui ne voient que des objets d'investissement. Enfin, je montre que cette politique de sécurisation est conçue comme neutralisation de toute forme de pouvoir, quelle que soit la manière dont le pouvoir est imaginé. Cette analyse s'appuie sur le parcours du théoricien du pouvoir Steven Lukes (1974, 2004).

La deuxième section analyse Ethereum dans la filiation de Bitcoin. Premièrement et à partir d'un cas d'utilisation dit « d'usage » d'Ethereum, je montre le lien entre calcul par les « *smart contracts* » et inscriptions (traces d'exécution de ces algorithmes). Programmés par les utilisateurs d'Ethereum, ces algorithmes prennent la signification de contrats. Ils problématisent le Web et ses données. À leur circulation est opposé le contrôle sur les inscriptions des transactions. Deuxièmement, je montre qu'Ethereum prolonge l'innovation de Bitcoin. Je propose de comprendre le protocole de consensus comme un « mécanisme de

Introduction générale

pouvoir » au sens de Michel Foucault (2004a), pouvoir prenant le sens de « pouvoir inscrire ». Troisièmement, je précise la notion de sécurité héritée de Bitcoin. Elle porte désormais sur le calcul programmé par les utilisateurs, résultats d'une décentralisation « architecturale » et « politique ». J'articule cette sécurité à la notion proposée par Foucault dans son histoire de la gouvernementalité pour proposer de situer Ethereum dans une histoire des technologies de gouvernement par le calcul informatique.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Les cryptoactifs ont défrayé la chronique à la fin des années 2010. Leur statut juridique intriguait autant que leur fonctionnement. Pourtant, ils s'institutionnalisèrent sous la plume du gouvernement français, sur des plateformes Web permettant de les échanger (*exchanges*) et *via* des associations qui parlaient en leur nom : comment comprendre cette institutionnalisation ? Je puise dans les pistes de la sociologie de l'argent et d'une littérature à la croisée des STS et de la sociologie économique pour analyser le développement de cryptoactifs particuliers, les jetons. Ces objets créés (émis) avec Ethereum prenaient différentes significations. Elles informent sur l'ingénierie relationnelle imaginée par leurs concepteurs ainsi que sur l'expansion d'Ethereum à une période charnière de son histoire.

La première section analyse, dans une perspective pragmatiste (Muniesa 2011), le développement de jetons qui ont marqué l'histoire d'Ethereum : les jetons « utilitaires ». Ces objets étaient imaginés comme relations d'un Web « décentralisé » autour de plateformes qui seraient elles-mêmes autonomes et décentralisées. Premièrement, j'analyse la vie imaginée des jetons utilitaires. Je suis les associations qu'ils forment, jusqu'aux *exchanges*. D'autres jetons entrent alors en scène, témoins d'agencement marchand (Callon et al. 2013) plus complexes que de simples marchés bifaces. Deuxièmement, je montre que les jetons utilitaires sont aussi une technique de financement entrepreneurial très répandue. Je nuance le télescopage entre usage et financement (Zook et Grote 2020) en pointant la richesse de significations sur les deux cas retenus. La programmabilité des *smart contracts* permet de concevoir finement des opérations de capitalisation (Muniesa et al. 2017), parfois

Introduction générale

d'*assetization* (Birch & Muniesa 2020). Enfin, je prends différentes coupes de ce processus étendu de rencontres entre des entrepreneurs et des investisseurs pour souligner son caractère institutionnel, et par là proposer une explication alternative à la stigmatisation de pratiques individuelles douteuses (spéculation) ou naïves (escroqueries).

La deuxième section analyse l'asymétrie entre, d'une part, un ensemble de concepteurs qui voient dans les cryptoactifs un foisonnement de significations, et d'autre part, leur diffusion comme des objets cotés sur des marchés financiers, comme un moteur de leur institutionnalisation. La conception des jetons n'était pas isolée d'une société qu'elle serait venue percuter pour le meilleur ou pour le pire. Elle se développait au travers de réseaux d'entrepreneurs et d'institutions publiques qui, à Singapour comme en France, voyaient ensemble ces objets comme des innovations ayant une dynamique propre, qu'il fallait encourager plutôt que problématiser, au risque d'en diminuer la vigueur et de « manquer le train » de cette innovation. Cette section lie une préoccupation méthodologique et analytique. Je présente les meetups organisés par ConsenSys comme postes d'observation de l'institutionnalisation des cryptoactifs au long cours ; des sites de problématisation des cryptoactifs (Callon 2012). Je mobilise certains de ces matériaux pour montrer qu'en réduisant la problématisation des jetons utilitaires à des objets marchands, les institutions publiques et différents portes-paroles du secteur des cryptoactifs en France favorisaient leur diffusion en laissant aux concepteurs le soin de définir leurs significations.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Deux ensembles d'utilisations d'Ethereum étaient distinguées par les acteurs, en fonction du type d'organisation économique : des réseaux économiques B2B ou B2C. Comment comprendre qu'Ethereum soit simultanément utilisé pour bâtir des organisations économiques aux gouvernances apparemment si éloignées ? Je réponds en distinguant deux opérations de production des transactions avec Ethereum, la formation et la formulation. Cette distinction permet d'analyser Ethereum comme une technologie de gouvernance modalisable par ces deux opérations. Cette modalisation se lit dans la notion de

Introduction générale

« plateforme », attribuée par les concepteurs aux applications développées avec Ethereum, quel que soit le type d'utilisation B2B ou B2C. Cette modalisation implique de faire se rencontrer deux utilisateurs inscrits dans la conception de ces plateformes (Akrich 1987) ; l'un est générique à la technologie de plateformes Ethereum, l'autre est spécifique à chacune.

La première section montre qu'Ethereum est devenue une technologie de plateformes par un processus entrepreneurial et technologique au centre duquel figurait l'entreprise ConsenSys. Loin d'être contradictoire entre elles, les différentes organisations économiques étaient appelées à converger vers une même infrastructure pour une économie numérique unifiée. ConsenSys était un bâtisseur de systèmes (Hughes 1983) et d'un « écosystème » de formulateurs de transactions ; typiquement, des concepteurs de DApps. À partir de ses premiers investissements et son activité de développement de logiciels, l'entreprise a proposé des offres de conseils et noué des partenariats enrôlant de grandes entreprises à l'utilisation d'Ethereum. Cette section documente différentes tactiques déployées par ConsenSys qui ont rendu la formation et la formulation des transactions ajustables aux deux types d'organisations économiques imaginées.

La deuxième section donne deux points de vue sur l'écosystème, ensemble des concepteurs de plateformes utilisant Ethereum : depuis des meetups organisés par ConsenSys où circulent les pratiques de conception entre utilisations B2B et B2C, et depuis le processus de conception d'une plateforme au sein d'Orange. Ce cas témoigne de l'ampleur des modalités de gouvernance d'Ethereum. Premièrement, j'indique l'intrication entre l'écosystème et la notion de plateforme, qui était également un horizon organisationnel partagé par les acteurs le constituant. Deuxièmement, j'analyse le cadrage de la conception du service LeVote d'Orange comme prescription d'un utilisateur mêlant utilisateur générique d'Ethereum et citoyen imaginé par les concepteurs. Troisièmement, j'analyse l'échec temporaire de la mise en œuvre commerciale du service comme une incompatibilité entre deux manières politiquement irréconciliables de former les transactions.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Une littérature en droit analyse les *smart contracts* comme de possibles instruments contractuels à l'aune de leurs caractéristiques ou règles « auto-exécutantes » ou « auto-appliquées », héritées du caractère « autonome » de l'infrastructure. Généralement prise pour acquise, l'autonomie de l'infrastructure est pourtant le résultat d'alliances temporairement stabilisées qui nécessitent des interventions régulières d'une « communauté ». Les principes de l'action communautaire font controverse au sein de la communauté. Je les analyse en termes de « rationalités infrastructurelles », par analogie avec la « rationalité gouvernementale » (Foucault 2004b).

La première section montre que la communauté problématise la construction de l'infrastructure de deux manières : à l'aune de la mystique (en termes de « centralisations » techniques et politiques) mais aussi, en la dépassant, au prisme des usages de l'écosystème. Cette deuxième proposition fait controverse, car elle contrevient à la mystique qui pose, par principe, que les usages ne doivent pas être un objet de connaissance et d'action ; leur signification devrait au contraire rester séparée de la production matérielle de l'infrastructure, exclusivement confiée aux *miners*. La communauté et l'infrastructure se fracturent dans cette opposition portant sur l'action communautaire sur l'infrastructure, mais aussi sur la manière de faire communauté. L'autonomie apparaît à cette occasion comme une fonction de l'infrastructure, qui nécessite d'être qualifiée et porte à controverse.

La deuxième section explore les difficultés des acteurs de la communauté à penser un bon gouvernement. Premièrement, je propose une grammaire de l'action collective communautaire en m'appuyant sur une controverse qui a fait date. Elle montre que l'infrastructure est le support incontournable de toute décision collective légitime : agir ensemble suppose d'inscrire la décision collective dans l'infrastructure. Deuxièmement, je m'appuie sur l'extension de l'action communautaire au « financement des biens publics ». Elle montre que la « bonne » gouvernance est dépouillée de toute forme d'organisation formelle, suspectes par hypothèse de toute forme de favoritisme envers certains membres

Introduction générale

de la communauté. Troisièmement, le « bon » gouvernement est un ensemble de mécanismes automatiques pensés selon la mystique : ils doivent produire une action collective (financer des « biens publics ») indépendamment de l'inclinaison rationnelle de chacun à les contourner. Enfin, j'expose une condition essentielle du fonctionnement de ces mécanismes. Les individus doivent agir « authentiquement » par le vote, c'est-à-dire penser leur intérêt individuel à la lumière de l'intérêt collectif, de la même manière que ce que prescrit la mystique aux *miners* qui doivent être indifférents aux significations des transactions.

Annexe 1 – Épisodes de terrain hors ligne

L'Annexe 1 résume mes différents épisodes d'enquête sur la période retenue : de février 2018 à mars 2020.

Annexe 2 – Meetups

L'Annexe 2 donne des informations détaillées sur les meetups, notamment la numérotation mobilisée dans le texte. Les meetups sont présentés au Chapitre 2, section 2.

Annexe 3 – Ethereum par un bord

L'Annexe 3 est un document de travail que je propose comme un glossaire situé. Il raconte une prise de contact avec Ethereum par un de ses bords, mon navigateur Web, en détaillant le cours d'action dans lequel une transaction est validée. Je l'ai rédigé en 2018 comme une auto-ethnographie dans laquelle je discute avec un lecteur fictif, anticipant ses surprises qui, souvent, étaient également les miennes.

Faisant face au foisonnement de termes techniques apparaissant sur l'interface du *wallet* en ligne MyEtherWallet comme les *nodes* (nœuds), *blocks* (blocs), ou *hash*, j'y ai consigné ma compréhension de relations entre différentes entités peuplant l'infrastructure. Je l'ai enrichie de recherches sur les nœuds et sur un autre système de *wallet*, Metamask (qui

Introduction générale

apparaît dans le Chapitre 3).

Avant de rédiger ce document, j'avais uniquement expérimenté l'usage des cryptoactifs *via* les plateformes d'échanges (*exchanges*), en l'occurrence Binance et Coinbase (pour des montants de quelques dizaines d'euros). Mais ces plateformes masquaient le fonctionnement du réseau auquel je souhaitais accéder. L'interface retenue permettait de mieux comprendre ce qu'il se passait.

Chapitre 1. Mystique du protocole : calculer sans connaître

What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions. (Buterin 2013 : 1)

Introduction. De Bitcoin à la blockchain : l'informatique faite théorie du contrôle

Une proposition de système doté d'un langage de programmation de « fonctions de transitions d'état » de « contrats ». Voilà en quelques mots la proposition formulée par l'inventeur d'Ethereum dans le « *whitepaper* » d'Ethereum. Ce document aux allures de publication scientifique relève du manifeste ; la forme *whitepaper* était déjà un repère pour les passionnés de Bitcoin et des projets de cryptomonnaies qui s'en inspiraient. En circulant dans leurs réseaux, notamment *via* les conférences où ils se retrouvaient comme la *Bitcoin Conference*, il participait à fédérer des enthousiastes de Bitcoin et des premières cryptomonnaies autour de Vitalik Buterin. L'auteur y mêlait description d'usages et du fonctionnement imaginés en développant deux arguments principaux. D'une part, Bitcoin était une technologie « sous-jacente » appelée « blockchain ». D'autre part, cette technologie existait par les différentes « applications alternatives » à la monnaie numérique de Bitcoin, connues sous l'appellation générique « cryptomonnaies ».

En 2013, l'enthousiasme suscité par la proposition de Buterin tenait moins à l'annonce d'une nouvelle infrastructure construite selon l'architecture de Bitcoin, plus petit dénominateur commun des différentes cryptomonnaies, que dans l'idée de calcul par cette infrastructure. Bitcoin et les cryptomonnaies enregistraient des soldes de comptes des utilisateurs dans un registre commun à tous. Ethereum imaginait un autre type d'usage pour ce registre : l'enregistrement de calculs dont les règles seraient programmables par les utilisateurs, dans un langage universel³³. Ces règles seraient des contrats, et l'exécution de

33 L'universalité de ce langage se comprend au sens informatique, par la notion de langage « Turing-

ces règles (calculs) signifieraient état des contrats. Cinq ans plus tard, cette vision se traduit par plus d'un millier d'applications dites « décentralisées » ou DApps. Encore trois ans plus tard, en 2020, ce chiffre était multiplié par quatre³⁴. Bitcoin est central dans l'analyse d'Ethereum comme une « technologie de gouvernance », au sens défini dans l'introduction générale de cette thèse. L'architecture est mise en « boîte noire » par les concepteurs d'Ethereum : son fonctionnement et ses effets politiques sont supposés et partagés par ses concepteurs, sans être rediscutés. Ethereum fait de Bitcoin une technologie de calcul.

Ce chapitre analyse Ethereum dans les termes de la technologie de gouvernance (les connaissances, les pratiques, les modes de raisonnement assemblés dans la conception d'Ethereum pour gouverner les relations numériques) en se concentrant sur la filiation technologique entre Bitcoin et Ethereum : de quelles qualités politiques prêtées à Bitcoin hérite Ethereum ? Dans la suite de cette introduction, je commence par présenter une littérature interdisciplinaire qui analyse, précise et conteste une qualité politique de la blockchain tirée de Bitcoin : des relations numériques se passant de confiance dans toute forme d'institution. Puis, à la suite de travaux qui ont directement pris en charge la question de la gouvernance avec Bitcoin, je précise comment j'analyse l'héritage de Bitcoin avec Ethereum : une théorie du contrôle inscrite dans le protocole du réseau.

Blockchain et le social « sans confiance » dans les institutions

Une vaste littérature (sciences sociales, gestion, économie, géographie) a approché la blockchain par la promesse associée à Bitcoin et par extension aux cryptomonnaies : la constitution de relations numériques affranchie de « confiance » dans des institutions extérieures aux entités mises en relation. Les acteurs de leur développement étaient sans doute les premiers à affirmer l'absence de confiance comme une qualité intrinsèque à ces

complet », et par l'ambition d'Ethereum, détaillée plus loin : rendre toute relation numérique codable comme un contrat.

34 En novembre 2021, le site StateOfTheDapps référençait ces différentes applications en « catégories ». Elles donnent une idée de l'ampleur des domaines, objets ou relations qu'elles visent : *Games, Gambling, Finance, Social, High risk, Exchanges, Development, Media, Wallet, Marketplaces, Governance, Security, Property, Storage, Identity, Energy, Health, Insurance* (StateoftheDApps 2021).

Chapitre 1. Mystique du protocole : calculer sans connaître

objets. En creux, ils affirment la possibilité technologique de relations existant entre individus isolés, sans médiation d'ordre institutionnel, culturel, politique ou social. En confrontant la promesse de *trustlessness*, ces travaux pointent des rapports de confiance des utilisateurs à la technologie, des imaginaires et héritages politiques, et plus généralement une multitude d'acteurs impliqués dans la constitution de relations numériques : développeurs, *miners*, utilisateurs, entrepreneurs, mais aussi des objets techniques comme le protocole, le réseau, les *coins* et leurs places d'échange.

Un premier ensemble de travaux a testé, discuté, ou nuancé la promesse de « *trustlessness* » de la blockchain. Reprenant la rhétorique des acteurs du développement de la blockchain, en posant que cette technologie répond à une « crise de confiance qui balaya le monde aux premiers jours de la crise financière de 2008 », des auteurs proposent de comprendre la blockchain comme une « *confidence machine* » plutôt que comme une « *trustless technology* » (De Filippi et al. 2020). Ainsi, les règles cryptographiques, les mathématiques et des incitations économiques accroissent une confiance procédurale (*confidence*) dans les opérations du système de calcul, tout en nécessitant de faire confiance (*trust*) à des acteurs liés au réseau sous-jacent. D'autres voient la blockchain comme une technologie permettant de construire des preuves de droits et d'actions passés, c'est-à-dire des « tenues de compte publique » alternatives aux institutions assurant aujourd'hui ce travail, bien qu'encore inaboutie pour permettre de « (re)configurer le pouvoir » qui subit une défiance généralisée en raison des « failles » des institutions contemporaines (Lemieux 2020). Du point de vue de la nouvelle économie institutionnelle, les blockchains sont une forme émergente de protocoles comparable au protocole diplomatique qui se développa entre 2400 et 1200 avant notre ère au niveau de l'actuel Proche-Orient : en faisant de ces deux formes de protocoles des instruments de coordination économique entre agents séparés par des « frontières de possible manque de confiance », l'auteur affirme le potentiel de la blockchain à produire de nouvelles institutions (Berg 2017). Du point de vue de la science politique, la « *decentralized governance* » promue dans les blockchains serait une théorie organisationnelle qui interroge les « mécanismes traditionnels » que sont l'autorité de l'État, la citoyenneté et la démocratie (Atzori 2015). L'autrice refuse d'y voir une théorie

Chapitre 1. Mystique du protocole : calculer sans connaître

politique, comme le suggèrent des discours de promotion des blockchains relevant selon elle de l'utopie technologique appelant à la chute des « institutions centralisées », et met en garde sur le risque d'affaiblissement des citoyens soumis aux « pouvoirs privés dans des écosystèmes distribués ». Soumise à investigation philosophique, des auteurs étudient les impacts normatifs de la technologie conceptualisée comme ensemble de « *narrative technologies* » qui « configurent les récits par lesquels nous comprenons notre réalité sociale » (Reijers & Coeckelbergh 2018).

Un deuxième ensemble de travaux voit la promesse de « *trustlessness* » et d'affranchissement des institutions comme imaginaire d'une gouvernance immatérielle par le code informatique *a minima* irréaliste, sinon purement utopique. Des travaux en anthropologie de la finance ont discrédité la supposée *trustlessness* au profit d'un déplacement de la confiance dans les algorithmes et les plateformes d'échanges de cryptomonnaies (Maurer et al. 2013) et soulignent l'imaginaire économique cultivé dans une forme d'entre-soi par des communautés fermées et gardées, opérant dans l'illusion que leur communauté ne suppose pas d'institution médiatrice (Nelms et al. 2018). Dans la même veine, la blockchain est critiquée par l'examen des « aspirations et insatisfactions » exprimées dans les « rêves » de futurs alternatifs, de décentralisation et de désintermédiation, d'autonomie et d'automatisme qu'elle véhicule (Swartz 2015). Ce déplacement de la confiance dans les dispositifs est parfois directement posé comme hypothèse de travail : par exemple, des analyses quantitatives de publications en ligne proposent une série d'« attributs » les plus susceptibles de « créer et maintenir la confiance des utilisateurs dans Bitcoin » (Marella et al. 2020). Des travaux prennent les qualités imaginées des blockchains comme des résultats de négociations, qui se comprennent dans l'activité de conception de ces artefacts, par exemple dans des activités entrepreneuriales, dont le suivi révèle des tensions et de ruptures qui transforment simultanément les artefacts et les imaginaires (Jabbar & Bjorn 2019). Des auteurs en géographie sociale ont critiqué la « foi » de gouvernement par le code en remplacement de la confiance dans les institutions en pointant la matérialité du code et des espaces de ces dispositifs (Zook & Blankenship 2018).

Ces efforts témoignent d'un intérêt interdisciplinaire pour saisir l'objet de recherche « blockchain » en général. Mais ce faisant, ils supposent que la blockchain existe en toute généralité depuis Bitcoin, dont la filiation est reconnue par la référence au moins allusive à son *whitepaper* (Nakamoto 2008). Ces travaux donnent à voir une grande richesse de problèmes et d'acteurs impliqués dans le développement rapide de ce nouvel objet de recherche. Toutefois, ils tendent à prendre pour acquis que la blockchain présente en général certaines qualités politiques propres, notamment la *trustlessness*, qu'ils prennent soin de nuancer, de préciser ou de critiquer. Dans ce chapitre, je propose de ne pas supposer que nous savons ce qu'est la blockchain en général, en partant du seul constat unanimement partagé par les acteurs comme la littérature de la filiation entre Bitcoin et un dispositif spécifique qui en hérite, Ethereum. Avec cet angle des dispositifs, je m'inspire de travaux d'auteurs se revendiquant des *Science and Technology Studies* qui ont analysé la promesse de *trustlessness* comme le résultat du processus de développement continu de Bitcoin.

Analyse de la gouvernance : la mystique du protocole

La *trustlessness* est le résultat du travail de certains acteurs, développeurs ou des participants à la maintenance du réseau et fortement capitalisés (propriétaires de grands calculateurs), qui jouissent d'une influence importante dans le développement du système. Vidan & Lehdonvirta (2019) voient une « *maintenance of trustlessness* » assurée par ces acteurs qui contrôlent des sites critiques : les arènes d'élaboration du code du protocole, et les entrepôts de serveurs qui sont contrôlés par une poignée d'entreprises (« fermes de minage »). Les auteurs proposent de comprendre ces dissonances par la mise en place de « stratégies d'autorisation » qui font perdurer le discours et les imaginaires en même temps que la matérialité de Bitcoin. De Filippi & Loveluck révèlent ce qu'ils appellent « une structure de pouvoir hautement technocratique » dans l'élaboration du code du protocole, en décrivant deux mécanismes de gouvernance par l'analyse d'une controverse qui cliva la « communauté » autour d'un choix d'évolution du protocole de Bitcoin (2016). Leur analyse de la gouvernance « par » l'infrastructure³⁵ révèle que des principes de marché sont embarqués dans le protocole informatique, et la gouvernance « de » l'infrastructure fait

³⁵ Ce concept est repris de Musiani et al. (2016).

Chapitre 1. Mystique du protocole : calculer sans connaître

apparaître que seul un petit nombre de développeurs expérimentés a un rôle clé dans son développement. Ces deux travaux font apparaître des différences de positions entre acteurs humains en présence.

Poser le problème de la gouvernance pour analyser les qualités prêtées à un dispositif est l'angle développé par des auteurs inspirés par la sociologie de la traduction (Akrich et al. 2006) qui analysent Bitcoin par l'étude de controverses. « Bitcoin », « les intermédiaires » ou la « *trustlessness* » ne sont ni essentialisés ni examinés selon un prisme dessiné par une promesse préalable ; ils sont les résultats d'un processus d'innovation en train de se faire, en témoigne les titres de leurs travaux : « *The Paradoxes of Distributed Trust* » (Mallard et al. 2014), « *Governing what wasn't meant to be governed* » (Musiani et al. 2018).

Les discours d'experts participent à former la confiance dans le système lui-même, à la valeur de son jeton et par là au monde qu'ils cherchent à faire advenir (Mallard et al. 2014). Les mêmes auteurs prennent pour objet la gouvernance de Bitcoin telle qu'elle se conçoit. Ils montrent que les positions de développeurs ne peuvent pas être distinguées du « cœur » de l'infrastructure, en raison de l'importance de leur activité de développement et de maintien du code (Musiani et al. 2018). Les mises à jour résultent de décisions qui sont priorisées, du déploiement de conflits, de normes produites par l'alignement des acteurs en présence. Les autrices et auteur pointent des « micro-hiérarchies », entre les développeurs eux-mêmes ou entre développeurs et intermédiaires, lesquels sont appelés par les premiers pour résoudre des tensions. Par là, ils assurent des fonctions de gouvernance. Enfin, ils invitent à ouvrir les catégories habituellement naturalisées de « *miners* » et d'« utilisateurs » qui constituent les deux catégories d'acteurs habituellement retenues pour Bitcoin, en étant attentifs à leurs relations à l'infrastructure respectivement en termes de point de passage obligés et de relations aux intermédiaires pour analyser comment ces acteurs sont rendus, dans des degrés variés, passifs ou actifs.

Ce chapitre s'inscrit à la suite de ces travaux qui pluralisent la notion de gouvernance étudiée au niveau d'un dispositif (Bitcoin). Mais plutôt que d'étudier la gouvernance de Bitcoin ou d'Ethereum de manière située dans le temps comme le font ces travaux, ce

chapitre se concentre sur la politique inscrite dans le protocole de consensus de Bitcoin. Comme l'indique le titre de ce chapitre, ce protocole a une « mystique ». Plus petit dénominateur commun entre Bitcoin et ses descendants comme Ethereum, c'est lui qui est systématiquement désigné par les concepteurs et promoteurs pour expliquer la filiation technique et politique. Mon objectif est moins d'éclairer la gouvernance de Bitcoin ou d'Ethereum telle qu'elle se fait, que de cerner la manière dont les concepteurs imaginent gouverner les relations numériques avec un protocole informatique.

Du problème institutionnel au problème du contrôle des relations numériques

Le concept de gouvernance permet de décaler le regard porté sur des institutions postulées en avance aux opérations par lesquelles les acteurs du développement des blockchains imaginent une politique des relations numériques. La littérature esquissée plus haut note bien un problème institutionnel posé par les acteurs dans leurs discours. Mais ces acteurs ne luttent pas en pratique et frontalement « contre » des institutions, également appelées « autorités » et dénoncées pour leur « contrôle ». Leur opposition à ces institutions est de l'ordre de l'alternative : elles existent, et plutôt que de les combattre directement, les blockchains permettraient, selon les acteurs, de se prémunir de leur présence.

Le problème des acteurs des blockchains, prolongé à partir de Bitcoin, peut être formulé ainsi : comment conjurer le contrôle d'institutions sur des relations numériques par l'innovation technologique ? J'analyse le vocabulaire employé par les acteurs comme éléments réflexifs. J'examine comment ils définissent les problèmes qui les font agir et les solutions qu'ils esquissent. Je mobilise des verbatims des acteurs eux-mêmes, extraits d'observations en situation ou d'écrits. La démarche d'enquête que je restitue dans ce chapitre est la suivante : à partir d'éléments choisis de discours des acteurs en présence, je caractérise le mode de pensée qui les anime à la fois dans les problèmes qu'ils identifient en définissant des solutions technologiques, notamment le problème de pouvoir dans l'administration de la monnaie pour Bitcoin et du Web pour Ethereum.

Chapitre 1. Mystique du protocole : calculer sans connaître

Ce choix analytique rend compte du télescopage entre le vocabulaire critique, formulé en termes d'institutions, et un vocabulaire informatique et calculatoire dans lequel le monde est non seulement problématisé, mais dans lequel sont aussi formulées des alternatives ; dit autrement, un vocabulaire par lequel un monde nouveau advient. Je m'appuie sur l'approche du discours de Norman Fairclough dite « *critical discourse analysis* » (Fairclough 1989). Ce linguiste cherchait à proposer une méthode d'analyse des conventions sociolinguistiques, notamment dans les discours des responsables politiques, qu'il voyait comme sites d'incorporation de différences de pouvoir et d'émergence de relations de pouvoir particulières. Selon lui, ces conventions sont les produits de relations ou de luttes de pouvoir ; elles embarquent des hypothèses constituant des idéologies dans leur « sens commun ». Expliquer la formation de l'idéologie était à l'époque un enjeu majeur de recherche, dans la mesure où l'idéologie était vue comme le premier moyen de fabriquer le consentement au pouvoir. Langage, pouvoir et idéologie : les relations entre ces trois objets de recherche devaient, pour Fairclough, être systématisées.

Méthodologiquement, je considère que le protocole informatique est une convention sociolinguistique au sens de Fairclough. Toutefois, le vocabulaire des acteurs me sert de point d'accès (réflexif) à un autre vocabulaire : le protocole lui-même. Il n'est pas question ici de chercher à identifier une idéologie qui serait partagée par les développeurs et les promoteurs de Bitcoin et d'Ethereum. Je prends leurs discours et leur vocabulaire comme des explicitations langagières du protocole informatique lui-même. Ils visent, sinon à former un consentement de leurs utilisateurs, au moins à naturaliser une manière de gouverner les relations ; cette naturalisation est reprise, en « boîte noire » ou de manière « conventionnelle », de Bitcoin aux autres cryptomonnaies et à « la blockchain ». Ces discours peuvent effectivement être analysés comme explicitations du protocole en raison de leurs contextes d'énonciation : les écrits (ouvrages et sites spécialisés) comme les oralités (conférences de promoteurs et interview des concepteurs par des sites spécialisés) sont dirigés vers des auditoires convaincus ou en train d'être intéressés par ces technologies.

J'approche les blockchains comme des dispositifs de contrôle (des relations) plutôt que de

Chapitre 1. Mystique du protocole : calculer sans connaître

voir le contrôle comme quelque chose dont les acteurs se défont : le contrôle est un objectif fixé au dispositif numérique. Ils prolongent une histoire qui a commencé avec l'invention du terme « cybernétique » (Wiener 1948). Né de la volonté de croiser ensemble différentes lignes de recherche scientifique jusque-là très éloignées, ce terme fait référence à l'idée d'une science du contrôle compris comme « commande », « *the science of steermanship* » (Pickering 2009). Au lendemain de la seconde guerre mondiale, les cybernéticiens pensaient le monde comme un chaos moral auquel il s'agissait d'apporter un ordre (Mirowski 2002) atteignable par des activités de recherche et de développement de « systèmes » qui seraient « adaptatifs » à leur environnement. C'est dans ce rapport adaptatif qu'apparaissent les notions de communication, puis d'information et de contrôle, à l'image du travail de Wiener consistant à prédire la position d'un avion soumis à des tirs de missiles.

Envisagé comme « commande » d'un système orienté vers un objectif, le contrôle est renversé (d'institutionnel à alternative par un dispositif) : les relations numériques peuvent être contrôlées individuellement grâce à un système qui est commandé vers un objectif ad-hoc plutôt qu'orienté vers les personnes elles-mêmes. Le contrôle protège chacun. Andrew Pickering associe la notion de contrôle portée par la cybernétique à un regard porté sur le monde : l'impossibilité de connaître déplace l'attention vers le devenir. Le contrôle se comprendrait alors avec l'idée d'adaptation, de faire avec, de saisir à son avantage un monde qu'il n'est pas possible de faire avancer dans un sens donné (Pickering 2009 : 383). Pour les cybernéticiens, le contrôle se comprend dans un monde qui n'est pas prédictible et qu'il s'agit de « révéler » depuis un système plutôt que de « cadrer » ou de « dominer » :

If cybernetics staged an ontology in which the fundamental entities were dynamic systems evolving and becoming in unpredictable ways, it could hardly have been in the business of Big Brother-style domination and enframing. It follows immediately from this vision of the world that enframing will fail. The entire task of cybernetics was to figure out how to get along in a world that was not enframable, that could not be subjugated to human designs—how to build machines and construct systems that could adapt performatively to whatever happened to come their way. (Pickering 2009: 31-32)

Dans l'esprit des analyses de Pickering, les concepteurs et promoteurs des blockchains

Chapitre 1. Mystique du protocole : calculer sans connaître

agissent dans un monde en faisant avec ce monde, en saisissant à leur avantage ce qu'il offre : en dépit des institutions qu'ils contestent, ils bâtissent des systèmes permettant de s'associer. S'il est illusoire de connaître le monde, il est toutefois possible d'en contrôler des éléments par des technologies : c'est le cas des relations numériques.

Plan du chapitre

Ce chapitre est organisé en deux sections. La première section analyse le protocole de Bitcoin comme un ensemble de règles informatiques élaborées pour gouverner des relations numériques indépendamment des sujets de ces relations. Elle montre que les promoteurs et concepteurs de Bitcoin font du contrôle des institutions un problème épistémique. En effet, alors que leur gouvernement suppose une connaissance des relations entre individus, Bitcoin répond en instaurant une ce que je désigne comme une « rupture épistémique »³⁶ : la dissociation entre ce qui est su par ceux qui sont en relation, d'une part, et par ceux qui reconnaissent cette relation à l'échelle d'Internet en entier, d'autre part. Cette reconnaissance passe par la sécurisation du registre de transactions, objet élaboré en commun. La sécurité du registre est l'objectif « commandé » du système, au sens de la cybernétique. Dans ce système, la relation numérique est « transaction » : contrôlable par les individus sans institution autre que le réseau lui-même, et reconnue par tous en raison de son mécanisme d'inscription. Ce faisant, le protocole est une théorie de la neutralisation du pouvoir qui s'appuie sur des hypothèses anthropologiques proches de celles de Friedrich Hayek.

La seconde section analyse comment Bitcoin est vu par les concepteurs d'Ethereum, au sens donné par le chercheur en sciences cognitives et intelligence artificielle Marvin Minsky et repris par l'historien spécialiste des modèles scientifiques et techniques Franck Varenne :

Pour un observateur B, un objet A est un modèle d'un objet A dans la mesure où B peut utiliser A* pour répondre à des questions qui l'intéressent au sujet de A.*

36 Cette notion est proposée sans aucun lien avec celle de « rupture épistémologique » proposée par les philosophes Gaston Bachelard ou Louis Althusser.

Chapitre 1. Mystique du protocole : calculer sans connaître

(Minsky 1965, cité par Varenne 2016 : 12)

L'objet transaction permet aux concepteurs d'Ethereum d'imaginer un système d'inscription similaire à Bitcoin, mais programmable par les utilisateurs : le code permettrait à chacun de définir des relations à l'instant de la transaction mais aussi dans le futur, en programmant la relation comme un contrat. Les relations contrôlées ne sont plus seulement monétaires, mais établies au travers du Web au sens large. À la suite de Bitcoin, l'exécution des règles de ce contrat, c'est-à-dire le calcul et son inscription, serait séparée de la signification donnée au résultat de ce calcul. Au sens de Michel Foucault, Bitcoin est mobilisé comme un « mécanisme de pouvoir », au sens de « pouvoir inscrire ». Avec Ethereum, les stratégies et tactiques développées avec Bitcoin sont mobilisées pour infléchir un « art de gouverner » par le calcul informatique.

1. Bitcoin : gouverner des relations sans sujets de connaissance

Le protocole de Bitcoin est un artefact politique (Winner 1980) imaginé : un artefact qui est conçu pour avoir des effets politiques, qui « a » une politique imaginée, notamment des effets d'autorisation et d'exclusion³⁷. La première sous-section analyse la problématisation de Bitcoin à partir de verbalisations de promoteurs (livres, prises de paroles publiques, entretien) que je prends comme moments de réflexivité. Ils donnent accès à la manière dont ils pensent la politique : des relations inter-individuelles formées par un système « autonome ». La deuxième sous-section analyse l'autonomie de Bitcoin en suivant les traductions (Akrich et al. 2006) opérées par le protocole de consensus, agenceur des acteurs en présence. Elle met en évidence que la politique de Bitcoin tient à une opération de rupture épistémique : le réseau est « sécurisé » par le protocole dans la mesure où les relations des utilisateurs ne sont pas connues des participants du réseau qui ne voient que des objets d'investissement. La troisième sous-section montre que cette politique de sécurisation est conçue comme neutralisation de toute forme de pouvoir, quelle que soit la manière dont le pouvoir est imaginé. Cette analyse s'appuie sur le parcours du théoricien du pouvoir Steven Lukes (1974, 2004).

1.1. Problématisation des institutions comme systèmes corruptibles

Bitcoin problématise les institutions comme des systèmes corruptibles. Considérer les organisations humaines comme des « systèmes » conduit les promoteurs de Bitcoin à assimiler gouvernement et domination. Cette problématisation s'enracine historiquement dans l'imaginaire d'échanges pair-à-pair sur Internet, sans institutions totalisant un espace social. Elle est formulée en termes d'« autorités ». Avec Bitcoin, ce problème est étendu à

³⁷ Le cas de la conception de l'infrastructure routière autour du parc de Long Island est éloquent : en dessinant des ponts suffisamment bas pour desservir le parc, l'architecte excluait de cet espace les populations défavorisées de New York qui se déplaçaient principalement en bus.

une critique des monnaies fiduciaires qui supposent une confiance diffuse dans les institutions, hypothèse naïve ou dangereuse pour les promoteurs de Bitcoin. La formulation de ce problème est concomitante avec la solution proposée par ses promoteurs : un protocole « autonome » qui garantit des échanges sans intermédiaires, et qui n'est lui-même garanti par aucun acteur en lequel les utilisateurs devraient avoir confiance.

Bitcoin dans une généalogie du problème des « autorités » sur Internet

Avant d'exister comme un système technique, Bitcoin était proposé dans un article intitulé *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto 2008). Le titre de cette publication résume la proposition du ou des auteur·e·s qui se dénommaient Satoshi Nakamoto : un système d'argent électronique échangeable de pair-à-pair sur Internet. L'implication des institutions financières dans les échanges d'argent sur Internet, et plus généralement de tout « tiers de confiance », était le problème principal auquel ce « système » devait alors répondre :

“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.”
(Nakamoto 2008: 1)

Ces deux premières phrases du résumé de l'article situent Bitcoin dans une généalogie d'autres solutions au même problème. Ces dernières y ont répondu par les « signatures numériques », en référence à des expériences de solutions cryptographiques, mais impliquant toujours un « tiers de confiance » pour régler le « problème de la double dépense », c'est-à-dire (positivement) garantir un état global des comptes de chaque membre d'un groupe ou (négativement) empêcher que quiconque puisse utiliser deux fois une même unité. Bitcoin répond à ce problème par un registre unique, vu comme authentique en toute circonstance, sans qu'aucune personne morale ou physique garantisse sa tenue.

Éviter l'intermédiation est un problème ancien et central dans les tentatives de conception

Chapitre 1. Mystique du protocole : calculer sans connaître

d'argent numérique. Nakamoto reformulait le problème rencontré par des tentatives de systèmes de paiement numériques plus anciennes qui cherchaient à s'affranchir d'intermédiaires financiers en utilisant la cryptographie. Par exemple en 1983, avant la popularisation d'Internet, l'informaticien David Chaum avait conçu eCash. Ce système de gestion de l'argent liquide de manière électronique permettait à un acheteur de réaliser des paiements de façon chiffrée et certifiée par sa société Digicash, sans besoin ni d'ouvrir un compte chez son fournisseur ni de transmettre ses références de carte bancaire. Cette solution impliquait toujours l'activité d'un acteur certifiant les comptes, la société Digicash elle-même (qui finit par faire faillite). Deux autres tentatives restées à l'état de concepts envisageaient des solutions de paiement s'affranchissant de tout « tiers de confiance », plutôt que de remplacer un intermédiaire par un autre comme le proposait Digicash. L'idée était de produire un registre de transactions public. B-money puis Bit gold, annoncés respectivement en 1998 par Wei Dai et en 2005 par Nick Szabo, étaient pensés respectivement comme un système de monnaie électronique anonyme et comme une proposition de monnaie électronique « décentralisée ».

L'inscription revendiquée de Bitcoin dans cette généalogie³⁸ a été interprétée dans la continuité de projets politiques développés tout au long de l'histoire d'Internet et des réseaux pairs-à-pairs par des universitaires explicitement critiques (Golumbia 2016) ou plus modérés (Brunton 2019), ainsi que par des promoteurs (Favier et Takkal Bataille 2017) de Bitcoin. Ces différents auteurs voient dans le système technique Bitcoin l'incarnation d'idées politiques. Les porte-voix de la communauté Bitcoin en France écrivent par exemple : « Bitcoin, un projet sociétal autant que technique : se passer d'intermédiaires et d'autorité » (Favier et Takkal Bataille 2017 : 31). Au moins de manière théorique et discursive, ils dénonçaient l' « intermédiation » constituée par une entité dotée d'une personnalité, qu'elle soit physique ou morale : un individu, une entreprise, une association, un gouvernement. Cette tendance a été analysée au travers de différentes dynamiques, notamment militantes, intellectuelles ou culturelles.

38 Voir par exemple la page « *Literature* » du « Satoshi Nakamoto Institute », qui fait de l'article de Satoshi Nakamoto l'héritier de dizaines de publications d'entrepreneurs, de philosophes, de militants ou de développeurs informatiques : « *Bitcoin was not forged in a vacuum. These works serve to contextualize Bitcoin into the broader story of cryptography and freedom.* » (Satoshi Nakamoto Institute 2021).

Chapitre 1. Mystique du protocole : calculer sans connaître

Cette généalogie assimile intermédiation technique d'une part et intermédiation sociale ou institutionnelle d'autre part, une tendance qui se retrouve dans le mouvement cypherpunk et la pensée crypto-anarchiste auxquels sont souvent associés Bitcoin. Les concepteurs de B-money et de Bit gold, respectivement ingénieur informatique et cryptographe, étaient des représentants médiatisés de cette inclinaison politique. Les cypherpunks partagent une sensibilité pour des pratiques : ils constituent un groupe informel de personnes se donnant pour objectif de défendre le respect de la vie privée par le développement et l'utilisation proactive de la cryptographie. Ils luttent contre le « contrôle » des gouvernements et des grandes entreprises sur les transactions financières, échanges monétaires et paiements, au double sens de « surveillance » et de « possibilité d'interrompre » une transaction ou une communication (Favier et Takal Bataille 2017 : 33). Les cypherpunks luttent par l'action, à l'image de Philipp Zimmerman, inventeur du populaire logiciel de cryptographie Pretty Good Privacy (PGP), ou de Julian Assange, fondateur de Wikileaks (Assange 2012). Le crypto-anarchisme est une pensée politique qui pose que le développement et l'utilisation de la cryptographie sont la meilleure défense contre la surveillance des communications informatiques, notamment sur Internet. Ses représentants dénoncent en particulier l'application de réglementations de prévention du terrorisme ou anti-blanchiment nées dans les années 2000 avec le Patriot Act qui autorisent le déchiffrement d'informations (chiffrées) sur demande d'un juge, et exigent que des intermédiaires financiers (comme les banquiers) identifient précisément leurs clients. En réponse, ils plébiscitent l'anonymisation des communications numériques.

Le mouvement cypherpunk et les principes crypto-anarchistes partagent le thème de la liberté individuelle contre les gouvernements vus comme une forme de soumission institutionnelle. Ils se rejoignent en un phénomène appelé « cyberlibertarisme »³⁹ dont le principe a été résumé par « aucun gouvernement ne doit réguler l'Internet » au nom du principe, assez flou, d' « *Internet freedom* » (Malcolm 2013). Ce principe qui se retrouve dans des textes prenant souvent la forme de « manifestes »⁴⁰ ou de « déclarations »⁴¹ vient

39 Voir par exemple Barbrook and Cameron (1996) ; Winner (1997).

40 Voir par exemple Hughes (1993) et May (1992), deux textes inspirés des écrits du fondateur d'eCash David Chaum.

41 Voir par exemple la « Déclaration d'indépendance du cyberespace » de Barlow (1996), co-fondateur de

Chapitre 1. Mystique du protocole : calculer sans connaître

en corollaire de l'idée selon laquelle la liberté émergera du développement des technologies numériques, lesquelles constituent notre destin collectif (Golumbia 2016). Le thème de la liberté s'y comprend alors comme une « liberté vis-à-vis des gouvernements » qui auraient un pouvoir oppressif sur toute forme d'entité sociale, des individus jusqu'aux banques commerciales. Ce thème s'est directement cristallisé autour d'un épisode souvent mentionné par les promoteurs de Bitcoin eux-mêmes. Lorsque Bank of America, Visa, MasterCard, PayPal et Western Union isolèrent Wikileaks en 2010 en « bloquant » les dons à l'organisation (conformément à ce que la loi américaine exigeait), son fondateur Julian Assange regretta publiquement que ces entreprises soient « des instruments de la politique étrangère américaine » (AFP 2010). Ce faisant, Assange dénonça comme censeur non pas ces entreprises, mais en premier lieu l'intervention du gouvernement américain. De concert, Jon Matonis, membre fondateur de la Bitcoin Foundation, expliqua alors que Bitcoin était une solution face à l'action d'entreprises qui subiraient des pressions politiques.

Les discours et actions d'inspiration cyberlibertarienne sont mobilisés par un large spectre d'acteurs ; il serait périlleux de chercher à les énumérer exhaustivement. Golumbia remarque que différents réseaux véhiculaient ces inspirations par la promotion de Bitcoin : des figures emblématiques de l'industrie numérique et de la Silicon Valley⁴², des « think tanks » qui développaient des thèmes libertariens comme le Cato Institute, the Heartland Foundation, the Mises Institute, des mouvements comme le Tea Party ou des figures politiques comme Ron Paul ou Rand Paul. Une forme comparable d'alliance d' « intérêts politiques » a été mise en évidence par Benquet et Bourgeron (2021). Ces sociologues ont montré, en analysant les financements des camps du « Leave » et « Remain » dans le cadre de la campagne du Brexit, que les think tanks libertariens avaient activement participé à soutenir le « Leave ». Concernant Bitcoin, cette alliance pourrait être comprise comme une stratégie de géants de l'industrie numérique visant à conserver leur « pouvoir privé sur l'économie et les citoyens et protéger leur richesse » en « diminuant le pouvoir de gouvernement et des politiques publiques pour éviter qu'ils entravent leur domination croissante sur leurs parts de l'économie et taxent leurs obscènes quantités d'argent » (Ames

l'Electronic Frontier Foundation.

42 Comme Elon Musk, Peter Thiel, Marc Andreessen ou Ben Horowitz.

Chapitre 1. Mystique du protocole : calculer sans connaître

2015, cité par Golumbia 2016, ma traduction). Ce type d'analyse est repris par Golumbia qui interroge Bitcoin en termes de pouvoir :

*Power is one of the central subjects for political analysis, and perhaps the central subject: **who has power, who wants power**, what the perspectives those who have and want power are on **the creation and maintenance of methods for the management of power**.* (Golumbia 2016, caractères gras ajoutés⁴³)

Ce cadrage « essentialiste » du pouvoir, dans la mesure où il est pensé comme possédé, désiré et géré pour lui-même, conduit Golumbia à analyser Bitcoin comme un exemple d'alliance de mouvements de droites (souvent extrêmes). L'auteur explique que ces mouvements cherchent à éviter les entraves à l'accumulation du pouvoir, par opposition aux mouvements de gauche qui en favoriseraient une distribution égalitaire. Bitcoin serait alors un « logiciel comme programme politique » (titre de la cinquième partie de l'ouvrage) dans la mesure où il favoriserait l'accumulation du pouvoir en instanciant directement des pensées économiques et politiques associées à l'extrême droite. Golumbia pointe deux héritages : les inspirations de la science économique de l'École de Chicago de Milton Friedman, ainsi que les théoriciens du complot dénonçant (notamment) la Réserve Fédérale (banque centrale des États-Unis) comme une « banque privée » qui « vole la valeur » des citoyens. Liberté se comprend, pour ces littératures, dans le même sens que « marché libre », une « liberté vis-à-vis des gouvernements » qui auraient un pouvoir uniquement oppressif.

Golumbia analyse les liens entre ces différents courants par l'établissement d'une relation d'équivalence entre « gouvernements » et « pouvoir » d'une part, et par une opposition radicale entre « Internet » et « pouvoir » d'autre part. Cette conception est, selon Golumbia, accessible directement par les théories développées par des anarcho-capitalistes comme Murray Rothbard et David Friedman, dont les idées ont été popularisées par Ronald Reagan et Margaret Thatcher. Si Golumbia se défend de sous-entendre que tous les supporters de Bitcoin souscrivent directement à ces théories, il suggère qu'ils participent à les véhiculer dans leurs actions de promotion. Les paragraphes qui suivent précisent empiriquement la problématisation des promoteurs de Bitcoin, en s'appuyant sur la lecture de leurs écrits (et

43 Dans tout le manuscrit, les caractères gras dans les citations sont ajoutés.

d'un entretien avec un auteur porte-parole de la communauté Bitcoin en France) et d'observation de prises de parole publiques.

Le problème des autorités (et) de la valeur

Le glissement entre intermédiation technique et politique et l'opposition à l'« autorité » des « élites » financières et des gouvernements est autant un diagnostic produit par des analystes critiques, comme Golumbia, qu'un mot d'ordre brandi par de nombreux promoteurs de Bitcoin. Alors que de nombreux commentateurs voient Bitcoin comme une manière de se passer de confiance, Jacques Favier et Adli Takal Bataille défendent l'idée d'une « confiance inédite » comme « enjeux d'une monnaie sans État et sans banque » (Jacques Favier et Adli Takal 2017 : 78), résultat d'un « exploit conceptuel à l'origine du bitcoin : une confiance sans police ni garant » (ib. : 44).

La monnaie acéphale est un ouvrage hybride, vanté comme une excellente introduction à Bitcoin dans les réseaux de sympathisants français que j'ai fréquentés entre 2018 et 2020 et lu par des responsables politiques. L'ouvrage propose une analyse de Bitcoin mêlant perspective historique et explication de son fonctionnement. Les deux auteurs sont fondateurs du Cercle du Coin, la principale association qui animait ces réseaux, et porte-paroles de la « communauté Bitcoin » auprès des pouvoirs publics au moment de l'enquête. Je me suis fait recommander la lecture de cet ouvrage par le président d'un groupe de travail d'une institution ministérielle sur les blockchains, auquel j'ai participé bénévolement en 2018⁴⁴. J'ai remarqué la présence de députés (de la majorité parlementaire de l'époque) à la table de ces auteurs dans le cadre de déjeuners organisés par l'association. Jacques Favier a été entendu au Parlement comme expert de Bitcoin.

L'ambiguïté de la position de ces auteurs apparaît peut-être plus nettement en lisant la quatrième de couverture de leur ouvrage publié chez CNRS Éditions, qui présente le livre comme une « première grande synthèse en français, claire et accessible, sur la nouvelle monnaie du troisième millénaire ». Cette description peut paraître étonnante alors que

⁴⁴ Ces travaux ont conduit à la publication d'un rapport intitulé « Les enjeux des blockchains » publié par France Stratégie (Toledano et Janin, 2018).

Chapitre 1. Mystique du protocole : calculer sans connaître

« monnaie » était un qualificatif largement controversé au moment de la publication de l'ouvrage (et en particulier, rejetée par la Banque de France). La maison d'édition (rattachée à l'organisme public CNRS) vantait l'accompagnement offert par Bitcoin à « Internet dans son évolution et la société dans sa décentralisation grâce à son architecture et à son registre, la blockchain », adoptant ainsi le vocabulaire et les arguments de promotion de Bitcoin déployés par les auteurs.

Avec Bitcoin, « autorité » est une notion conjuguée au pluriel pour contester la légitimité d'institutions financières et gouvernementales. Le lexique est le même que celui de Nakamoto : cette contestation s'exprime en termes de « tiers de confiance » ou d'« intermédiaires » (Favier et Takkal Bataille 2017 : 40). Les tiers de confiance doivent être évités, car ils seraient faillibles et potentiellement malintentionnés ou malhonnêtes (ib. : 44-45). Favier et Takkal Bataille indiquent qu'un gouvernement est faillible dans la mesure où son autorité n'empêche pas l'émission de fausse monnaie (ib. : 47) flouant ainsi le vendeur dans une transaction commerciale. Jacques Favier m'expliquait en entretien⁴⁵ que la confiance au sens de « tiers de confiance » ne pouvait pas se comprendre au sens de l'étymologie « fides » ou de l'anglais « *confidence* », termes qui renvoient à une dimension intime ou religieuse. Ce rapport ne serait pas le même qu'un rapport individuel à l'État ou à une banque. La confiance dans l'État ou dans une banque se comprendrait au contraire au sens de « trust » dont l'étymologie se réfère à « *tree* » (bois). Cette idée, qui suggère une forme de robustesse, serait inenvisageable dans un rapport à une institution, incertaine par hypothèse. L'auteur et militant, ancien cadre d'une grande banque française, m'expliquait qu'il ne lui semblait pas légitime d'accorder sa confiance à des institutions impliquées dans des scandales financiers comme la manipulation du Libor et qui relayaient les embargos monétaires, par exemple en empêchant leurs clients de verser de l'argent à des amis vivant dans certains pays sur liste noire, comme l'Iran.

« Autorité » problématise le rapport entre individu et la société par la monnaie, dont la valeur serait factice. Dès les premiers paragraphes de l'introduction de *La monnaie acéphale*, la Reine Elizabeth II et le Président Nicolas Sarkozy sont moqués pêle-mêle alors

45 Cet entretien a eu lieu au tout débuts de l'enquête, en avril 2018.

qu'ils affichaient en 2008, et depuis leurs pays respectifs, leur surprise de voir Lehman Brothers faire faillite. Pour Jacques Favier et son co-auteur, les positions de ces dirigeants sont au mieux naïves, sinon de mauvaise foi. Le problème venait selon eux du « système » dans lequel il ne serait pas possible d'avoir confiance étant donné que la monnaie, créée à 90% par écritures de banques privées, c'est-à-dire par inscription d'un passif à leur bilan en accordant des prêts à leurs clients (ib. : 14-15 ; 68-69), n'aurait pas de valeur à leurs yeux. Favier et Takkal Bataille évoquent « une sorte de fausse monnaie assise sur la confiance naïve des citoyens » (ib. : 70). Ce problème de valeur monétaire se traduit en pratique par la dénonciation du caractère public des monnaies (d'États) : les gouvernements, déléguant l'administration à des banques commerciales, auraient renoncé au caractère démocratique de l'administration de la monnaie. Bitcoin serait un « commun » dans la mesure où quiconque peut en devenir utilisateur (ib. : 244-246).

La solution : un protocole « autonome » de la cité pour une confiance inter-individus

En rejetant les « autorités », ces auteurs systématisent la domination institutionnelle. Le concept d'autorité comme pouvoir légitime prend racine dans la sociologie de la domination de Max Weber. Le sociologue allemand identifie trois formes idéales-typiques de dominations vues comme socialement légitimes (Weber 2014) : la domination traditionnelle (légitimée par les traditions, les coutumes, les habitudes), la domination charismatique (légitimée par le prestige social d'un individu ou d'une institution), la domination rationnelle légale (légitimée par le respect porté au droit). En définissant l'autorité par les formes de domination de certains sur d'autres (individus ou groupes), Weber place au centre de l'analyse sociologique les relations sociales. Ce sont ces relations de domination que rejettent les promoteurs de Bitcoin. Favier et Takkal Bataille invoquent « l'ancestrale méfiance de l'épargnant vis-à-vis des pouvoirs publics ou l'animosité que suscite la position exceptionnelle des banques ». Ils ne rejettent pas en bloc la notion anthropologique de « confiance », mais la réduisent à une relation entre individus : « Les hommes se font d'abord confiance l'un à l'autre. On ne recompte pas une liasse de billets

Chapitre 1. Mystique du protocole : calculer sans connaître

remise par un ami. Quand on ne partage pas une addition on dit 'je te revaudrai ça !' » (ib. : 79). Pour ces auteurs, il ne peut pas y avoir de légitimité associée à un « capital confiance » face à des établissements qui établissent des « liens de clientèle » plutôt que des relations de confiance (ib. : 79). Au contraire d'une confiance supposant une domination institutionnelle, Bitcoin permettrait de limiter la confiance à une relation inter-individus qui prend la forme de transactions. Ils expliquent :

[Bitcoin est un] système sans confiance dans le sens où il n'est nullement nécessaire de faire confiance à quelqu'un dans l'environnement proche ou lointain d'une transaction, puisque celle-ci est exclusivement garantie par le réseau et le protocole eux-mêmes, sans intervention humaine (ib.).

Tout un chacun peut manger un fruit cueilli dans la nature ou s'appuyer contre un mur sans craindre qu'il ne s'effondre : de la même manière, chacun peut former une transaction avec Bitcoin sans craindre l'intervention d'autrui. Bitcoin est imaginé comme un système « autonome » du reste de la cité. La société imaginée par les promoteurs de Bitcoin est un agrégat d'individus établissant des relations inter-personnelles. Bitcoin participe à constituer leurs relations (en l'occurrence monétaires) sans possibilité d'intervenir, de les « corrompre » :

*En définitive, qu'est-ce que l'autonomie dans Bitcoin ? Cela semble être **le principe code is law** ; le protocole obéit uniquement à son code et n'a pas besoin d'intervention extérieure et autoritaire. **La notion d'autonomie du système est primordiale en ce sens que Bitcoin se distingue, pour continuer de parler grec, de la polis qui, elle, est corruptible.** Ainsi les lois de la cité peuvent-elles être changées ou enfreintes (les tyrans se servent fort bien des lois démocratiques antérieures, les États de droit peuvent suspendre certaines garanties) et **l'ordre public même n'est essentiellement garanti que par un pouvoir central et non par les citoyens eux-mêmes, leur implication n'étant que symbolique.** (ib. : 45)*

Pourtant, certains travaux nuancent radicalement la disparition de la confiance individuelle dans des mécanismes institutionnels dépassant l'individu. Des travaux en anthropologie de la monnaie ont analysé le caractère « *trustless* » de Bitcoin comme un déplacement de la confiance dans les institutions à une confiance dans les algorithmes et les plateformes d'échanges (Maurer et al. 2013; Nelms et al. 2018). Des auteurs inspirés par les STS ont remarqué que le code pair-à-pair distribue les interactions de manière spécifique et engage

Chapitre 1. Mystique du protocole : calculer sans connaître

des formes de confiance spécifiques chez les utilisateurs (Mallard et al. 2014: 4). Ils soulignent trois effets structurants sur la confiance dans Bitcoin mis en avant par les « experts » de Bitcoin⁴⁶.

Les promoteurs de Bitcoin minimisent ces dimensions, opposant un dispositif qui ne nécessite pas de « conditions préalables à l'échange ». Traditionnellement, un individu qui utilise une monnaie accorde préalablement sa confiance, sans en être nécessairement conscient, aux institutions gouvernant cette monnaie (Aglietta 2008 ; Orlean 2009). Pour Adam Smith, c'était le « soin » que les individus apportent à leurs « intérêts » qui constituait les conditions préalables à l'échange (Smith 1776). Témoin de ce refus de penser ces conditions, Favier et Takkal Bataille qualifiait la proposition de Smith de « bibliothèque rose de l'économie ». Pour eux, l'échange est une réalité anthropologique première, et l'usage de la monnaie pour faire exister les transactions est imposé par les gouvernements, *via* le fisc, qui réclament des impôts libellés en devise légale (Favier et Takkal Bataille 2017 : 67).

Bitcoin est un dispositif régulé au sens de Durkheim, qui se distingue, aussi bien conceptuellement que méthodologiquement, des propositions de Weber concernant l'analyse de l'autorité. Le sociologue français place au cœur de son analyse la société comme entité spécifique qui doit être analysée pour expliquer les effets individuels : elle « dépasse infiniment l'individu dans le temps comme dans l'espace », et se trouve « en état de lui imposer les manières d'agir et de penser qu'elle a consacré de son autorité » (Durkheim 1895). Durkheim décline cette idée empiriquement en montrant que le suicide (d'un individu) est un fait social à part entière, résultat d'un « pouvoir de coercition » extérieur à l'individu qui s'est donné la mort (Durkheim 1897). L'autorité se comprend pour lui en termes de régulation. Pour ses promoteurs, Bitcoin est également consacré d'une autorité naturelle : son « autonomie » est attribuée aux formes de régulation produites par

46 Premièrement, une forme d' « engagement collectif » dans le partage de ressources informatiques qui sanctionne une participation explicite à la maintenance du système. Deuxièmement, une complexité technique qui participe à la résilience de l'infrastructure par la décentralisation, bien qu'elle risque de diminuer la confiance des utilisateurs dans le système. Troisièmement, une différenciation partielle entre l'élaboration du code et du « contenu » du système selon des rôles et des niveaux d'engagement en fonction des modes d'intervention.

Chapitre 1. Mystique du protocole : calculer sans connaître

son protocole qui ne souffre d'aucune intervention extérieure, ou dans le vocabulaire de Nakamoto, qui assure que les transactions ne dépendent pas d'un « tiers de confiance » (*trusted third party*) :

*[dans] le sens commun du mot [protocole] on retrouve « l'ensemble de règles » et surtout l'idée que **le protocole est la règle et en même temps ce qui fait appliquer la règle**. Et dans Bitcoin cela fonctionne remarquablement bien dans la mesure où code is law, maxime que l'on devrait étendre de la sorte : **code is law and police**, même si cela sonne moins bien. En effet, dans Bitcoin **la norme est autonome**, le protocole se suffit à lui-même et à ses utilisateurs pour conserver son intégrité. On se rapproche dès lors du sous-titre de notre livre : **Bitcoin est bien une monnaie acéphale, du fait qu'il n'admet pas de police**, ses principes intrinsèques étant censés empêcher toute malversation (par rapport à ses règles) dans ses fondements-mêmes. (Favier et Takkal Bataille 2017, italiques « code is law and police » dans le texte)*

Le protocole informatique permettrait à la monnaie d'être normative. Elle devient autonome au sens littéral : elle possède sa propre norme. Mais en plus, le protocole informatique permet d'assurer le respect de cette norme. Adli Takkal Bataille détaillait, lors d'une présentation de Bitcoin à la première édition du P2P Festival à Paris en janvier 2020 :

*Donc **Bitcoin c'est avant tout un protocole**, et ça, il faut vraiment prendre en compte cela, dans le sens où c'est un système normalisé, **un système de règles normalisé pour communiquer entre plusieurs machines, ou entre plusieurs humains**. En tout cas un protocole recoupe ce sens et c'est le cas de Bitcoin. Donc le grand B, **le Bitcoin avec un grand B c'est un protocole**, et c'est comme http, comme de nombreux autres protocoles qu'on utilise au quotidien. On les voit, on les voit pas forcément, mais en tout cas c'est **grâce à eux qu'on peut communiquer de manière normalisée**, et que vous pouvez accéder par exemple au web que ce soit depuis un appareil mobile ou que ce soit depuis n'importe quel appareil embarqué, ou un appareil qui peut avoir en tout cas accès à ces protocoles-là. (Takkal Bataille, janvier 2020)*

Le mot(-clé) « protocole » est l'un des plus utilisés dans l'ouvrage *La monnaie acéphale*, avec 154 occurrences. « Protocole » est aussi le titre d'un film qualifié de « documentaire » par son réalisateur Rémi Cussièrè. Les membres du Cercle du Coin ont organisé une projection privée en avril 2019 dans un cinéma du 6^e arrondissement de Paris, à laquelle j'ai pu assister avec d'autres membres de la « communauté Bitcoin ». Jacques Favier et Adli Takkal Bataille étaient des acteurs très présents dans la série d'entretiens qui rythme ce film

de promotion de Bitcoin. Le film donnait également un espace à d'autres analystes de Bitcoin, promoteurs revendiqués ou chercheurs qualifiés par les dirigeants du Cercle du Coin d' « observateurs » universitaires. Selon un autre membre du bureau de l'association Le Cercle du Coin, ces derniers apportaient « leur éclairage et [venaient] renforcer cette évidence que Bitcoin, ses hypothèses de départ et sa démonstration finale sont pertinents et disruptifs » (Stilmant 2019).

1.2. Instauration de la rupture épistémologique : l'autorité déléguée à un réseau d'entités passives

L'autonomie de Bitcoin est imaginée comme résultat de l'agencement produit par le protocole. Le protocole instaure une rupture épistémologique par l'objet transaction qui signifie transfert d'argent pour les utilisateurs, et source de rémunération pour les *miners*. Les premiers agissent à distance sur le réseau qu'ils prennent comme une garantie, un registre sûr, tenu par les seconds transformés en agents passifs. Cette passivation, intégrée dans le protocole de consensus, traduit différentes hypothèses sur l'espace transactionnel imaginé au travers de Bitcoin et les entités peuplant cet espace.

Autonomie et autorités sont des thèmes analysés par des auteurs intéressés par la question du pouvoir dans les années 1980 en termes de délégation et d'action à distance (Barnes 1984, Callon 1984, Law 1984a). Ces auteurs n'ont pas recours à des structures sociales en arrière plan pour expliquer l'action collective. Ils ont nourri ce qui a été appelé la sociologie de la traduction quelques années plus tard qui cherche à analyser les efforts produits pour définir la société en termes d'associations qui engagent, notamment, des dispositifs techniques par lesquels les humains résolvent leurs problèmes d'organisation avec des objets durables, notamment sous forme d'inscriptions (Latour 2005, Law 2009, Muniesa 2015). Cette perspective conduit à analyser l'innovation comme une activité politique : en cherchant à rendre certaines associations durables, les concepteurs et promoteurs de systèmes techniques font de la politique. Cette politique se lit dans une sémiotique matérielle : en associant, les systèmes techniques traduisent des énoncés en chaîne.

Chapitre 1. Mystique du protocole : calculer sans connaître

Cette analyse prend les notions vernaculaires d'autonomie, de contrôle, ou encore d'intérêts associées au concept de pouvoir comme résultat d'un travail d'association produit par les acteurs. Elle suit les préconisations de Bruno Latour, qui propose d'oublier ce concept qu'il qualifie de « malléable et vide » (Latour 1984). Le philosophe et anthropologue des sciences affirme que le pouvoir n'est pas quelque chose qu'un acteur possède ou exerce, mais le résultat d'associations qui devraient être les objets de l'analyse. Le pouvoir devient alors un objet d'enquête (un effet) qu'il s'agit d'expliquer plutôt qu'un concept explicatif (une cause). Pour Latour, le pouvoir permet au mieux de résumer les conséquences de l'action collective, pas d'expliquer ce qui la fait tenir⁴⁷. Le pouvoir devient une composition d'acteurs temporairement enrôlés dans des schèmes en fournissant leurs efforts à un projet. Plutôt qu'une structure sociale, des ensembles de personnes cherchent à définir la nature de la structure sociale et à persuader les autres de souscrire à leur définition.

Le protocole : agenceur du registre, passif des miniers

*Toute l'astuce du système [monétaire] consiste, en laissant circuler quelques billets (fiduciaires), à laisser croire que l'énorme amas de monnaie scripturale, qui n'est plus elle-même que très marginalement convertible en cette monnaie émise par la Banque centrale, a la même nature, et qu'il est lui-aussi « tangible ». **Mais tangible ou pas, même le billet de banque n'est jamais qu'un bout de dette et de papier inconvertible.** Le bitcoin n'est pas tangible avec les doigts. Mais avec un protocole informatique, **celui qui le contrôle en fait lui-même ce qui lui plaît (virement, paiement, transfert ou don)** sans avoir à demander à un tiers de le faire, ou la permission de le faire. Dans le cyberspace, **le bitcoin est tangible.** Et surtout, il est indépendant de toute relation débitrice. C'est une monnaie-valeur. (Favier et Takal Bataille 2017)*

L'autorité des institutions sur l'argent devrait être abolie pour donner à chacun le contrôle total sur ses avoirs. L'argent est cadré comme un objet qui doit être « tangible » pour que son détenteur soit capable d'agir sur lui de manière exclusive. Les utilisateurs de Bitcoin sont imaginés comme autonomes : virements, paiements, transferts ou dons relèvent de la toute puissance individuelle. Cet imaginaire dirige la conception de Bitcoin : le dispositif

47 Latour oppose le modèle de diffusion qui décrit une source de pouvoir à l'origine d'un mouvement au modèle de la traduction, avec lequel le mouvement se comprend comme une succession d'opérations d'agents en chaîne.

Chapitre 1. Mystique du protocole : calculer sans connaître

doit permettre d'agir unilatéralement, sans appel à un tiers (individu ou organisation) susceptible d'entraver les actions individuelles. Il s'oppose aux formes instituées de l'argent, dont la conversion (dans une autre devise ou dans une autre forme, comme d'un billet à une écriture comptable) suppose une institution financière habilitée pouvant ou non exécuter l'ordre que le détenteur d'argent demande (pour des raisons légales ou commerciales).

Le protocole fait de l'argent un objet tangible, un registre, que tout utilisateur peut modifier. Virement, transfert, paiement ou don sont des « transactions », des modifications du registre : ajustement du montant de bitcoins inscrit dans le registre au compte de l'utilisateur à l'origine de la transaction (débit) et à celui du destinataire (crédit). Le protocole, accessible à tout Internaute, fait de la transaction ce que John Law appelle une « action à distance » (Law 1984b) sur le registre. Le protocole est une « technique de communication sans distorsion » (ibid : 17). Law montre que ces techniques et l'action à distance sont le résultat d'assemblages sous forme de réseaux, qui permettent à des émissaires de circuler du centre à la périphérie de ce réseau de manière sécurisée. Il s'appuie sur le cas du réseau de navigation portugais, qui repose sur une série d'innovations techniques inter-reliées, permettant au pouvoir lisboète d'agir à distance par la circulation de documents, d'objets, de personnes dans le monde entier.

L'action à distance des utilisateurs sur le registre est conditionnée à la passivité des entités qui constituent le réseau, connues sous le nom de « *miners* ». C'est parce qu'elles n'interviennent pas sur les transactions qu'elles font circuler que Bitcoin garantit le « contrôle » à ses utilisateurs : les transactions y conservent leurs propriétés données par les utilisateurs, elles circulent dans un média « sans distorsion ». Le travail de Law s'inscrit dans une réflexion plus générale, au milieu des années 1980, sur les rapports entre savoir et pouvoir. Law participait à ces débats, avec d'autres figures de la sociologie des sciences et de la future sociologie de la traduction, en proposant d'étudier les méthodes de réduction de la « discrétion » dans les capacités d'action (Law 1984a : 14), allant jusqu'à la passivation d'entités. Barry Barnes participait à la discussion. Il inversait la définition weberienne de l'autorité comme « pouvoir plus » légitimité en « pouvoir moins » discrétion (Barnes

Chapitre 1. Mystique du protocole : calculer sans connaître

1984) : le pouvoir suppose une capacité à former des jugements propres et à prendre des décisions de manière discrétionnaire, à la différence de l'autorité.

Le protocole est la pièce centrale de l' « autonomie » de Bitcoin. Il désigne un ensemble de règles, d'instructions distribuées aux *miners* qui se comptent en dizaines de milliers. Chaque *miner* réplique le registre conformément à la version des autres, ce qui permet de conjuguer registre au singulier malgré ses dizaines de milliers d'instanciations simultanées dans le monde. Les *miners* sont des autorités au sens de Barnes, privées de pouvoir, c'est-à-dire sans capacité d'action discrétionnaire sur (les comptes de) chaque utilisateur. Les travaux de Barnes, portant sur les méthodes de production d'agents humains passifs, ont rencontré ceux des auteurs participant à l'élaboration de ce qui deviendra la sociologie de la traduction. Ces auteurs étendaient la préoccupation pour la réduction de la discrétion aux agents non-humains. Michel Callon proposait une forme concise : il indiquait que toute lutte implique de définir les acteurs en présence et leurs caractéristiques. Les acteurs en présence exercent une action sur d'autres en empruntant leur force par un processus en quatre étapes appelé « traduction » (Callon 1984)⁴⁸.

Cet agencement, un unique registre répliqué en autant de sites que de *miners* dans le monde entier, ainsi que la passivation des *miners* eux-mêmes, n'ont rien d'évident. Des travaux d'anthropologie des techniques ont pointé le caractère politique du cadrage des capacités des acteurs insérés dans des réseaux, irréductibles à des caractéristiques ontologiques. Madeleine Akrich propose de comprendre les objets techniques dans leur participation à des réseaux hétérogènes d'acteurs, qu'ils soient humains ou non, par l'identification des rôles qu'ils jouent et font jouer (Akrich 1989 ; 1992). L'approche anthropologique d'Akrich décrit les artefacts technologiques comme parties de longues chaînes (incluant par exemple des personnes, des produits, des outils, des machines, de l'argent). Les objets techniques ont une « force politique » dans la mesure où ils « changent des relations sociales, mais

48 Premièrement, un acteur tente de se rendre indispensable aux autres. Deuxièmement, l'acteur cherche à se positionner entre ces autres et leurs alternatives, c'est-à-dire à piéger ces autres en les transformant en autorités au sens de Barnes : c'est l'intéressement. Troisièmement, l'acteur élabore un schème liant entre elles les différentes « autorités », chacune ayant un rôle défini : c'est l'enrôlement. Les autorités forment alors un réseau d'agents passifs, qui constitue en partie l'acteur qui l'a généré. Enfin, l'acteur emprunte la force d'agents passifs en s'érigeant en leur porte-parole : c'est la mobilisation.

aussi les stabilisent, naturalisent, dépolitisent, et les traduisent dans de nouveaux médias » (Akrich 1992).

Les paragraphes suivants identifient différentes hypothèses sur le monde à partir à desquelles le protocole est vu comme clé de voûte d'un registre distribué et « autonome ». D'une part, j'analyse le protocole comme un dispositif d'intéressement et d' enrôlement pour faire apparaître quelles sont les caractéristiques qu'il attribue aux *miners* pour les coaliser et en faire un réseau d'agents passifs. D'autre part, je cherche à analyser les hypothèses des innovateurs dans le protocole de consensus, ce qu'Akrich appelle « script » (Akrich 1987). Tout objet technique est le résultat d'un processus consistant, pour des innovateurs, à inscrire leurs visions du monde dans le contenu technique d'un objet. Décrire le script d'un objet technique permet de faire apparaître des postulats, hypothèses agissant dans le monde en faisant advenir ces hypothèses en pratique. Ces hypothèses portent notamment sur les compétences ou les capacités des acteurs du réseau.

Le problème des généraux byzantins : faire calculer un réseau ouvert de calculateurs faillibles

Le protocole de Bitcoin est une solution à un problème classique en informatique connu sous le nom métaphorique de « problème des généraux byzantins », qui peut être résumé ainsi : comment s'assurer qu'un système de calcul composé de différents composants communiquant entre eux, mais chacun susceptible de faire défaut à l'ensemble, produise un calcul correct ? Dans un article de 1982, les informaticiens Leslie Lamport, Robert Shostak et Marshall Pease énoncent ce problème et les différentes manières de le résoudre en fonction d'hypothèses portées sur le système et sur ses composants (Lamport et al. 1982). L'objectif de ces auteurs est d'identifier les problèmes de « conflictualité » des informations envoyées par des composants du système de manière systématique. Pour présenter leur raisonnement et leurs résultats, ils assimilent chacun de ces composants à un « général de l'armée byzantine » qui communique avec les autres généraux au moyen de « messagers » pour élaborer un « plan de bataille commun ». Cette métaphore heuristique guide leur recherche de solutions computationnelles à un « bon fonctionnement » du

Chapitre 1. Mystique du protocole : calculer sans connaître

système, requérant que le « plan de bataille » communiqué entre généraux soit effectivement mis en œuvre. Le résumé de l'article indique :

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed. (Lamport et al. 1982 : 382)

Les solutions sont envisagées en termes algorithmiques : quel algorithme permet de faire parvenir les généraux (ou composants) à un accord (ou calcul correct du système) ? Cette question est déclinée en différentes questions en fonction d'hypothèses supplémentaires sur la nature des messages qu'échangent les généraux pour parvenir à un accord. Par exemple, dans le cas de messages « oraux », c'est-à-dire reçus par un composant sans que le composant émetteur puisse vérifier son intégrité, les auteurs montrent que deux tiers des généraux doivent être « loyaux » pour que le système fonctionne : si plus d'un tiers des généraux est composé de « traîtres » (détournés de leurs fonctions, intentionnellement ou non), les généraux loyaux (qui fonctionnent correctement) ne pourront pas parvenir à un accord (le calcul correct). La notion de « trahison » est une métaphore qui désigne le mauvais fonctionnement d'un composant, quel qu'il soit : les auteurs assimilent toute cause interne au système à un élément du système qui produirait une information non conforme à son fonctionnement attendu, que cette information soit une erreur de fonctionnement (matérielle ou logicielle) ou « volontairement » produite par un « comportement malveillant » (« *malicious intelligence* ») (ibid : 400).

Avec Bitcoin, les « composants » du système sont les *miners* ; leur calcul correspond à la mise à jour du registre avec les transactions passées dans une période de quelques minutes précédentes par les utilisateurs. Les « messages » que les *miners* échangent sont des

transactions en attente d'enregistrement, assemblées dans ce qui est appelé des « blocs ». Ces blocs circulent donc entre *miners* ; chaque bloc est un « plan de bataille » élaboré par un *miner* qui le propose aux autres pour « affronter » la mise à jour du registre. Chaque *miner*, comme chaque général, peut être loyal, c'est-à-dire ajouter des transactions réellement formées par des utilisateurs, ou chercher à corrompre Bitcoin. Le protocole est chargé de cette double injonction : permettre à quiconque de devenir utilisateur ou *miner*, quelle que soit la localisation et les intentions d'utilisation, tout en garantissant l'intégrité du registre.

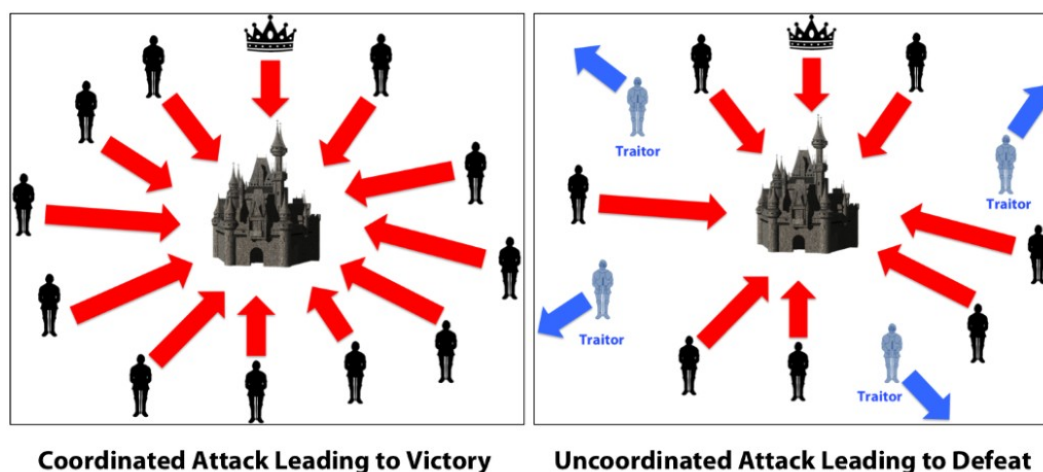


Figure 2 : Illustration de la métaphore du « Problème des Généraux Byzantins » proposée dans un article promouvant et vulgarisant le fonctionnement des cryptomonnaies (crédit : DeCoste 2019)

Un système impérativement fiable

Si la métaphore des généraux byzantins était utile à Nakamoto dans la conception d'origine de Bitcoin, elle est aussi devenue une référence régulière dans les activités de présentation ou de promotion qui détaillaient son fonctionnement technique⁴⁹. La métaphore était par exemple relayée par des représentants de la communauté Bitcoin en France. Voici ce qu'expliquait Bob, un représentant d'une association de promotion de Bitcoin⁵⁰ :

49 Par exemple mobilisée par des enseignants du MIT dans une présentation du protocole de consensus de Bitcoin (Tomescu & Devadas 2016).

50 Ce meetup, organisé dans les locaux de ConsenSys, rassemblait sur scène plusieurs des principaux représentants d'associations de promotion de Bitcoin et des cryptomonnaies en France.

Chapitre 1. Mystique du protocole : calculer sans connaître

*Alors les généraux byzantins, je ne sais pas si vous connaissez, mais c'est en gros : César est à Paris, ou à Lutèce, on va dire. **Astérix tout ça ils veulent récupérer Paris, ils sont tous éparpillés** partout et le seul moyen de remporter la victoire, c'est qu'ils soient tous coordonnés et synchronisés. **Il faut qu'ils communiquent...** Et il y a toujours un risque dans la communication que la communication soit altérée par César, par n'importe qui, qui a intérêt à justement défendre cette communication pour les empêcher de gagner. Et donc la résolution de ce problème des généraux byzantins, dans Bitcoin, c'est quoi ? **On peut faire transmettre une information quel que soit le média par lequel ça la traverse, l'information ne peut pas être altérée.** Et donc ben cela aurait permis à ces Gaulois de gagner contre César s'ils avaient pu se synchroniser avec Bitcoin. (Bob, meetup #9, avril 2019).*

La formulation de Bob témoigne de la traduction du problème des généraux byzantins par Bitcoin fait. Elle est ludique : les *miners* loyaux sont des Gaulois, les traîtres sont les Romains. Le problème qui doit être évité avec Bitcoin est l'envoi d'une information contraire à la bonne tenue du registre (information conflictuelle). Par exemple, un *miner* pourrait tenter de modifier l'historique des transactions, ou chercher à valider une transaction qui ne serait pas signée par des utilisateurs réels (afin de leur dérober des bitcoins, par exemple). Dire qu'une telle tentative est fructueuse revient à la traduire en comportement global du système, c'est-à-dire faire que l'ensemble des *miners* transforment une transaction frauduleuse en transaction authentique. Dans le langage de Lamport et de ses coauteurs, le bloc de transactions frauduleux constitue le « plan de bataille » retenu par le système dans son ensemble. Avec la métaphore de Bob, cela reviendrait à dire que les Romains déguisés en Gaulois insèrent des messages frauduleux dans les communications entre Gaulois, pour inciter les Gaulois à « fuir » plutôt qu'à se coordonner pour prendre Lutèce, et que cette fuite est effective.

Les *miners* ne sont pas distingués en termes de « loyauté » ou de trahison dans le langage usuel, a contrario du problème général posé par Lamport et ses coauteurs ou de la métaphore de Bob qui articule le problème (généraux byzantins) à sa solution (Bitcoin). Un bloc n'est pas non plus distingué en fonction de sa validité (le plan de bataille conduisant à la « victoire ») ou caractère frauduleux (le plan de bataille conduisant à la « fuite »). Les cellules grisées dans la troisième colonne du Tableau 1, qui fait correspondre les principaux objets utilisés dans la modélisation du problème des généraux byzantins (deux premières

Chapitre 1. Mystique du protocole : calculer sans connaître

colonnes de gauche) avec les objets correspondants dans la solution Bitcoin (deux dernières colonnes), matérialisent ces assimilations. Elles s'expliquent par une hypothèse implicite à Bitcoin : les blocs doivent être valides en toute circonstance (« l'information ne peut pas être altérée », selon Bob), quelles que soient les intentions des *miners*, à chaque instant. Le système doit être fiable pour que le registre conserve son intégrité. Pour Lamport et ses coauteurs, l'absolue fiabilité est une hypothèse qui implique des principes de conception spécifique, alors qu'avec Bitcoin, la fiabilité absolue est une hypothèse, une manière de poser le problème.

| Science informatique (Lamport et al. 1982) | | Bitcoin (enquête) | |
|--|---|-------------------------|---|
| Scientifique | Métaphorique | Usuel | Métaphorique (Bob) |
| <i>Functioning component</i> | <i>Loyal generals of the Byzantine army</i> | Miners | Les gaulois / Astérix |
| <i>Malfunctioning component</i> | <i>Traitor in the Byzantine army</i> | | Les romains / César |
| <i>Information</i> | <i>Message</i> | Bloc de transactions | Information |
| <i>Communication</i> | <i>Reach an agreement</i> | Inscrire un bloc | Rempporter la victoire |
| <i>Conflicting information</i> | <i>Confound the loyal generals</i> | | Empêcher la victoire |
| <i>Algorithm</i> | <i>Common battle plan</i> | Algorithme de consensus | Coordination et synchronisation pour récupérer Lutèce |

Tableau 1 : Correspondance entre désignations utilisées pour décrire Bitcoin

Des autorités sans intentionnalité ni périmètre

Les systèmes « fiables » sont un des cas analysés par Lamport et ses coauteurs. Ils pointent deux solutions à ce problème : soit chaque composant est « intrinsèquement » fiable, sinon le calcul doit être exécuté par chaque composant, puis chacun doit voter à la majorité :

*Other than using intrinsically reliable circuit components, the only way we know to implement a reliable computer system is to use **several different "processors" to compute the same result**, and then to **perform a majority vote on their outputs to obtain a single value** (Lamport et al. 1982 : 397).*

Bitcoin retient la deuxième possibilité : le vote à la majorité. Par hypothèse, il est en effet

Chapitre 1. Mystique du protocole : calculer sans connaître

impossible de garantir qu'un *miner* soit intrinsèquement fiable. Lorsqu'un *miner* constitue un bloc de transactions, les autres votent sur sa conformité. Toutefois, cette délibération n'est pas suffisante. À la différence des systèmes décrits par Lamport et ses coauteurs, les frontières du « système » Bitcoin ne sont pas définies : elles évoluent à chaque instant en fonction des connexions et déconnexions de nouveaux et d'anciens *miners*. Contrairement à une armée comptant quelques généraux véreux ou espions infiltrés envoyés par César parmi les Gaulois, les *miners* sont des Internaute. Bitcoin s'étend à Internet entier, il est exclu par hypothèse d'imposer de barrière à l'entrée du système ; un tel filtrage supposerait l'existence d'une autorité compétente, ce qui est exclu (cf sous-section 1.1).

L'organisation d'une délibération suppose de pouvoir identifier les participants pour constituer un corps électoral. Or, dans un espace ouvert comme Bitcoin, il n'est pas évident de définir une identité. L'adresse IP⁵¹, aisément multipliable artificiellement, n'est pas une solution à ce problème. Avec un vote par adresse IP, un « traître » pourrait aisément se « démultiplier » afin d'influencer la délibération en son sens⁵². Pour répondre au problème de l'unicité des votes dans le processus de délibération, Bitcoin pondère chaque vote en fonction de la puissance de calcul investie par chaque *miner* dans le réseau. À la genèse publique de Bitcoin, Nakamoto écrivai(en)t :

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU⁵³-one-vote. (Nakamoto 2008 : 3)

Le protocole identifie chaque *miner* à sa puissance de calcul, ou schématiquement, au nombre de processeurs que chacun utilise pour produire un bloc. Pour mesurer la puissance de calcul de chacun, le protocole rend l'opération d'assemblage des transactions (passées par les utilisateurs en un bloc) artificiellement coûteuse. Ce coût répond directement, et

51 Une adresse de l'*Internet Protocol* (IP) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique sur Internet.

52 Un même Internaute peut artificiellement se connecter à un même réseau (ou plus généralement, à un même serveur) en utilisant différentes adresses IP, y compris simultanément. Par conséquent, l'adresse IP ne permet donc pas d'identifier de manière certaine un individu ou une organisation.

53 Central Processing Unit, ou « processeur » en français.

exclusivement, à ce problème d'identité. Sans ce problème d'identité, l'opération d'assemblage des transactions en un bloc serait rudimentaire. Pour le résoudre, le protocole inclut dans le processus de constitution d'un bloc l'exécution d'un algorithme dit de « hashage » dont le résultat est un « *hash* », une suite de caractères. L'idée est la suivante : un *miner* collecte des transactions en attente de validation (qui circulent par le protocole). Ces transactions, ainsi que le numéro du dernier bloc ajouté au registre, sont les données d'entrée de l'algorithme de hashage. Dans le même temps, le protocole impose aux *miners* de produire des *hashs* commençant par un certain nombre de zéros. Par conséquent, si le *hash* obtenu ne commence pas par ce nombre imposé de zéros, le *miner* doit recommencer l'opération de hashage⁵⁴. Le premier *miner* qui obtient un *hash* satisfaisant diffuse le « bloc » (les transactions et le *hash*, ou le « message » dans le vocabulaire de Lamport et de ses coauteurs) à l'ensemble des autres *miners* qui l'ajoutent individuellement à leur version du registre, mettant individuellement à jour « le registre » distribué.

La transaction, matière première d'un processus de validation rémunérateur

Le coût en énergie électrique de cette identification par la puissance de calcul est rémunéré par le protocole : le premier *miner* qui propose un bloc correct obtient la récompense associée à un bloc. Cette rémunération comporte deux composantes : d'une part, le protocole prévoit une rémunération fixe (une forme d'émission monétaire, codée à l'avance), et d'autre part, les frais de transactions payés par les utilisateurs. Cette (double) rémunération est la clé de voûte de l'enrôlement des *miners* comme composants d'un réseau fiable. Sans cette rémunération, l'organisation de la délibération, payante (en énergie électrique) pour chaque *miner* contraint d'exécuter l'algorithme de hashage après chaque ajout de bloc, n'attirerait que des militants. Or, aucune hypothèse ne porte sur l'intentionnalité des *miners*, sinon celle de l'appât du gain monétaire, en bitcoin : plus un *miner* investit de puissance de calcul dans le protocole, c'est-à-dire plus il exécute

54 L'algorithme de hashage prévoit un paramètre appelé « *nonce* ». Ce chiffre permet, à partir d'un même ensemble de données (en l'occurrence, de transactions), de faire varier le « *hash* » produit par l'algorithme.

Chapitre 1. Mystique du protocole : calculer sans connaître

l'algorithme de hachage, plus ses chances de trouver un *hash* satisfaisant le premier sont élevées. Autrement dit : la rémunération est proportionnelle à la puissance de calcul dépensée.

Ainsi, la constitution d'un bloc de transactions prend un sens tout à fait différent de celui de participation à la sécurisation du registre : il s'agit d'un investissement en matériel informatique et en électricité rémunérée en bitcoins. La partie du protocole qui organise la coordination des *miners* est un algorithme de consensus dit de type « preuve de travail », le travail correspondant à l'effort produit pour trouver un *hash* satisfaisant.

Le protocole instaure une compétition entre *miners* selon un mécanisme adaptatif à deux titres. D'une part, plus le nombre de *miners* (mesurés en puissance de calcul totale) est important, plus le protocole augmente le nombre de zéros à trouver en tête de *hash*, de manière à augmenter la puissance de calcul nécessaire à la constitution d'un bloc pour les mêmes chances de réussite. Ainsi, le protocole maintient la création d'un bloc toutes les dix minutes : la difficulté est inversement proportionnelle au nombre de *miners* connectés au réseau. D'autre part, les frais de transactions instaurent un marché de la transaction à valider : plus la demande de transactions à valider est importante, plus les *miners* pourront choisir parmi les transactions proposant les commissions les plus avantageuses. Les dirigeants du Cercle du Coin expliquent que cette compétition vise à faire « combattre » les *miners*, à organiser l'escalade de la bataille en termes de puissance de calcul :

*Comme nous l'avons vu auparavant, le réseau nécessite un consensus décentralisé pour que tout le monde puisse statuer sur une version de la blockchain. Ceci implique qu'un pair ait le droit de valider un bloc parce qu'il a prouvé qu'il a fourni un travail au sein du réseau. **La concurrence entre les mineurs permet, elle, de faire en sorte que les mineurs ne soient pas tous les mêmes et qu'ils combattent en accroissant leur puissance de calcul pour augmenter la sécurité du réseau. Cette preuve de travail est le seul moyen de limiter la tricherie dans le réseau.** (Favier et Takkal Bataille 2017)*

La sécurité du réseau dépend directement de cette course à la dépense énergétique. Elle est la limite à « la tricherie dans le réseau », obtenue en intéressant et en enrôlant de nouveaux *miners*. En effet, plus la somme de la puissance de calcul de tous les *miners* sera

Chapitre 1. Mystique du protocole : calculer sans connaître

importante, plus il sera difficile pour un *miner* qui ne serait « pas loyal » d'inscrire un bloc frauduleux. Pour cela, il devrait contrôler plus de la moitié de la puissance de calcul du réseau, de manière à être majoritaire dans le vote d'ajout d'un bloc organisé à la majorité (cf *supra*). Ce type d'inscription est appelé « attaque à 51 % » dans le langage de Bitcoin. Ainsi, l'augmentation de la puissance de calcul totale rend plus difficile l'exercice de la « discrétion » sur le système, dans le langage de Barnes et de Law. Autrement dit, la compétition organisée par le protocole passive les *miners*, elle en fait des autorités qui agissent conformément aux règles du protocole.

Les paragraphes précédents ont identifié différentes hypothèses embarquées dans le protocole, nécessaires pour faire tenir le registre distribué de manière « autonome ». Le monde est abordé comme un espace ouvert peuplé d'individus, réunis par le protocole comme seule institution d'un ordre social. Le protocole est imaginé comme régulation des rapports de force entre individus, supposés s'exprimer de manière libre, pour garantir la sécurité du registre en réseau. La seule délibération ne suffit pas à se prémunir de la « trahison », qui peut être généralisée à plus de la moitié des *miners*. La liberté (d'intention et) d'action est en effet une hypothèse prolongée par le protocole. La compétition, rendue possible par le caractère adaptatif du protocole, vise à faire agir les *miners* dans leur « intérêt » économique individuel, calculé comme un rapport entre un coût (matériel et énergie électrique) et un bénéfice (la rémunération en bitcoins, émise par le protocole et par les frais payés par les utilisateurs).

L'instauration d'un mécanisme de gouvernance « autonome » fait des transactions des objets hybrides : pour les utilisateurs, elles signifient transferts (ou dons, ou virements, etc.) d'argent ; pour les *miners*, elles signifient objets de « travail » dans laquelle investir. Le protocole opère une séparation nette entre la production de la transaction elle-même, impliquant deux utilisateurs, et sa validation par des *miners*. Il fait de la validation des transactions une activité des *miners* vis-à-vis d'eux-mêmes, auto-centrée sur un calcul économique, qui ne dépend pas des transactions elles-mêmes, tout en produisant des résultats valables pour tout un « système » composé de tous les *miners* et de tous les utilisateurs. La totalisation des transactions, ou leur inscription au registre, est indépendante

du contenu de la transaction. Il s'agit là d'une manière d'analyser le projet politique des promoteurs de Bitcoin : déposséder les banques et autres institutions d'une « autorité centrale », au sens de pouvoir « discrétionnaire » sur les transactions.

1.3. Le protocole : technique de neutralisation du pouvoir de gouvernants sur des gouvernés

La sécurisation du registre passe par une rupture épistémique dans l'objet « transaction » : la signification du transfert d'argent pour les utilisateurs est inconnu pour les *miners* administrateurs du réseau qui ne voient qu'un investissement. Les paragraphes qui suivent proposent une autre lecture de cette rupture mise en évidence à la section précédente en termes de sécurisation : le protocole informatique est une technique de neutralisation de toute forme de pouvoir qui pourrait compromettre l'intégrité d'un registre de transactions distribué. Les éléments présentés à la section précédente sont confrontés, de manière successive et énumérative, à différentes théories du pouvoir identifiées à partir de la lecture du parcours du théoricien du pouvoir Steven Lukes (1974, 2004). Le protocole de consensus intègre des hypothèses anthropologiques spécifiques, comme pour toute conception du pouvoir, qui apparaissent ici comme des choix de conception. Notamment, cette neutralisation témoigne d'une angoisse pour toute forme de pouvoir susceptible de limiter la toute puissance individuelle. Lukes et Nakamoto partagent un intérêt commun pour le pouvoir : le premier cherchait à l'analyser, le second à le conjurer.

Conjurer tout pouvoir sur les transactions

[R]ien n'oblige une banque à accepter de recevoir une personne qu'elle ne souhaite pas voir. (Favier et Takkal Bataille 2017)

Pour les auteurs de *La Monnaie Acéphale*, le bitcoin serait une « valeur numérique » disponible sans compte en banque. Bitcoin serait « inclusif » en permettant à tous les « non bancarisés », « précaires » ou victimes de « délits de faciès » de disposer d'un compte. À la différence des banques exerçant un pouvoir discrétionnaire, spécifique à chaque individu,

Chapitre 1. Mystique du protocole : calculer sans connaître

Bitcoin favoriserait l'inclusion bancaire. Cette signification des transactions est tout à fait étrangère aux *miners*, qui voient les transactions comme des objets à inscrire contre rémunération. Parce qu'ils ne voient pas les significations d'usage des transactions, les *miners* n'exercent pas de pouvoir sur elles.

L'existence du pouvoir est problématique pour les concepteurs de Bitcoin. Il est potentiel : il peut être exercé à tout moment par les institutions publiques ou privées ; en particulier, il menace la liberté d'échanger. Le protocole de consensus est une solution générique à ce que Bitcoin cadre comme une épée de Damoclès. Pour s'en prémunir, Bitcoin se veut être une solution radicale, systématique, à toute forme de pouvoir qui pourrait être exercée sur le registre de transaction. Il doit être « sûr », inattaquable, autonome, quelle que soit la situation. Durant l'enquête, j'ai entendu plusieurs fois que Bitcoin, comme Ethereum, étaient capables de survivre à tout événement, y compris « une troisième guerre mondiale ».

Le cadrage des *miners* est tout aussi générique (et pessimiste) : leur « trahison », dans le vocabulaire du problème des généraux byzantins, doit être évitée par leur enrôlement, leur passivation en autorité au service de la sécurité du réseau. Cet enrôlement n'est pas situé, comme l'est celui des coquilles Saint-Jacques décrit par Michel Callon (1984). Ici, l'enrôlement est imaginé en termes théoriques et généraux, en réponse à la généralisation de la « trahison » de chacun vis-à-vis de l'intégrité du registre. Individu malintentionné (ou *miner* « traître ») et institution sont logées à la même enseigne : des ennemis en puissance de la sécurité du registre.

Satoshi Nakamoto et Steven Lukes sont préoccupés par le problème du pouvoir. Le premier cherchait à le conjurer avec Bitcoin, le second cherche à l'expliquer depuis les années 1970. Steven Lukes, sociologue à la London School of Economics, est un acteur majeur et analyste des débats qui se sont déployés autour de ce concept du milieu du XX^e siècle au début du XXI^e siècle. Il les restitue dans son ouvrage *Power A Radical View* (Lukes 1974, 2004 ; plus loin « PRV »). Dans la version d'origine de PRV (Lukes 1974), l'auteur posait la question « comment penser au pouvoir théoriquement, et comment l'étudier empiriquement ? ». Plus de trois décennies plus tard, il resituait le débat dans lequel il

s'engageait lors de la première publication en discutant les réactions que ce dernier a suscitées, et affinait sa conception du pouvoir. Les paragraphes qui suivent observent le protocole Bitcoin au prisme des théories discutées par Lukes. Puisque Bitcoin problématise les « autorités » qui gouvernent les relations, les utilisateurs de Bitcoin sont considérés comme « gouvernés ».

L'exercice du pouvoir comme domination de gouvernants sur des gouvernés

En 1974, Lukes participait à un débat entre sociologues et politistes qui pensaient le pouvoir en termes d'impuissance, de domination, et de lien entre les deux notions. À partir des années 1950 et notamment aux États-Unis, une série de travaux expliquait la domination de populations impuissantes par les positions hiérarchiques d'élites dans les organisations modernes (États, entreprises) détenant les moyens centralisés d'information et de pouvoir⁵⁵.

Des politistes de Yale contestèrent l'explication de la domination par la hiérarchie, relevant selon eux de l'hypothèse plutôt que de l'analyse empirique (Dahl 1958)⁵⁶. Ils préféraient poser la question de la distribution du pouvoir, exercé comme décisions dans un espace politique constitué de gouvernants et de gouvernés. Cette approche conduisait à identifier le pouvoir à son exercice plutôt qu'à une position (hiérarchique) permettant de l'exercer, à l'examiner dans des contextes locaux selon la question de recherche « combien de pouvoir ont les acteurs pertinents selon les problèmes clés en ce lieu et à ce moment-là ? ». Le pouvoir était alors pensé comme intentionnel et actif, il était « mesuré » par son exercice dans des situations de prise de décision. Ces travaux dits « pluralistes » cadraient le pouvoir selon ce que Lukes appelle une « première dimension » du pouvoir. Ils montraient que le pouvoir était distribué de manière pluraliste en fonction d'acteurs (plutôt que concentré dans une « élite dirigeante ») qu'ils soient individus ou groupes d'intérêts, différents selon les espaces et les problèmes. Les pluralistes analysaient le pouvoir par son exercice, limité à

55 Voir par exemple Hunter (1953) et Mills (1956).

56 Les mêmes proposent une méthodologie pour tester cette hypothèse avec une méthodologie spécifique (Dahl 1961).

Chapitre 1. Mystique du protocole : calculer sans connaître

ses éléments « mesurables » par les « décisions concrètes » prises par les gouvernants.

En réaction à la proposition des pluralistes, des auteurs pointaient que le pouvoir ne se reflète pas uniquement dans des décisions concrètes : à l'échelle d'une société (« communauté »), une personne ou une association peut limiter la prise de décision à des sujets non controversés en influençant les valeurs, les procédures politiques et les rituels sans que cet exercice soit forcément mesurable (Bachrach & Baratz 1962). Lukes voit une « deuxième dimension » du pouvoir proposée par les contradicteurs des pluralistes : dans la mesure où une personne ou un groupe crée ou renforce consciemment ou inconsciemment des barrières structurant ou prévenant des conflits politiques, cette personne ou ce groupe a du pouvoir. Cette dimension pointe les « non-décisions » qui limitent le périmètre de la prise des décisions (observables), consciemment ou pas, par exemple en excluant de potentiels adversaires. Ce faisant, elle inclut les problèmes potentiels, que les « non-décisions » empêchent de devenir concrets, dans ce qui compte comme problème politique. Les problèmes « clés » peuvent être concrets ou potentiels. À contrario pour les pluralistes et Dahl, un problème politique est fixé dans les frontières du système politique observable.

Les promoteurs de Bitcoin utilisent des concepts proches de ceux mobilisés par ces théories du pouvoir. Bitcoin est une réponse à une forme de domination : Bitcoin est imaginé en opposition à la domination des élites financières sur les échanges monétaires et financiers, définis comme opérations ne devant relever que de la toute puissance individuelle. Selon cette vue, les citoyens sont soumis à ce qu'ils appellent des « autorités » et des « intermédiaires ». À la manière des pluralistes, les promoteurs de Bitcoin voient ce pouvoir comme un exercice intentionnel et actif (bien que potentiel) au travers d'opérations concrètes qu'ils dénoncent, comme la possibilité d'ouvrir un compte en banque sans discrimination et « délit de faciès », ou la pratique de l'embargo vers des pays sous sanction. Ce pouvoir s'exprime également dans ce que les contradicteurs des pluralistes appellent des « non-décisions ». En restant fermées aux pays des Suds, les institutions financières occidentales empêchent leur développement économique. Cette dénonciation est une réponse des promoteurs de Bitcoin aux analyses de Bitcoin en termes d'objet financier spéculatif.

Les intérêts, dans l'analyse (de Lukes) et dans la neutralisation (par Bitcoin) du pouvoir

L'opposition des pluralistes à l'analyse du pouvoir en termes de position hiérarchique repose sur l'identification des intérêts des citoyens d'un système politique. Les intérêts sont pensés comme des préférences politiques exprimées de manière comportementale (donc observables) dans les prises de décision sur des sujets-clés. Leurs critiques Bachrach et Baratz ont une conception plus large des intérêts. Si les « règles du jeu » placent ceux qui en bénéficient dans une position favorable pour faire valoir leurs intérêts, elles ne représentent pas les seuls moyens de les faire valoir. Bachrach et Baratz considèrent non seulement les préférences exprimées au travers de comportements politiques au sens institutionnel, mais aussi dans les comportements de ceux qui sont exclus du système politique au sens de ses mécanismes institutionnels.

La sécurisation de Bitcoin donne aux intérêts un rôle théorique central et tout à fait indépendant d'institutions contestées. Les promoteurs de Bitcoin qualifient l'intérêt des utilisateurs de manière absolue, en termes de liberté (potentiellement empêchée) : jouir de la monnaie ou d'actifs financiers. En d'autres termes, l'intérêt des utilisateurs de Bitcoin est un rapport de propriété exclusive sur les avoirs qui exclut toute possibilité d'action de quiconque autre que le propriétaire. Les notions de solidarité ou de redistribution à l'échelle du groupe constitué des utilisateurs de Bitcoin n'existent pas, en dehors de ce que décide le protocole qui, seul, incarne la gouvernance imaginée du système.

En 1974, Lukes s'inscrivait à la suite des deux premières dimensions du pouvoir. Il déplaçait le problème de la mesure du pouvoir exercé (et de sa « distribution ») à la nature « véritable » (*real*) des intérêts des acteurs. Il proposait de définir le pouvoir selon l'assertion suivante : « A exerce du pouvoir sur B quand A affecte B de manière contraire aux intérêts de B »⁵⁷. Il prolongeait ainsi l'analyse du pouvoir comme exercice entre une personne qui l'exerce et une personne sur qui il est exercé. Lukes critiquait le penchant

57 En version originale : “A exercises power over B when A affects B in a manner contrary to B's interests”.

Chapitre 1. Mystique du protocole : calculer sans connaître

comportementaliste des deux premières dimensions qui ramenait les problèmes à l'origine de l'exercice d'un pouvoir au paradigme de la décision, la limitation aux conflits observables, et l'ignorance des vrais intérêts. Il refusait de réduire les intérêts à l'expression de revendications ; en leur absence, il n'était pas possible de considérer qu'un « consensus authentique » soit atteint, ce qui revenait à ignorer les « conflits latents »⁵⁸.

Bitcoin conçoit les intérêts comme Lukes les analysait : un rapport de continuité dans lequel s'exerce le pouvoir comme domination. Pour neutraliser le pouvoir de gouvernants en puissance sur tout un chacun, c'est précisément un objectif de « consensus » qui est fixé au protocole informatique ; on parle de « protocole de consensus ». Ce faisant, le protocole élimine les conflits latents, en dissociant les intérêts des gouvernants et des gouvernés. Bitcoin organise une rupture épistémique entre les deux groupes, chacun ayant un rapport de connaissance spécifique à l'objet transaction, que Bob illustre avec la métaphore de la lettre et de l'enveloppe qui distingue le contenant du contenu :

*Sur le protocole de consensus, trustless, ça repose sur ces méthodes de preuve de travail où au final, **la motivation de la personne qui va valider les transactions, qui va faire ce travail, qui va fournir cette preuve de travail pour apporter cette confiance sur les blocs sur le réseau Bitcoin, son intérêt n'est pas du tout... n'est pas du tout placé sur le contenu des transactions.** En fait, on s'en fiche. C'est juste un postier, lui il veut juste enregistrer des timbres, ce qu'il y a dans la lettre il n'en a rien à faire.* (Bob, meetup #9, avril 2019)

La métaphore du courrier est classiquement utilisée pour expliquer le fonctionnement de la circulation des paquets Internet. Les routeurs sont souvent décrits comme des aiguilleurs des paquets, des postiers qui transmettent le paquet à l'aiguilleur suivant. La différence importante avec Bitcoin est l'adressage de la transaction : elle est destinée au « tout » social

58 “In summary, the three-dimensional view of power involves a thoroughgoing critique of the behavioural focus of the first two views as too individualistic and allows for consideration of the many ways in which potential issues are kept out of politics, whether through the operation of social forces and institutional practices or through individuals' decisions. This, moreover, can occur in the absence of actual, observable conflict, which may have been successfully averted – though there remains here an implicit reference to potential conflict. This potential, however, may never in fact be actualized. What one has here is a latent conflict, which consists in a contradiction between the interests of those exercising power and the real interests of those they exclude. These latter may not express or even be conscious of their interests, but, as I shall argue, the identification of those interests ultimately always rests on empirically supportable and refutable hypotheses.” (Lukes 2004 : 28 ; italiques dans le texte d'origine)

qui la reconnaît par son inscription, alors que les paquets Internet sont adressés à un destinataire distant particulier. Le registre fait se rencontrer les *miners* et les utilisateurs et matérialise le « consensus » reproduit à l'ajout de chaque bloc.

L'agentivité et la structuration par les intérêts individuels

En faisant reposer le concept de pouvoir (comme exercice entre deux individus dotés d'intérêts homogènes) sur celui d'intérêt (individuel), Lukes déplaçait sa question d'origine (« comment penser au pouvoir théoriquement, et comment l'étudier empiriquement ? ») vers des questions propres à l'identification des intérêts des acteurs en présence. Ces questions se lisent dans les deux « difficultés » majeures que Lukes identifiait lui-même. D'une part, il reconnaissait qu'il était compliqué d'analyser le « contrefactuel », c'est-à-dire que les intérêts des acteurs ne sont pas ceux qui apparaissent de manière évidente, brouillés par l'exercice d'un pouvoir⁵⁹. L'objet d'enquête devient alors l'« authenticité » d'un consensus, lequel est évalué à la lumière des « vrais » intérêts des acteurs, c'est-à-dire analytiquement isolés de l'« exercice » du pouvoir. Pour répondre à cette question, Lukes invitait l'analyste à s'interroger sur ce que les acteurs auraient fait en l'absence de cet exercice (« *would have done otherwise* »). D'autre part, Lukes suggérait d'identifier les « mécanismes » d'exercice du pouvoir par leurs effets. Il pointait trois problèmes : prendre en compte l'inaction autant que l'action, considérer les réactions inconscientes, et attribuer le pouvoir aux groupes autant qu'aux individus.

La définition du pouvoir retenue par Lukes dans les années 1970 fait des intérêts une « notion irréductiblement évaluative » : leur définition suppose une position politique et morale⁶⁰. L'importance théorique accordée aux intérêts est située dans des débats intellectuels et politiques qui animaient les sciences sociales et la théorie politique de

59 Lukes donne comme exemple le cas d'habitants de Gary dans l'Indiana, lesquels toléraient l'activité productive de l'entreprise locale malgré les dangers induits sur leur santé (Crenson 1971)

60 Lukes juge que chacune des dimensions du pouvoir a sa propre politique. Il les désigne respectivement « libérale », « réformiste » et « radicale » ; le dernier qualificatif, donné à cette « troisième dimension », est repris dans le titre de l'ouvrage.

Chapitre 1. Mystique du protocole : calculer sans connaître

l'époque⁶¹. Lukes participait au débat concernant la primauté à accorder à la structure ou à l'agentivité dans l'analyse en sciences sociales. Le geste analytique consistant à porter l'attention sur ce que les acteurs auraient fait en l'absence de pouvoir rejoignait la question de l'agentivité que Lukes définissait comme possibilité « d'agir différemment » (Lukes 1977) : le pouvoir existe si l'agent a la capacité de choisir d'agir différemment dans les circonstances de l'analyse. Des critiques lui reprochaient de défendre une position volontariste, malgré son intention de dépasser l'opposition classique entre volontarisme et déterminisme : en se concentrant sur l'exercice du pouvoir, Lukes oublierait le pouvoir propre à la structure sociale⁶².

Bitcoin agence les *miners* par la recherche d'une récompense : l'émission d'un nombre d'unité fixé par le protocole. La récompense est obtenue par le premier *miner* qui propose un « bloc » de transactions aux autres *miners* que les autres ajoutent. Il s'agit du seul « vrai » intérêt de chaque *miner*. Si le bloc proposé n'est pas conforme (c'est-à-dire que le *miner* en question « triche » ou n'est « pas loyal »), les autres *miners* ne l'ajoutent pas au registre et l'énergie dépensée par le premier est, à coup sûr, perdue. Autrement dit, les *miners* n'ont aucune possibilité d' « agir autrement », comme le suggère Lukes. Leur agentivité repose sur un principe de concurrence qui les incite à résoudre un problème cryptographique (algorithme de hachage) qui participe directement à construire la raison

61 La tradition conceptuelle amorcée par les pluralistes répondait aux interprétations marxistes du pouvoir en termes de « classe dirigeante » qui centrait l'analyse sur les conflits d'intérêts entre élites dirigeantes et populations. La critique des pluralistes, pointant la limitation de la prise de décision à des sujets non controversés, faisait écho au concept marxiste d'idéologie, en particulier l'idée développée par Gramsci de sécurisation du consentement à l'exploitation capitaliste (Gramsci 1971). Selon Lukes, une première interprétation de Gramsci est que la culture ou l'idéologie constitue le mode de règle de classe par les moyens du monopole bourgeois sur les appareils idéologiques (Femia 1981). Le consentement est alors un état psychologique qui peut varier de l'adhésion volontaire à la soumission à la seule forme de société viable. Une seconde interprétation fait de l'hégémonie une base matérielle de coordination des intérêts réels ou matériels des groupes dominants et subordonnés (Przeworski 1985). Si l'idéologie oriente les gens dans leurs vies quotidiennes, elle doit exprimer leurs intérêts et leurs aspirations. Le consentement qui sous-tend la reproduction des relations capitalistes ne consiste pas en états mentaux individuels mais dans des caractéristiques comportementales des organisations, et ne devrait pas être expliqué en termes psychologiques ou moraux : le consentement est cognitif et comportemental. Il s'exprime quand les gens choisissent des cours d'action et les suivent en pratique. Le consentement correspond alors aux « vrais intérêts » de ceux qui consentent.

62 Voir par exemple Layder (1985) qui renvoie dos-à-dos la proposition de Lukes et la théorie de la structuration de Giddens en proposant de voir le pouvoir comme un concept d'analyse de l'agentivité autant que de la structure.

d'être de Bitcoin, un intérêt collectif qui dépasse chacun :

*Finally, **grâce à un consensus décentralisé fondé sur la concurrence du minage par résolution du problème cryptographique, tous les acteurs du réseau se mettent au diapason.** Cette technique de validation est nécessaire pour permettre à tout le système (à tous ceux qui participent au réseau, à tous ceux qui ont téléchargé le registre) de **s'harmoniser avec une seule et même base de données.** Bitcoin réussit avec brio à obtenir un consensus de manière décentralisée et permet ainsi de **conserver la fiabilité de sa base de données et l'immutabilité des écritures de ses transactions.** (Favier et Takkal Bataille 2017)*

Cet extrait dit que les acteurs du réseau sont « mis au diapason », « harmonisés » autour d'une « seule et même base de données », par le protocole qui est « fondé sur la concurrence ». Le registre de transactions matérialise l'intérêt collectif, une forme de téléologie de « l'immutabilité des écritures de ses transactions ». Ce champ lexical d'un ordre unidimensionnel partant d'intérêts individuels pour former un intérêt collectif est aussi souvent formulé en termes d' « alignement ». Un des auteurs expliquait lors d'une intervention publique dédiée à Bitcoin sur la scène du premier « P2P Festival » parisien :

***L'alignement des intérêts** ça veut dire que tout Bitcoin et la cryptomonnaie fonctionnent sur une logique d'alignement des intérêts, qui est extrêmement, finalement, **importante pour réussir à faire en sorte que tout le monde aille dans la même direction et soit impliqué dans le développement du réseau, au mieux, parce qu'il a tout intérêt à ce que le réseau se porte le mieux possible.** (Adli Takkal Bataille, P2P Festival, janvier 2020)*

La notion d'alignement des intérêts articule la robustesse (« immutabilité ») de la seule « structure » de l'ordre social (du « système ») avec l'agentivité des *miners* contraints dans leur capacité à agir selon les règles du protocole.

Capacité et « pouvoir de » : la limite matérielle de la puissance de calcul

Trente ans après son premier ouvrage, Lukes revenait sur son analyse de 1974⁶³. En 2004, il

63 Différentes conceptualisations du pouvoir ont été proposées entre-temps. En discussion avec elles, Lukes souligne différentes « erreurs et imprécisions » dans sa proposition initiale, en particulier la conception du pouvoir comme exercice.

Chapitre 1. Mystique du protocole : calculer sans connaître

reconnaissait que s'intéresser à l'exercice du pouvoir asymétrique entre acteurs dotés d'intérêts unitaires offrait une réponse partielle au problème du pouvoir. Maintenant sa volonté de proposer une cartographie et une théorie générale, il redéfinit le pouvoir comme capacité des agents à faire advenir des « effets significatifs » selon leurs propres intérêts ou en affectant ceux des autres. Plutôt que de parler d'exercice du pouvoir, Lukes propose désormais de s'y intéresser, de manière générale, en termes de capacité ou de faculté des agents. Il définit alors le pouvoir comme un « concept dispositionnel⁶⁴, comprenant une conjonction d'énoncés conditionnels ou hypothétiques spécifiant ce qui se produirait dans une série de circonstances si et quand le pouvoir est exercé. » (ib. : 63).

En définissant le pouvoir comme capacité, Lukes confirme une intuition épistémologique : le pouvoir se référerait à des agents (leurs capacités), et pas à des structures, des relations ou des processus qui ne pourraient pas être caractérisés par des agents. L'enjeu, similaire à celui de 1974 mais formulé plus généralement, devient celui de la comparaison entre pouvoirs : s'il est facile de dire qu'un agent peut faire advenir des effets significatifs, comment les comparer à ceux provoqués par d'autres agents ? Lukes reconnaît que l'analyse repose toujours sur des jugements moraux dans la mesure où elle implique d'évaluer la signification de ce que les agents sont capables de produire en dernière analyse. Sous l'angle de la capacité d'acteurs à faire advenir des effets significatifs, Lukes étend sa définition du pouvoir au « pouvoir de » ou « *potentia* » dans le langage de Spinoza, un sens très général désignant le pouvoir des choses en nature, y compris des personnes qui existent et agissent. Le « pouvoir sur » d'autres ou « *potestas* », recouvrant la notion de « domination », qui a guidé sa réflexion dans les années 1970, se comprend comme un cas particulier du sens précédent.

Alors que la question de la domination posée en termes de « pouvoir sur » équipe la critique de Bitcoin vis-à-vis des institutions de la monnaie, la question de recherche de Lukes reformulée en termes de « pouvoir de » équipe positivement la proposition de Bitcoin : « comment la conformité volontaire à la domination est-elle sécurisée par les

64 Le Larousse en ligne définit l'adjectif dispositionnel ainsi : « Dans la terminologie de l'empirisme logique, se dit d'un terme qui ne décrit pas un caractère immédiatement observable d'un objet, mais une régularité manifestée par des événements ou des comportements dans des conditions appropriées. »

dominants ? ». Les dominants de Bitcoin imposent le protocole par la puissance de calcul. Celui-ci n'a pas de garant : son existence n'est prolongée que dans la mesure où l'ensemble des *miners* l'exécutent en même temps. Cette réduction de la capacité d'action, ou manière d'exprimer un pouvoir d'inscrire, est généralisé : les institutions financières comme les États ont pour seul moyen d'accès matériel sur le réseau de mobiliser de la puissance de calcul.

La capacité d'action de quiconque sur le réseau est limitée à deux opérations : proposer un bloc de transaction, ou inscrire un bloc de transaction. Proposer un bloc non conforme ne permet pas de faire advenir des « effets significatifs » : il serait rejeté par l'ensemble des autres *miners*. Ces derniers n'ont eux-mêmes pas intérêt à ajouter un bloc frauduleux, bien qu'ils aient cette capacité d' « agir autrement ». Théoriquement, les *miners* peuvent chercher à se coordonner (autrement que par le protocole de consensus) pour inscrire un bloc frauduleux ; il leur suffit de réunir plus de 51 % de la puissance de calcul du réseau. Mais cette action collective n'aurait pas d'effet significatif conforme à leur intérêt : même s'ils se créditaient de nombreuses unités de bitcoin, la détection de la fraude dans les minutes qui suivent par les passionnés attentifs et par les outils de suivis du réseau conduiraient à un effondrement du cours de l'unité bitcoin, et à un effondrement de sa valeur dans toute unité autre qu'elle-même.

Conclusion intermédiaire. Gouverner par le calcul distribué : inscrire sans connaître

Cette section analyse Bitcoin comme un dispositif de gouvernement des relations *via* Internet. Bitcoin est imaginé comme un système autonome, en réponse à la problématisation des institutions comme systèmes corruptibles. Cette problématisation s'inscrit dans une histoire politique d'innovations informatiques et monétaires confrontées au problème de la garantie des échanges dans un espace où la communication est incertaine. L'assimilation des institutions à des « systèmes » n'est pas (que) métaphorique : elle témoigne d'un glissement entre relation sociale instituée et résultat d'un calcul, c'est-à-dire

Chapitre 1. Mystique du protocole : calculer sans connaître

entre gouvernement et énonciation des règles formelles et des modalités du calcul des relations en société. Cette section a articulé les discours de promoteurs de Bitcoin avec les règles définies dans le dispositif pour analyser la réponse de Bitcoin au problème institutionnel, formulé en termes d' « autorités », « intermédiaires » et « tiers de confiance » : il serait naïf ou dangereux de faire confiance en général, sinon au sens très restreint de confiance inter-personnelle.

Bitcoin gouverne par les transactions : le dispositif organise une rupture épistémique entre l'usage (en l'occurrence monétaire) et la totalisation de ces relations en faits. Les relations sont gouvernées, sans que ceux qui participent au gouvernement (le réseau, *miners*) ne puissent exercer de pouvoir sur le contenu des communications (et sur les utilisateurs). Bitcoin est un agencement qui sécurise un registre distribué, vu comme matérialisation d'un ordre. Il rompt qui sait quoi des relations, tout en organisant la continuité dans une chaîne matérielle-sémiotique. Le réseau est fait d'agents passifs auxquels les utilisateurs délèguent l'opération d'inscription dans le registre qui fait tenir ensemble des individus vus comme des ennemis en puissance, et envers cet ordre. Les *miners* sont érigés en « porte-paroles » des utilisateurs. Le registre est l'ordre, sécurisé, quelles que soient les actions individuelles. Bitcoin est une technique de neutralisation de toute forme de pouvoir (concept compris selon de nombreuses significations avec Steven Lukes) en produisant une compétition matérielle entre chacun des participants au « gouvernement » au sens d' « action sur le registre ».

Bitcoin produit un ordre dans lequel les aspirants gouvernants n'ont pas la capacité de connaître les actions des gouvernés. Ces derniers peuvent agir et faire reconnaître leurs actions collectivement sans contraindre leur liberté, postulée comme absolue et irréductible. Ainsi, Bitcoin n'est pas un contrat social puisqu'il ne suppose aucunement de renoncer à l'expression de la toute puissance individuelle. Il s'agit plutôt d'une promesse d'ordre entre entités susceptibles de s'opposer par la force, mais individuellement protégées par un objet commun sécurisé contre les démonstrations de force. La consommation de puissance électrique est la clé de voûte de l'autonomie du système. Elle est une référence commune pour les *miners* et les utilisateurs : les premiers la payent, les seconds savent que les

Chapitre 1. Mystique du protocole : calculer sans connaître

premiers la paye et qu'à ce titre, leur enrôlement en garanti la sécurité. Elle est une référence car vue comme une « externalité » en langage économique, au système. L'énergie électrique est imaginée comme une ressource disponible en quantité illimitée⁶⁵.

L'ordre imaginé avec Bitcoin résonne avec la théorie de la connaissance défendue par l'économiste Friedrich Hayek : la connaissance de tout phénomène pouvant affecter l'économie ne peut pas être détenue par une entité donnée, pour des raisons aussi bien théoriques que méthodologiques (Hayek 1945)⁶⁶. En effet, Hayek problématise le gouvernement comme un problème de connaissance : les institutions ne peuvent pas gouverner correctement par manque d'information. Il dénonce les « autorités » dites « centrales », au sens des connaissances dont elles seraient supposées disposer. Hayek n'est pas opposé à toute forme d'institutions, en particulier si elles sont composées d'experts bien choisis ; mais selon lui, les institutions ne devraient pas être chargées d'un pouvoir d'administration qui supposerait de détenir une connaissance seulement accessible en situation par chaque acteur de l'économie. Hayek indique que chaque acteur dispose individuellement d'une connaissance des phénomènes qui l'entourent. Cette connaissance est naturellement décentralisée ; le problème à résoudre devient la question de la connaissance de ce qui n'est pas directement accessible à chacun dans la prise de décision économique.

Hayek et Bitcoin se retrouvent sur une problématisation du gouvernement comme un problème de calcul. Hayek proposait d'organiser l'économie par un système de prix comme solution d'accès à la connaissance dans une économie composée de producteurs et d'utilisateurs de ressources. Il défendait la levée des entraves à la compétition, permettant de faire émerger un ordre économique naturel par le seul jeu des intérêts des producteurs et

65 Le Chapitre 4 reviendra sur le décalage entre l'indignation unanime dans la sphère publique concernant la consommation de Bitcoin et la minimisation de ce problème par les acteurs participant à son développement, et les controverses liées au protocole lui-même.

66 Hayek s'oppose à la thèse socialiste (comme alternative au capitalisme) qui suppose que l'économie peut être planifiée, laquelle suppose d'avoir une connaissance complète (« centralisée ») des phénomènes à tout instant. Cette hypothèse serait pour lui impossible à satisfaire, sinon conduirait à une forme de totalitarisme au sens de privation de liberté individuelle. Hayek s'oppose dans le même temps aux hypothèses des marginalistes qui supposent qu'un économiste connaît tout de l'économie pour établir un état d'équilibre à partir d'équations mathématiques.

Chapitre 1. Mystique du protocole : calculer sans connaître

des consommateurs. Avec Bitcoin, le problème de connaissance porte sur l'administration de la monnaie, un objet par nature institutionnel au sens où son existence suppose sa reconnaissance par tous les acteurs économiques. Les *miners* ne font que calculer : mais leur calcul ne porte pas sur une connaissance économique construite à partir des actions individuelles ; le calcul est un artifice pour mettre les gouvernants en concurrence et les détourner du contenu des objets du gouvernement qu'ils seraient susceptibles de corrompre.

L'innovation de Bitcoin remarquée dans cette section consiste à s'appuyer sur les principes qu'Hayek pose comme des caractéristiques irréductiblement anthropologiques (notamment la compétition et la liberté d'entreprendre en économie) ou naturels pour imaginer un ordre. Hayek imaginait les membres de l'économie comme détenteurs d'une connaissance qu'il était impossible (et pas souhaitable) de centraliser. De la même manière, les *miners* ne sont pas imaginés comme entités connaissant les phénomènes qui les entourent : au contraire, en raison du média par lequel ils communiquent (Internet), et du possible manque de « loyauté » de ses composants, Bitcoin présuppose au contraire que toute information produite par un *miner* n'est pas fiable, et que seul le processus de validation collectif des blocs produit une connaissance collective.

Le protocole de Bitcoin peut être comparé à une « cyborg science » imaginée, au sens de Philipp Mirowski (2002) ; ici il ne s'agit pas d'une métamorphose de la discipline économique au contact des développements de la cybernétique, mais d'une tentative d'élaboration d'une théorie politique au contact de l'informatique. Deux héritages associés aux transformations récentes de l'économie et décrits par Mirowski doivent être distingués. Premièrement de la théorie des jeux : le thème d'acteurs adoptant des comportements stratégiques en situation de coopération posée comme « jeu » apparaît nettement avec la métaphore des généraux byzantins. Chaque participant au système a la possibilité de jouer pour ou contre le système, avec un gain espéré proportionnel à sa puissance de calcul ou une perte nécessairement égale à cette dépense. Deuxièmement de la cybernétique : l'enjeu des concepteurs de Bitcoin est de maintenir le fonctionnement d'un système, d'anticiper le comportement global du système en élaborant des rétroactions permettant de régler l'incertitude posée sur chacun de ses composants susceptibles d'être « défaillant ». Dans les

Chapitre 1. Mystique du protocole : calculer sans connaître

termes des acteurs, il s'agit de rendre le système « autonome » malgré cette incertitude, ou en écho de la thèse de Pickering concernant là aussi le développement des systèmes dans l'histoire de la cybernétique, de rendre le système « adaptable » (comme le fait le protocole en faisant varier le niveau de rémunération des *miners*) face à un monde qui ne peut pas être contrôlé (Pickering 2009).

2. Ethereum : libérer le calcul par le gouvernement des inscriptions

Cette section analyse Ethereum dans la filiation de Bitcoin. La première sous-section montre, à partir d'un cas d'utilisation dit « d'usage » d'Ethereum, que les transactions deviennent des traces d'exécutions d'algorithmes appelés « *smart contracts* ». Programmés par les utilisateurs d'Ethereum, ces algorithmes prennent la signification de contrats. Ils problématisent le Web et ses données. À leur circulation est opposé le contrôle sur les inscriptions des transactions. La deuxième sous-section montre qu'Ethereum prolonge l'innovation de Bitcoin, analysée à la section précédente en termes de rupture épistémique. Je propose de comprendre le protocole de consensus comme un « mécanisme de pouvoir » au sens de Michel Foucault (2004a), pouvoir prenant le sens de « pouvoir inscrire ». La troisième sous-section précise la notion de sécurité héritée de Bitcoin. Elle porte désormais sur le calcul programmé par les utilisateurs, résultats d'une décentralisation « architecturale » et « politique » pour son inventeur. Cette sécurité est articulée à celle proposée par Foucault dans son histoire de la gouvernementalité pour proposer de situer Ethereum dans une histoire des technologies de gouvernement par le calcul informatique.

2.1. Les transactions : inscriptions contrôlables plutôt que données circulantes

Cette sous-section s'arrête sur ce qui est appelé un « cas d'usage » dans le jargon du développement informatique en entreprise : un cas pratique d'utilisation. Ce cas illustre que les *smart contracts* sont imaginés comme instruments de contrôle des relations par les utilisateurs. Les *smart contracts* et Ethereum sont des problématisations d'un Web vu comme espace de données qui circulent, détachées des Internauts. Les *smart contracts* s'appuient sur cette circulation, que des analystes des *big data* décrivent comme des doubles numériques. Ethereum infléchit cette gouvernementalité algorithmique en contrôlant le travail des données : ils mettent leur circulation et leur abondance au service

de la production de relations numériques dans les termes des utilisateurs.

Smart contracts : les relations numériques comme contrats autonomes

« AXA se lance sur la Blockchain avec fizzy » titrait le groupe d'assurances AXA en septembre 2017. Le service fizzy proposait les opérations suivantes : souscription d'une offre d'assurance contre les retards d'avion par l'assuré·e d'AXA (via une interface Web), enregistrement du contrat sous forme d'un *smart contract* codé par l'assureur (sur Ethereum), indemnisation automatique de l'assuré en cas de retard d'avion (déclenchée par le *smart contract*, contraignant AXA à régler l'assuré).

AXA est le premier grand groupe d'assurance à proposer une offre utilisant la technologie blockchain. Découvrez fizzy, une plateforme d'assurance paramétrique 100 % automatisée, 100 % sécurisée, permettant de couvrir les retards d'avion.

*fizzy est un produit d'assurance d'un genre nouveau. Il propose à ses souscripteurs d'être **indemnisés directement et automatiquement** en cas de retard de leur vol. Si votre avion a plus de deux heures de retard, fizzy vous rembourse instantanément.*

*Comment ça marche ? Quand vous achetez une assurance retard d'avion sur la plateforme fizzy, **nous enregistrons la transaction dans la blockchain Ethereum, un réseau informatique inviolable, ce qui rend le contrat lui-même également inviolable.** Ce smart contract est connecté aux bases de données du trafic aérien mondial, et dès lors qu'un retard de plus de deux heures est constaté, l'indemnisation se déclenche automatiquement. **AXA délègue donc la décision d'indemnité à un réseau indépendant**, renforçant ainsi la confiance que le client peut avoir en AXA. (AXA 2017)*

Trois acteurs sont liés dans ce contrat d'assurance : l'assuré (ou utilisateur du service), AXA (son application Web « fizzy »), et le *smart contract* (sur la blockchain Ethereum). Ce dernier se distinguait des autres acteurs humains : cet algorithme était programmé par AXA et exécuté indépendamment des autres acteurs en présence (assuré et assureur). Le *smart contract* était imaginé comme acteur : en fonction des informations qui lui étaient envoyées, il changeait ses paramètres en fonction d'un code défini lors de sa création.

Chapitre 1. Mystique du protocole : calculer sans connaître

Les actions du *smart contract* et ses relations aux autres acteurs est représenté sur la Figure 3. Un membre de l'équipe de développement de *fizzy* faisait apparaître les différentes actions possibles sous forme de « *workflow* » entre l'utilisateur du service (client d'AXA, à gauche), AXA (« *fizzy* », au centre) et un *smart contract* exécuté sur Ethereum (à droite) dans un article aux allures de tutoriel (Clement 2019). Ce document était mis en ligne sur la plateforme web de blogs Medium, très utilisée pour les discussions autour des cryptomonnaies et de la blockchain à cette époque.

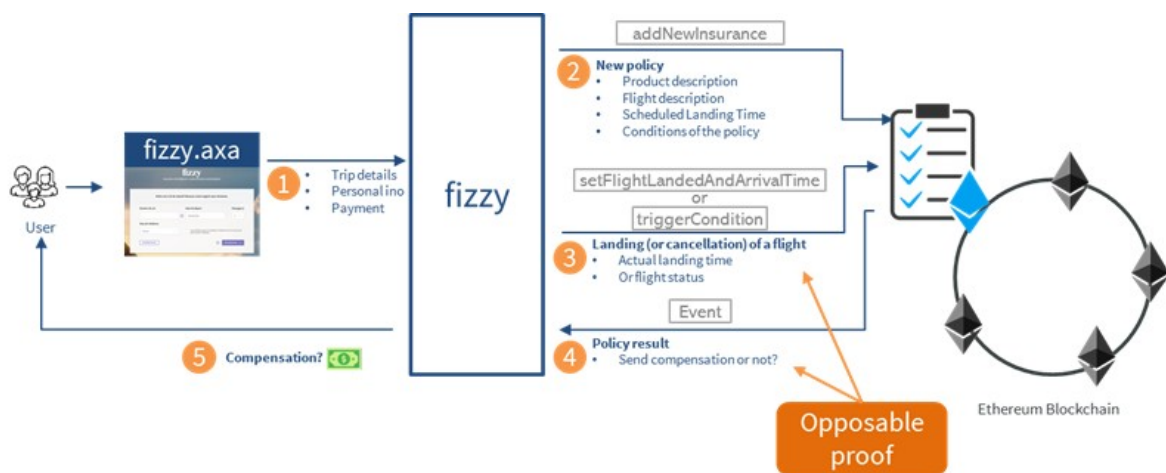


Figure 3 : Image reproduite depuis Clement (2019). Titre d'origine : « High Level workflow of the interactions between the fuzzy app and its Smart Contract »

Le Tableau 2 récapitule les acteurs en présence, en reprenant la numérotation du « workflow » de la Figure 3 quand ils apparaissent, ainsi que les types et formes d'informations qui circulent entre acteurs. En tout, quatre acteurs sont en jeu : l'utilisateur, AXA (ses serveurs hébergeant l'application *fizzy*), le *smart contract* (code « autonome » enregistré sur la blockchain Ethereum) et Flightstats (fournisseur de données spécialisées sur le trafic aérien)⁶⁷.

⁶⁷ Le service est accessible via une interface grand public sur <https://www.flightstats.com/> en janvier 2021.

Chapitre 1. Mystique du protocole : calculer sans connaître

| Numérotation sur Figure 3 | Émetteur d'informations | Opération | Type d'information | Récepteur d'informations |
|---------------------------|--------------------------------|---|--|--------------------------------|
| 1 | Utilisateur (devant son écran) | Demande de souscription d'un contrat | Informations contractuelles : personnelles et vol | AXA (fizzy) |
| 2 | AXA (fizzy) | Souscription du contrat : inscription du contrat sur Ethereum | Transaction : ID anonyme et informations du vol | Smart contract |
| 3' (non représenté) | Flightstats | Flux d'informations sur les vols en temps réel | Informations avions : heure d'arrivée réelle du vol si maintenu | AXA (fizzy) |
| 3 | AXA (fizzy) | Mise à jour du contrat avec le statut réel du vol | Transaction : vol maintenu annulé (oui/non), vol en retard (oui/non) ? | Smart contract |
| 4 | Smart contract | Décision d'indemnisation | Information : indemnisation due (oui/non) | AXA (fizzy) |
| 5 | AXA (fizzy) | Indemnisation | Crédit bancaire | Utilisateur (compte en banque) |

Tableau 2 : Flux et type d'informations entre acteurs impliqués dans un contrat fizzy

Le *smart contract* est imaginé à la fois comme un contrat et comme mise en œuvre de ce contrat prenant la forme d'une mise à jour en fonction d'événements ultérieurs à sa rédaction. L'utilisation d'Ethereum limite l'action humaine sur ce contrat au temps qui précède la rédaction ou souscription du contrat, lequel prévoit les actions futures sur les acteurs en présence. Ce temps préalable de rédaction du contrat d'assurance suppose des actions manuelles, des démarches, un travail administratif, aussi bien de la part de l'utilisateur-assuré que du fournisseur-assureur AXA. L'utilisateur remplit des informations sur un formulaire en ligne, à partir desquelles une « négociation » s'établit (bien que les prix des contrats sont établis selon des modèles de *pricing* développés par AXA). Ces prix sont codés par AXA (l'application fizzy) dans le langage du *smart contract*. Après la rédaction, et avant le vol assuré, la mise à jour de ce contrat est automatique avec des informations sur le vol. L'indemnisation éventuelle du souscripteur du contrat est provoquée par le *smart contract* en cas de retard, sans que le souscripteur ait besoin de demander une indemnisation auprès d'AXA.

Chapitre 1. Mystique du protocole : calculer sans connaître

Les concepteurs décrivent l'action du *smart contract* comme « automatique » et « opposable » : l'auteur a pris soin de faire apparaître que les opérations ont des « *Opposable proofs* » en gros caractères par l'utilisateur-souscripteur sur la Figure 3. Ce dernier a, d'une part, la possibilité de vérifier que le *smart contract* a bien été mis à jour, et d'autre part, la possibilité de vérifier la « décision » du *smart contract*. Le traitement « automatique » et son caractère « opposable » par l'utilisateur-souscripteur-client participaient, dans le langage de l'entreprise, à « [renforcer] la confiance que le client peut avoir en AXA ». De manière comparable à Bitcoin dont les promoteurs voyaient la confiance comme une qualité purement inter-personnelle, AXA promouvait le désengagement des institutions dans l'exécution des contrats. Une fois inscrit sous forme de *smart contract*, le contrat d'assurance était exécuté sans possibilité d'interférence ultérieure à condition que les « événements » du monde, comme le comportement « réel » et futur de l'avion assurant le vol objet du contrat, soient bien alimentés par les prestataires de données spécialisés (en l'occurrence, FlightStats).

Les actions de et sur le *smart contract* sont des transactions. Sur la Figure 3, les actions sur le *smart contract* sont numérotées 2 (souscription du contrat formulé par AXA au sens d'inscription sur Ethereum) et 3 (actualisation du contrat avec les données sur le vol) ; l'action du *smart contract* est numérotée 4 (décision d'indemnisation). Ces transactions ont un coût, qui est payé par AXA. C'est en effet AXA qui paye une transaction pour inscrire le contrat sur Ethereum (opération 2), ainsi que pour communiquer l'horaire d'arrivée au *smart contract* (opération 3). Le *smart contract* calcule l'état du contrat (est-ce que l'avion est en retard ?) en fonction de ces informations, et inscrit le résultat sur la blockchain Ethereum.

Le *smart contract* automatise un travail de « back office » : confronter les termes d'un contrat à la réalité d'un événement du monde au travers de données alimentées en temps réel, et décider si l'indemnisation doit être accordée ou non. En proposant ce service, AXA espérait convaincre ses clients du sérieux de ses engagements, dans la mesure où les contrats en question seraient effectivement exécutés. La société pensait ainsi répondre à l'exaspération des assurés face aux démarches administratives nécessaires pour obtenir

l'indemnisation à laquelle ils peuvent prétendre suite à un sinistre. Pour convaincre de ses bonnes intentions, l'assureur délègue à un tiers impartial, un « réseau informatique inviolable » et « indépendant » la décision éventuelle d'indemnisation. « Exécution » prend ici un double sens : l'exécution informatique signifie exécution du contrat, les deux opérations tendant à se confondre dans la mesure où la décision du *smart contract*, indépendamment vérifiable par son client suffisamment habile avec les technologies pour accéder à des sites permettant de visualiser l'état de la blockchain Ethereum, contraint AXA à exécuter le remboursement le cas échéant.

Problématisation du Web : un espace de données détachées des individus et agissantes

Avec Ethereum, AXA problématise le calcul des relations numériques par des algorithmes à la main de fournisseurs de services sur le Web. Cette question préoccupe différents auteurs intéressés par le développement des technologies numériques en général et d'Internet en particulier. Dans *A quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Dominique Cardon cherche à comprendre notre « société des calculs » (Cardon 2015 : 11). Le sociologue du numérique et d'Internet voit, au travers de ces objets, des logiques de « personnalisation » qui s'installent dans nos vies sans que nous soyons conscients de la manière dont elles nous transforment. Cardon propose de mieux comprendre les algorithmes afin de pouvoir discuter et critiquer la manière dont ils marquent nos existences, plutôt que de les laisser devenir indiscutables et invisibles. Pour cela, Cardon invite à considérer les algorithmes comme une technologie intellectuelle et cognitive, à « ouvrir la boîte noire » sans la dissocier des humains.

Pour Cardon, les algorithmes posent un problème de connaissance : ces instruments statistiques sont devenus une technologie de gouvernement avec la massification de « données » en tous genres. L'auteur voit un tournant dans nos sociétés contemporaines : alors que les algorithmes concernaient surtout les entreprises et les États, ils ont fait une entrée spectaculaire dans nos vies. Le problème contemporain que posent les algorithmes tiendrait à leur capacité de traitement de ces immenses quantités de données souvent

Chapitre 1. Mystique du protocole : calculer sans connaître

résumées sous le label *big data*. Ils produisent des indicateurs qui hiérarchisent, devinent, ou sélectionnent notre activité sur Internet. Les « comportements » des Internauts deviennent traduits en données calculées et recalculées, agrégées, croisées, recoupées, pour produire différents effets sur lesquels l'auteur regrette que nous n'ayons pas prise. Les algorithmes sont des « capteurs » qui rendent le monde « mesurable en tout » :

Le savoir et les connaissances, les photographies et les vidéos, nos mails et ce que nous racontons sur Internet, mais aussi nos clics, nos conversations, nos achats, notre corps, nos finances ou notre sommeil deviennent des données calculables.
(Cardon 2015 : 8)

Les algorithmes posent un problème d'asymétrie de contrôle dans l'espace numérique. Qu'ils soient signaux ou traces, c'est-à-dire explicites comme un statut Facebook ou implicites comme un clic (Cardon 2015 : 62), de plus en plus de nos comportements deviennent les « données » participant à une politique des indicateurs. L'auteur voit deux dynamiques concomitantes qui nous font perdre le contrôle sur nos existences numériques. D'une part, les données sont toujours plus nombreuses et leur circulation croît avec des phénomènes comme l'*open data*. D'autre part, les formes d'interprétation des algorithmes évoluent et se complexifient avec leur sophistication technique. Cardon voit dans ces deux tendances un risque d'assujettissement pesant sur les Internauts. En s'adaptant à nos désirs et en se réglant sur le trafic des signaux et traces produits à partir des comportements de tous les Internauts, la promesse d'autonomie et de liberté que portent les algorithmes se traduit en une forme d'assujettissement : à trop nous « montrer la route » dans un univers où l'information prolifère, nous risquons d'oublier « le paysage » (Cardon 2015 : 105-106).

Pour AXA comme pour Cardon, les relations numériques contemporaines posent un problème de contrôle des individus concernés : les données agissent, indépendamment de celles qu'elles désignent ou à qui elles sont attachées. Pour AXA, le problème se comprend en termes de liberté d'action individuelle : un fournisseur de service est un libre dépositaire de données dont il contrôle les significations. En l'occurrence, AXA est libre d'exécuter les termes du contrat passé avec un assuré, ou pas. Le couplage technologique des *smart contracts* et d'Ethereum permet de dessiner une alternative : donner à l'individu le contrôle

Chapitre 1. Mystique du protocole : calculer sans connaître

de ses relations, lesquelles sont cadrées comme des contrats. Ainsi, la circulation des données est mise au service de l'exécution de termes contractuels fixés à l'avance, indépendamment du fournisseur de service.

C'est aussi un tournant contemporain dans l'utilisation des outils de calcul qu'analysent Antoinette Rouvroy et Thomas Berns avec le concept de « gouvernement algorithmique » (Rouvroy & Berns 2013). Selon les auteurs, la gouvernamentalité algorithmique se distingue de l'information statistique par son caractère « a-normatif ». Ils rappellent qu'Alain Desrosières a souligné que l'information statistique peut se comprendre comme stabilisation provisoire et fragile de conventions entre des êtres ; elle est à la fois une référence vis-à-vis du phénomène auquel on l'associe et un élément du débat à part entière. Si cette tension représente une difficulté importante pour penser les conditions de possibilités d'un espace public, la statistique produit une « réalité sociale » entendue au sens de « moyenne » qui signifie normalité. Avec les opérations de *data mining* portant sur les *big data*, les statistiques ne s'ancrent plus dans aucune convention ; elles contribuent au contraire à démultiplier les formes de normalités. Ainsi, et si ces statistiques échappent à la tension précédente, les auteurs déplorent les effets de la « personnalisation » des informations qu'elles produisent, comme la radicalisation des opinions, la disparition de l'expérience commune, la captation d'attention humaine, plutôt que le développement du débat démocratique et de l'intérêt général.

Rouvroy et Berns ont analysé tôt un phénomène que beaucoup ont découvert à la fin des années 2010 avec des documentaires comme *The Social Dilemma* qui mettent en lumière des dirigeants de l'industrie numérique qui font repentance en analysant les mécanismes qu'ils ont contribué à développer des années 1990 à aujourd'hui (Orlowski 2020). Les auteurs analysent ce tournant par la généralisation d'une nouvelle forme de « statistique décisionnelle »⁶⁸. Les opérations qui composent cette technique « évitent » plutôt qu'elles ne « ciblent » les sujets individuels en créant un « double statistique » des sujets, donc du réel. Les auteurs analysent ce procédé comme un obstacle aux processus d'individuation,

68 Ils désignent : « l'extraction automatisée d'informations pertinentes depuis des bases de données massives à des fins de prévision ou d'exclusion (consommation, risques, fidélisation, définition de clientèles nouvelles...) » (Rouvroy & Berns 2013 : 167)

Chapitre 1. Mystique du protocole : calculer sans connaître

pourtant essentiel pour comprendre ce gouvernement algorithmique contemporain. Plutôt que de se concentrer sur les individus, le gouvernement algorithmique se concentrerait sur les relations⁶⁹.

Un problème important que pose ce « double statistique », objet du gouvernement algorithmique, tient à son détachement des individus qu'il « double ». Il est formé comme produit de corrélations automatiques à partir de données collectées elles aussi de manière automatique. Le gouvernement algorithmique est indifférent des individus eux-mêmes. Rouvroy et Berns distinguent ce phénomène du problème du contrôle des données personnelles, intimes et sensibles, qui ont inspiré les législations de protection de la vie privée en proposant des barrières défensives et restrictives autour de l'individu. Cet argument résonne avec celui de Mary Ebeling qui a montré que les réglementations jouaient un rôle actif dans ce qu'elle appelle des « réseaux de divulgation » de ce type de données (Ebeling 2016 : 72, 78). Mais Rouvroy et Berns préfèrent souligner une dissonance générale entre ces informations transformées en données et les processus de subjectivation : le sujet algorithmique ne se pense pas comme tel.

Rouvroy et Berns identifient « trois temps » de la gouvernementalité algorithmique (Rouvroy & Berns 2013 : 180). Premièrement, le consentement du sujet est faible quand il transmet de l'information⁷⁰. Deuxièmement, les savoirs produits à partir de ces données paraissent émerger de la masse de données, en générant les hypothèses qui les constituent. Troisièmement, l'action normative découlant de ces processus statistiques équivaut à une action sur l'environnement de l'individu plutôt que sur lui-même, dont l'action n'est plus régie par une norme extérieure comme une loi, une moyenne, ou autre définition de la

69 Cette analyse fait écho à des travaux récents d'études sociales du numérique. Par exemple, à partir de la collecte de dizaines de publicités pour des biens et services destinés aux jeunes parents qu'elle reçoit plusieurs semaines après avoir fait une fausse couche, Mary Ebeling a montré que les opérations de ciblage publicitaires sont parvenues à faire exister ce que l'auteurice appelle son « bébé marketing » alors qu'elle a souffert d'une fausse couche mettant fin à sa grossesse (Ebeling 2016). Cet enfant était suffisamment réel après la date théorique d'accouchement pour être devenu l'objet de son enquête. Selon les statistiques, ce « double » devait normalement exister théoriquement et existait pratiquement au travers des différents dispositifs publicitaires reçus par l'auteurice.

70 Comment alors parler de « vol », si le sujet n'est pas en mesure de s'y opposer ? Des auteurs comme Mary Ebeling ont montré empiriquement que cette incapacité est orchestrée dans des infrastructures informatiques, organisationnelles et bureaucratiques ; en l'occurrence qui, aux États-Unis, conditionnent l'accès au soin à la transmission d'informations personnelles.

Chapitre 1. Mystique du protocole : calculer sans connaître

normalité. Ses actions possibles sont directement organisées au sein même de son environnement. Pour ces raisons, le danger que les auteurs voient dans la généralisation des pratiques statistiques réside non pas dans leur caractère individuel, mais dans leur indifférence vis-à-vis des individus :

*Notre **problème**, pour l'exprimer de la manière la plus explicite, n'est pas d'être dépossédé de ce que nous considérerions comme nous étant propre, ou d'être contraint à céder des informations qui attenteraient à notre vie privée ou à notre liberté, mais il viendrait bien plus fondamentalement du **fait que notre double statistique est trop détaché de nous, que nous n'avons pas de « rapport » avec lui, alors même que les actions normatives contemporaines se suffisent de ce double statistique pour être efficaces.** (Rouvroy & Berns 2013 : 181)*

Dans les relations numériques imaginées par AXA, il n'existe pas de norme autre que la loi des contrats : les relations sont codées dans les termes des contrats, de manière à ce que les traitements sur les données soient réduits à une donnée (un paramètre du *smart contract*) qui exprime l'état du contrat en fonction d'événements futurs. Ainsi, avec les *smart contracts* et Ethereum, AXA problématise le détachement de données agissantes à la manière de Rouvroy et Berns, mais suppose en même temps un processus de subjectivation : le sujet se pense comme un individu contractant ; sa subjectivité est alors garantie par l'exécution des termes des contrats qu'il passe grâce au caractère « inviolable » et « autonome » de la blockchain Ethereum. Cette capacité de subjectivation et de contrôle sur les relations passe par l'objet transaction, jugée « opposable » à des tiers : l'individu en chair et en os serait capable d'agir et éventuellement de s'opposer aux acteurs auxquels il est lié par contrat.

Les concepteurs d'Ethereum comme les auteurs problématisent la circulation des données sur le Web. L'analyse d'Antoinette Rouvroy et de Thomas Berns des traitements algorithmiques par les *big data* comme un « gouvernement des relations » place les opérations sur les données au cœur du problème et des « perspectives d'émancipation » (sous titre de l'article). Ce sont ces opérations qui empêchent les processus de subjectivation et prennent les individus pour « objet » ou « cible » des trois temps qu'ils identifient (Rouvroy & Berns 2013 : 184) : « Récolte de quantité massive de données et

constitution de *datawarehouse* », « Traitement des données et production de connaissance », « Action sur les comportements ». Comme ces auteurs, la problématisation d'AXA se lit dans les opérations de traitement des données attachées aux utilisateurs. Les transactions sont des opérations sur des données. Bien entendu, les transactions sont elles-mêmes des données dans un sens littéral d'inscriptions en mémoire informatique ; mais ce qui est attaché à l'individu tient aux termes du contrat, supposé librement accepté par l'individu, plutôt qu'aux données en circulation (l'horaire d'arrivée de l'avion, dans le cas *fizzy*). Avec les transactions les concepteurs imaginent un contrôle sur les relations, sans renoncer à la circulation de ces dernières : ce qui compte pour s'émanciper de leur circulation serait de contrôler les modifications et les usages des données.

Contrôler le travail des données par les transactions

Les *smart contracts* sont des algorithmes qui ont des effets différents de ceux auxquels se sont intéressés Cardon ou Rouvroy et Berns. Comme ces derniers (à l'image de l'algorithme de *pricing*), ils sont nourris de *big data* produites à partir de signaux ou traces d'autres individus (distribution statistique des temps de retard ou annulations de vols) pour produire des données personnalisées (le prix du contrat) qui participent à l'amélioration de l'algorithme (de *pricing*) lui-même. Mais les *smart contracts* sont programmés pour produire une information en fonction de données références dont la valeur témoigne d'événements futurs. Le résultat du calcul de ces algorithmes est une inscription qui signifie fixation de données individuelles, plutôt que statistique portant sur des quantités massives de données visant à profiler.

Pour incarner l'importance d'une « sociologie des données » comme programme de recherche, Jérôme Denis fait apparaître combien nos identités contemporaines sont ancrées dans les bases de données des différentes institutions avec qui nous sommes en relation (Denis 2018). En quelques pages, l'auteur raconte de manière aiguë et touchante les différentes opérations administratives que ses proches et lui-même ont dû engager suite au décès de son père. Denis témoigne de l'urgence de considérer le travail qui fait exister ces données et symétriquement, combien les données font agir : la mort ne peut pas, en

Chapitre 1. Mystique du protocole : calculer sans connaître

pratique, se comprendre comme une information évidente ou une « donnée brute ». L'auteur prend justement l'exemple d'une série d'échanges avec une société qui assurait les prêts du défunt pour montrer que l'exécution d'un contrat suppose des actions de documentation, de démonstration, pour que l'information « M. Denis est mort » soit traduite en « De quoi est-il mort ? » (Denis 2018 : 22).

Les données qui font tenir les institutions et nos identités numériques sont le produit d'un travail et, symétriquement, agencent. Denis invite à étudier le travail souvent invisible dont les données font l'objet, dans les coulisses des administrations. C'est précisément ce travail invisible de back office, de celles et ceux que l'auteur a décrit ailleurs comme les « petites mains de l'information » (Denis et Pontille 2012), qu'une entreprise comme AXA cherche à automatiser avec Ethereum. À partir des informations fournies lors de la signature du contrat d'assurance, la société promet une exécution « automatique » future du contrat une fois qu'il faudra en exécuter les termes. Codées sous forme de transaction dans un *smart contract*, les données des utilisateurs sont immobilisées jusqu'à ce qu'un événement, l'horaire d'atterrissage d'un avion, vienne les animer. L'automatisation permet l'agencement par les données elles-mêmes : l'indemnisation ne serait plus soumise à une action ultérieure.

Ethereum est une infrastructure scripturale originale : elle articule les *big data*, sur lesquelles les contractants s'appuient pour mettre à jour les contrats qui y sont inscrits, tout en cherchant à échapper aux errances de la « société des calculs » qui préoccupe Cardon ou aux problèmes de subjectivation causés par le « gouvernement algorithmique » décrit par Rouvroy et Berns. Ces auteurs voient dans la circulation des données et les traitements détachés de tout rapport avec l'individu duquel elles sont produites un pouvoir qui agit sur toutes et tous au futur. Rouvroy et Berns soulignent :

Le champ d'action de ce « pouvoir » n'est pas situé dans le présent, mais dans l'avenir. Cette forme de gouvernement porte essentiellement sur ce qui pourrait advenir, sur les propensions plutôt que sur les actions commises, à la différence de la répression pénale ou des règles de la responsabilité civile, par exemple, qui ne se trouvent concernées que par des infractions qui auraient été commises ou qui seraient en train d'être commises (en cas de flagrant délit), ou des dommages qui

auraient été causés. Plus activement, le gouvernement algorithmique non seulement perçoit le possible dans l'actuel, produisant une « réalité augmentée », une actualité dotée d'une « mémoire du futur », mais donne aussi consistance au rêve d'une sérendipité systématisée : notre réel serait devenu le possible, nos normes veulent anticiper correctement et de manière immanente le possible, le meilleur moyen étant bien sûr de nous présenter un possible qui nous corresponde et dans lequel les sujets n'auraient plus qu'à se glisser. (Rouvroy & Berns 2013 : 182-183)

Avec Ethereum, l'inscription permettrait de préparer des actions futures en fonction d'actions présentes : AXA et le souscripteur s'engagent à agir selon des termes définis au présent, sans qu'aucune intervention des parties de l'accord ne puisse renégocier les termes du contrat. Les statistiques et leurs traductions en *big data* ne sont pas absentes de ce processus. AXA fabrique le prix du contrat en fonction du « risque de retard ou d'annulation qui est calculé indépendamment pour chaque vol » par un algorithme de *pricing* développé par l'assureur. Ces données sont ensuite fixées et inscrites dans les *smart contract*, leur donnant une capacité d'action future. Le futur deviendrait « contrôlé » par les utilisateurs, dans la mesure où ils sont suffisamment équipés en connaissances et outils techniques pour agir sur leur traitement futur et vérifier leurs transactions. Par les *smart contracts*, les algorithmes deviendraient lisibles : le traitement des données ne souffrirait plus de l'opacité des algorithmes hébergés sur les serveurs d'entreprises, et symétriquement, n'exercerait pas sur les sujets le « travail invisible » décrit par Jérôme Denis.

2.2. En filiation avec Bitcoin : un mécanisme de pouvoir inscrire

Cette sous-section montre que l'objectif de « sécurité » vu à la section précédente porte sur le calcul informatique, résultat du cadrage des capacités d'action des Internauts par la décentralisation de l'architecture informatique et politique des entités coordonnées par le protocole. Cet objectif est confronté à la notion mobilisée par Michel Foucault pour désigner une technologie de pouvoir qu'il appelle « mécanisme de sécurité » : Ethereum fait du Web un champ d'intervention, gouvernant les événements « inscriptions » en s'appuyant sur la circulation des données, prise comme une réalité qui est contrôlée plutôt que niée ou

évitée. Enfin et à l'aide de quelques exemples issus de l'histoire de l'informatisation, cette section plaide pour une analyse des blockchains dans un art de gouverner par le calcul informatique compris comme une double opération d'exécution de règles (ou de code) et d'inscription du résultat de ces règles.

Des transactions monétaires aux transactions contractuelles : Bitcoin, du système au modèle

*There's a **new digital currency** that's looking to give bitcoin a run for its money: Ethereum. In a sense, it's **an offspring of bitcoin** that's capitalizing on and **enriching blockchain technology**. Developers and cryptomaniacs around the world are rejoicing about its **potential applications**. But you can so rejoice, too. And that's because **it's not exactly a digital currency**. It takes the **conceptual basis for bitcoin** and makes it **applicable to just about anything**. (Carmichael 2016)*

Ces lignes enthousiastes et ambiguës sont les premières d'un article de journal en ligne⁷¹ qui présentent Ethereum comme « *the 'World Computer' that may power the future* ». Elles affirment une descendance de Bitcoin : Ethereum « prend les bases conceptuelles de Bitcoin », « capitalise sur Bitcoin » et « enrichit la technologie blockchain ». Cet héritage fait hésiter l'auteur à qualifier Ethereum de « monnaie numérique » ; cet objet serait plutôt « potentiellement applicable » à « n'importe quoi » : des « applications potentielles » à un large spectre de services Web.

Le fondateur d'Ethereum, Vitalik Buterin, associe lui aussi directement la création d'Ethereum à Bitcoin. Dans une interview organisée, filmée et retranscrite par « une banque de monnaies numériques » appelée Abra, il racontait qu'il avait entendu parler de Bitcoin à l'âge de 17 ans, en 2011 (McGlynn 2019). Motivé par l'idée « intéressante » de Bitcoin, le jeune Vitalik explorait les forums Internet dédiés à Bitcoin jusqu'à se faire rémunérer en bitcoins pour publier des articles sur un blog dédié à Bitcoin. Sa curiosité le conduisit à une activité à temps plein : il fondait *Bitcoin Magazine* en 2012, un des premiers journaux en ligne dédié aux actualités de Bitcoin. Il participait par exemple à relayer les dernières

71 L'article est publié sur Inverse, un magazine décrit comme dédié aux technologies, aux sciences et à la culture pour un public de « millenials ».

Chapitre 1. Mystique du protocole : calculer sans connaître

actualités liées à l'utilisation de Bitcoin, comme l'acceptation des paiements en bitcoins par le système de gestion de contenus en ligne Wordpress (Buterin 2012). Ces premières activités lui permettaient de « s'enfoncer de plus en plus dans la communauté Bitcoin, et comprendre comment elle fonctionne sur le plan technique, comprendre les idées sociales et économiques ». Buterin expliquait que Bitcoin rassemblait tous ses centres d'intérêts dans un même « paquet » : mathématiques, informatique, programmation, cryptographie. Il racontait que la communauté Bitcoin était alors animée de discussions où émergeaient des idées politiques et sociales. Le libertarianisme, qui était très « fort », rencontrait des idées « socialistes et mutualistes » dans « d'amuses petites tribus » qui débattaient, par exemple, dans la section politique et société du forum en ligne *Bitcoin Talk*.

Dans le même temps, d'autres « projets » proposaient de nouveaux usages à partir de Bitcoin. Mastercoin était l'un d'eux. Il était présenté comme un protocole informatique qui « ajoute » des « fonctionnalités » à Bitcoin. L'idée était la suivante : Mastercoin permettrait de former des transactions plus complexes que des transactions monétaires de Bitcoin, où la transaction signifie débit du compte de l'émetteur et crédit du compte du destinataire. Ces transactions restaient cependant validées par les *miners* du protocole Bitcoin. L'innovation de Mastercoin consistait à ajouter une « couche » protocolaire « sur » Bitcoin, de manière similaire à d'autres protocoles réseaux, comme HTTP qui fonctionne comme une couche supérieure à TCP/IP. Cette couche permettait de former des transactions prenant cinq formes plus complexes, codées dans le protocole de Mastercoin, qui les rendaient interprétables et inscriptibles par les *miners* de Bitcoin de manière tout à fait indifférenciée des transactions Bitcoin classiques. Ce projet fit réagir Buterin :

*Vitalik Buterin: The first thing I did was I made a proposal to Mastercoin that would **replace basically five of the transaction types they have with a programming language designed to express financial contracts between two parties.** [...] Initially, for me, it was like, hey, they're doing this thing, they're trying to make it possible to do more stuff, **that seems cool, but I know how to do more**, how to make it possible to do more stuff with a protocol which is ten times simpler, which is **instead of basically having a Swiss Army knife with 100 different types of features, you would just have a programming language**, so then you could kind of build whatever you want on top. (McGlynn 2019).*

Chapitre 1. Mystique du protocole : calculer sans connaître

Intéressés par la proposition de Buterin, les développeurs de Mastercoin envisagèrent d'intégrer son idée au calendrier de leurs développements à horizon un an. Le principal intéressé jugea ce délai largement excessif pour ce qu'il pensait être la proposition la « plus importante du moment », et décida de travailler seul sur son projet :

*Vitalik Buterin: So free of the constraints of having to iterate an existing system, I kept on thinking, and eventually, **it took me a couple of weeks to figure out how to expand the model from just two-party contracts** of these computer programs that talk to each other and can do pretty much whatever they want, but once I made that one kind of leap, **suddenly everything made sense, that you could just do everything with contracts.** (McGlynn 2019)*

Toute relation numérique peut être formulée en termes de contrat : cette intuition apparût à Buterin quand il change son regard sur Bitcoin. Il ne voit plus un système à améliorer (en sophistiquant les transactions de Bitcoin avec des projets comme Mastercoin), mais une technologie d'inscription en réseau dont les significations ne sont pas attachées à l'activité d'inscription elle-même. Il imagine que les utilisateurs puissent eux-mêmes programmer la signification des relations numériques dont l'inscription est déléguée au réseau à l'aide d'un « langage de programmation » plutôt qu'en choisissant parmi « 100 différents types de fonctionnalités ».

Ainsi, Buterin imaginait de nouveaux utilisateurs. Sa tentative se démarquait des nombreuses répliques de Bitcoin au début des années 2010 pour d'autres projets de monnaies numériques. Il ne s'agissait plus d'un citoyen lésé par les politiques oppressives des banques et des gouvernements pour librement transiger avec une unité monétaire hors des institutions. Il s'agissait d'un Internaute dont « toutes » les actions sur le Web pourraient être traduites sous forme de « contrats » dont les traces d'exécution seraient des « transactions » informatiques inscrites de manière sûre et immuable, à la manière de Bitcoin. Et symétriquement, il supposait que ces relations pouvaient être codées dans un langage de programmation unique.

Bitcoin : architecture et véhicule de problématisation des institutions comme systèmes

L'intuition de Buterin conduit à Ethereum, est réseau inscripteur administrés par ses propres *miners*. Le protocole de consensus d'Ethereum était similaire à celui de son modèle Bitcoin. Les objets qu'inscrivent les serveurs connectés par le protocole Ethereum sont similaires : des transactions incluses dans des blocs par des *miners* qui recherchent une récompense en ethers en échange de la puissance de calcul. Autrement dit, Ethereum reprend l'architecture informatique de Bitcoin.

Les concepteurs d'Ethereum relayaient des critiques proches de celles des promoteurs de Bitcoin. Ils problématisaient des formes institutionnelles gouvernant les relations numériques par la notion de « confiance » ; mais alors que Bitcoin problématisait la monnaie, Ethereum problématisait plus généralement les relations *via* le Web. Ajar, cryptographe impliquée dans le développement de l'infrastructure d'Ethereum, s'exprimait lors du Festival P2P de janvier 2020 lors d'une présentation intitulée « Couche réseau »⁷² :

Blockchain is a distributed ledger. So what do we mean by that? So we have, so, instead of the web 2.0 system that we have a server and a client, communicating together, blockchain is having multiple servers, while storing different type of information. So why do we have that and what's the advantage of having such architecture? So the blockchain in fact appeared in 2009, not as a blockchain as an architecture, but it appeared as Bitcoin, which is a cryptocurrency. So the cryptocurrency Bitcoin appeared to... as a revolutionary idea, to kind of eliminate the need of banks, third parties, centralized third parties, where people cannot trust these centralized third parties, and they want to... to have, to create a system, where there is no need for trust, yet we have a system which is secure. So the blockchain technology helps to create that. And helps to eliminate one of the biggest problem of the web 2.0, which is a central, central point of failure. Because we have essential points of control. So when you have a certain server, and that server is being attacked so every information can be leaked, can be hacked, or even if the trust party that we are relying on is compromised and the information of course is also compromised. (Ajar, Festival P2P, janvier 2020)

L'assimilation des formes institutionnelles à des « systèmes » se voient nettement dans ce

⁷² Cette présentation avait lieu sur la même scène que l'intervention de Jacques Favier et d'Adli Takkal Bataille, citée à la section précédente.

Chapitre 1. Mystique du protocole : calculer sans connaître

passage, où « point de défaillance » technique et « point de contrôle » social sont confondus. La blockchain remplace les *back offices* des applications Web comme Bitcoin remplace ceux des institutions financières. La blockchain devient une « architecture » de « systèmes » informatiques, une technologie permettant de faire communiquer des serveurs de manière à ce qu'il n'existe aucun « point de contrôle » sur les transactions qui y sont inscrites. Ces points de contrôles peuvent être des banques ou des gouvernements, ou tout acteur du « Web 2.0 » susceptible de modifier des données stockées sur les serveurs qu'ils détiennent (ou qu'ils se font pirater).

*So Ethereum is different from Bitcoin, which I talked about earlier, **Bitcoin is more about one application which is the cryptocurrency, Ethereum is more complex than that. We can imagine it as... as a big computer, that can execute multiple and very complex calculation. So we can create new type of applications, which are decentralized applications on top of Ethereum. So... what is the difference? Again as I said, Bitcoin is more as offering a particular application on top of the blockchain technology, however Ethereum is focusing on executing decentralized applications, using smart contracts, to do so.** (Ajar, Festival P2P, janvier 2020)*

Ainsi, et dans la même veine que l'intuition rapportée *a posteriori* par Buterin vue plus haut, Ajar explique qu'Ethereum problématise le calcul détenu par les acteurs du Web. La notion de transaction incarne cette problématisation : le calcul peut être produit de manière décentralisée, visible et contrôlable par tout individu, à la différence d'une relation asymétrique entre une institution calculatrice et un individu. Vus comme les instanciations d'une « technologie », Bitcoin et Ethereum apparaissent comme des objets construits en deux « couches ». La première couche est infrastructurelle. Elle assure que le « système » est « sécurisé » ; on parle de *layer 1*. La seconde, *layer 2*, est une couche logicielle. Elle trouve sa finalité dans la mise à jour de comptes en monnaie numérique pour Bitcoin, dans un « gros ordinateur » ou un « ordinateur Monde » capable d'exécuter des « applications décentralisées » avec Ethereum.

Le protocole : mécanisme de pouvoir inscrire

La problématisation du calcul des relations numériques avec Ethereum s'inscrit dans une

Chapitre 1. Mystique du protocole : calculer sans connaître

généalogie avec Bitcoin. Les deux systèmes partagent une même politique qui tient dans ce que j'ai décrit à la section précédente comme séparation entre les significations des transactions comme usages et comme inscriptions. Cette filiation peut s'analyser avec le vocabulaire que développe Michel Foucault.

Le protocole est constitué de différentes « stratégies » : des procédures, dans une situation de confrontation, pour priver l'opposant de moyens de combattre et lui faire abandonner la lutte (Foucault 1982). Le protocole est en effet un ensemble de règles informatiques qui limitent la capacité d'action de tout acteur d'Internet à leur puissance de calcul. Ce sont précisément à des situations de confrontation potentielles que répond le protocole en réduisant les formes d'intervention à la mobilisation de puissance de calcul : le « problème des généraux byzantins » exprime par une métaphore guerrière qu'un système informatique est un espace menaçant pour les communications, les échanges, les organisations en réseau. Il pose comme hypothèse que les acteurs du réseau se méfient les uns des autres, et forme cette méfiance en instaurant la compétition entre pairs.

Foucault propose de se concentrer sur les stratégies pour analyser les relations de pouvoir en situations de confrontation, jeu ou guerre, où l'objectif est d'agir sur un adversaire de manière à rendre la lutte impossible. La stratégie est alors le choix d'une solution de victoire. La solution de victoire, avec le protocole, consiste à conserver le registre comme « sûr » ou « inviolable ». Elle s'accompagne d'hypothèses spécifiques, comme discuté à la section 1, notamment le choix de la délibération par la puissance de calcul comme identité en ligne. Ces différentes « tactiques » dans le langage de Foucault permettent de construire des « stratégies » prenant la forme de règles stabilisées destinées à « aligner les intérêts » des acteurs en présence.

Le protocole a été analysé comme ingénierie d'une neutralisation de toute forme de pouvoir sur le registre, avec Lukes. Pour Foucault, le pouvoir n'existe pas en dehors d'une action. Son exercice n'est pas seulement une relation entre partenaires, individus, collectifs : c'est une façon selon laquelle certaines actions modifient d'autres actions. Le pouvoir n'est pas fonction du consentement, ni le caractère de rapports de violence : une relation de pouvoir

Chapitre 1. Mystique du protocole : calculer sans connaître

est un mode d'action qui agit sur les actions des autres. Une relation de pouvoir suppose que celui sur qui est exercé le pouvoir continue d'agir, et que face à une relation de pouvoir, des réponses, réactions, inventions surviennent :

*It is a total structure of actions brought to bear upon possible actions; **it incites, it induces, it seduces, it makes easier or more difficult**; in the extreme it constrains or forbids absolutely; it is nevertheless always a way of acting upon an acting subject or acting subjects by virtue of their acting or being capable of action. **A set of actions upon other actions** (Foucault 1982 : 789)*

Positivement avec Foucault, le protocole problématise et organise le pouvoir d'inscrire : jusque-là réservé à certaines « institutions » (monétaires pour Bitcoin, du Web pour Ethereum) dont la qualité est justement de disposer de moyens d'actions particuliers dans un corps social, le pouvoir d'inscrire est empêché pour toute action qui ne suit pas le protocole. Dans le même temps, le protocole « incite », « rend plus ou moins difficile » d'inscrire selon un mécanisme adaptatif.

Cette définition du pouvoir en société conduit Foucault à la notion de « gouvernement » des « conduites » entre groupes ou individus impliqués. Gouverner signifie structurer le domaine d'action possible des autres. Le pouvoir comme exercice est un mode d'action sur les actions des autres. Ce mode d'action caractérise les actions de gouvernement de certains sur d'autres, tout en incluant la liberté : le pouvoir ne s'exerce que sur des individus libres, c'est-à-dire qui font face à différentes manières de se comporter⁷³. Cette liberté radicale est supposée par le protocole : quiconque peut inscrire en suivant le protocole, les utilisateurs quel que soit leur usage, et les *miners* pour obtenir une récompense, tout en incluant la liberté de chacun de falsifier le registre (ce que le protocole cherche à empêcher) ou de ne pas être intéressé par le registre.

Le protocole est un mécanisme qui gouverne les inscriptions en déplaçant le libre jeu de réactions antagonistes contre le registre de manière suffisamment certaine pour assurer

⁷³ Quand la détermination sature la relation (l'esclavage par exemple), il n'y a pas de relation de pouvoir, pas de confrontation du pouvoir et de la liberté qui s'excluent : la liberté est une condition à l'exercice du pouvoir. Pour Foucault, l'insubordination est au cœur des relations de pouvoir, une obstination pour la liberté avec la possibilité de s'échapper ou de fuir : toute relation de pouvoir implique, au moins potentiellement, une stratégie de lutte de deux forces qui ne perdent pas leur nature.

l'objectif (stratégique) de sécurité du registre. La recherche individuelle de la rémunération par la dépense de puissance de calcul remplace le jeu de réactions antagonistes qui pourraient conduire à falsifier le registre. Le protocole systématise des rapports de pouvoir entre acteurs du réseau supposés libres. Le protocole transforme des situations de confrontation (pour le maintien ou la corruption du registre, selon le point de vue) en actions d'individus intéressés par une action commune : en l'occurrence, d'inscrire.

Le point de vue de la technologie de pouvoir

Bitcoin et Ethereum ne gouvernent pas les mêmes « conduites » : monétaires, ou d'utilisation de services numériques cadrés comme des contrats. Mais toutes deux partagent une même exclusion du pouvoir d'inscrire des « institutions », des « intermédiaires » ou des « tiers de confiance ». La notion « technologie de pouvoir » proposée par Foucault permet d'aborder positivement ce que les acteurs du développement de ces systèmes décrivent par la négative, *via* des stratégies d'évitement ou d'exclusion. Avec son service *fizzy*, AXA limite sa propre capacité d'action sur le contrat conclu avec ses assurés, contrat qui est par là même réduit à une inscription dont pourraient se prévaloir aussi bien l'assureur que l'assuré, car gouvernée par Ethereum.

La question du pouvoir traverse l'œuvre de Michel Foucault, parfois résumée au concept de « bio-pouvoir » que l'historien et philosophe propose pour la première fois dans son cours de 1976 au Collège de France *Il faut défendre la société*. L'ambition de Foucault n'est pas, comme Lukes, de proposer une théorie générale du pouvoir. Foucault s'intéresse plutôt à des « mécanismes de pouvoir », d'« ensemble de procédures » : il s'agit d'analyser des relations plutôt que de voir le pouvoir comme une substance, un fluide ; une intuition proche de la proposition anthropologique de Bruno Latour (1984). Ces relations (quelles qu'elles soient de production, familiales, sexuelles, etc.) ne sont pas dissociables des mécanismes de pouvoir qui font au contraire partie intégrante de ces relations. Foucault se place sur un plan philosophique, qu'il définit comme « la politique de la vérité » : l'analyse des mécanismes de pouvoir a pour rôle de montrer quels sont les « effets de savoir » qui sont produits par les luttes, par les stratégies qui les guident et les tactiques de pouvoir qui

Chapitre 1. Mystique du protocole : calculer sans connaître

en sont les éléments.

Les mécanismes de pouvoir sont divers ; Foucault en étudie les corrélations pour proposer une analyse du gouvernement des conduites des hommes dans *Sécurité, Territoire, Population*, cours qui s'appuie sur les conclusions de travaux précédents (2004). Foucault identifie trois types de mécanismes associés à un phénomène donné⁷⁴. Cette typologie vise à proposer une histoire des « technologies de pouvoir », c'est-à-dire l'histoire globale de l'émergence des corrélations entre différents mécanismes dans tel secteur, de telle société, à une époque donnée. Pour Foucault, il ne s'agit pas de faire une histoire des techniques de pouvoir. Si différentes technologies de pouvoir se déploient concomitamment à toutes les époques, il existe des « dominantes ». Pour les distinguer, Foucault s'appuie notamment sur des travaux où il s'intéressait au « phénomène » de la maladie (Foucault 1972, 1975). Alors que les lépreux étaient exclus selon des mécanismes juridiques et religieux, le problème se pose en termes disciplinaires pour la peste avec l'apparition de règlements (comme l'obligation de mise en quarantaine). Juguler la variole se pose dans des termes sécuritaires (savoir combien de personnes sont affectées, à quel âge, avec quels effets) ; mais la gestion de l'épidémie n'implique pas moins un ensemble législatif et des obligations disciplinaires.

L'analyse des mécanismes de pouvoir permet à Foucault d'englober les institutions, sans réduire à elles seules l'analyse du gouvernement. Il part de la manière dont les hommes sont conduits pour analyser comment le gouvernement se pense à une époque donnée, dans une société donnée. L'« art de gouverner », dont Foucault fait les histoires, est le concept que je retiens comme central. En particulier, il fait « histoire de la gouvernementalité », sens politique contemporain de gouvernement d'un État ou d'un territoire donné au concept plus général d'art de gouverner. Selon ce dernier sens, Foucault montre que des « contre-

74 Le mécanisme légal ou juridique produit un partage binaire entre permis et défendu. Le mécanisme disciplinaire est caractérisé en termes de surveillance et de correction des personnes. Le dispositif de sécurité insère, lui, un « phénomène » ou une « expérience fondamentale » (la folie, la maladie, la mort, le crime, la sexualité, etc.) dans un ensemble d'événements probables, et définit des réactions en fonction de la position du phénomène par rapport à une moyenne, selon un calcul de coût. Plutôt qu'une histoire pensée selon un schéma linéaire, d'ancien (juridique) à contemporain (sécurité) en passant par moderne (disciplinaire), Foucault s'intéresse aux systèmes de corrélations entre ces mécanismes. Selon les époques, ces corrélations changent dans leurs techniques pour un secteur donné ; la statistique des crimes devient par exemple une technique complémentaire à la technique cellulaire pour le secteur pénal.

Chapitre 1. Mystique du protocole : calculer sans connaître

conduites », qui s'opposent au pastoralat à partir du XVI^e siècle, compris comme pouvoir spécifique qui prend pour objet la conduite des hommes, naît une nouvelle forme de gouvernement qui doit être distinguée de la souveraineté. Cette forme de gouvernement a une raison propre ; elle s'oppose à celle du pastoralat, appartenant à un monde anthropocentré et finaliste dans lequel l'homme doit faire son salut en le décodant. Alors que le souverain doit faire autre chose que Dieu vis-à-vis de la nature avec la *res publica*, la gouvernementalité de l'État répond ensuite alors à l'agouvernementalité de la nature. Mais l'État, institution contemporaine par excellence, est une « péripétie de la gouvernementalité » pour Foucault.

Par « gouvernementalité », j'entends l'ensemble constitué par les institutions, les procédures, analyses et réflexions, les calculs et les tactiques qui permettent d'exercer cette forme bien spécifique, quoi que très complexe, de pouvoir qui a pour cible principale la population, pour forme majeure de savoir l'économie politique, pour instrument technique essentiel les dispositifs de sécurité. Deuxièmement, par « gouvernementalité », j'entends la tendance, la ligne de force qui, dans tout l'Occident, n'a pas cessé de conduire, et depuis fort longtemps, vers la prééminence de ce type de pouvoir qu'on peut appeler le « gouvernement » sur tous les autres : souveraineté, discipline, et qui a amené, d'une part, le développement de toute une série d'appareils spécifiques de gouvernement [et d'autre part], le développement de toute une série de savoirs. Enfin, par « gouvernementalité », je crois qu'il faudrait entendre le processus, ou plutôt le résultat du processus par lequel l'État de justice du Moyen Âge, devenu aux XV^e et XVI^e siècles État administratif, s'est trouvé petit à petit « gouvernementalisé » (Foucault 2004a : 111-112).

Prendre la gouvernementalité comme objet permet à Foucault d'aborder l'État et la population en effectuant trois déplacements similaires à ceux de ses travaux antérieurs sur la discipline : se décentrer par rapport à l'institution (l'État comme l'hôpital psychiatrique) en « passant au-dehors » pour lui substituer le point de vue de la technologie de pouvoir (la ségrégation pour la psychiatrie, la biopolitique pour l'hôpital), substituer au point de vue intérieur de la fonction le point de vue extérieur des stratégies et des tactiques (les disciplines plutôt que la prison), et saisir la constitution d'un champ de vérité avec des objets de savoirs. Ces déplacements consistent à défonctionnaliser et désinstitutionnaliser : ils permettent de saisir la généalogie des formes de pouvoirs à partir d'autres choses que

Chapitre 1. Mystique du protocole : calculer sans connaître

d'elles-mêmes, en analysant leur filiation plutôt que leur genèse, et d'examiner en quoi elles sont instables.

Je m'inspire de ce geste en prenant le point de vue de la technologie de pouvoir pour poursuivre l'analyse d'Ethereum. Le Tableau 3 récapitule la correspondance que je propose entre le vocabulaire de Michel Foucault et l'analyse d'Ethereum. Ce point de vue permet de décentrer l'analyse par rapport aux institutions du Web (institutions financières, ou plus généralement toutes institutions formant des relations numériques) en insérant Ethereum dans une généalogie des formes de pouvoir sur et par les relations numériques. Ethereum se situe dans un art de gouverner par le calcul informatique. Cette section a montré qu'Ethereum s'inscrivait dans une filiation avec Bitcoin. Le point de vue de la technologie de pouvoir (d'inscrire) permet, dans la fin de cette section, de connecter cette filiation à la problématisation des concepteurs d'Ethereum et des chercheurs intéressés par les algorithmes et les *big data*. Ethereum prolonge cette histoire en infléchissant les manières de calculer et d'inscrire les relations numériques pour les gouverner. Cette inflexion consiste à séparer les parties prenantes de la relation contractuelle au calculateur et à l'inscripteur de cette relation. Cet enjeu se lit dans l'importance accordée à la sécurisation du registre et à la manière de sécuriser le registre.

| | Langage de Michel Foucault | Analyse du gouvernement avec Ethereum |
|----------------------------------|---|---|
| <i>Totalisations</i> | Institutions (État, hôpital, prison...) | Fournisseurs de services sur le Web (banques, assurances...) |
| <i>Relations individu / tout</i> | Phénomènes ou événements ⁷⁵ | Calcul et inscription de relations numériques |
| <i>Rapports de pouvoir</i> | Tactiques | Délibération d'acteurs connectés en réseau Messages cryptés Identification par la puissance de calcul Émission d'une unité monétaire |
| | Stratégies | Sécurisation du registre, neutralisation du |

75 Exemples d'événements ou phénomènes examinés ou cités par Foucault : la folie, la maladie, la mort, le crime, la sexualité, la disette...

| | | |
|--------------------------|-----------------------------------|---|
| | | pouvoir (au sens de la théorie politique) |
| <i>Limite à l'action</i> | Technique ou mécanisme de pouvoir | Le protocole de consensus |
| <i>Gouvernement</i> | Technologie de pouvoir | Séparation épistémique dans l'opération de calcul entre le calculateur et l'inscripteur |

Tableau 3 : Correspondance entre le langage de Foucault et l'analyse d'Ethereum

2.3. Ethereum dans un art de gouverner par le calcul informatique

Cette sous-section montre que l'objectif de « sécurité » vu à la section précédente est posé sur le calcul informatique qui cadre les capacités d'action des Internautes par la décentralisation de l'architecture informatique et politique des entités coordonnées par le protocole. Cet objectif est confronté à la notion mobilisée par Michel Foucault pour désigner une technologie de pouvoir qu'il appelle « mécanisme de sécurité » : Ethereum fait du Web un champ d'intervention, gouvernant les événements « inscriptions » en s'appuyant sur la circulation des données, prise comme une réalité qui est contrôlée plutôt que niée ou évitée. Enfin et à l'aide de quelques exemples issus de l'histoire de l'informatisation, cette section plaide pour une analyse des blockchains dans un art de gouverner par le calcul informatique compris comme une double opération d'exécution de règles (ou de code) et d'inscription du résultat de ces règles.

Sécuriser le calcul par la décentralisation

Un pan du champ de savoirs et d'hypothèses mobilisé dans la construction d'Ethereum tient dans la notion de « décentralisation ». Nombre de ces savoirs et hypothèses sont repris de Bitcoin et de son architecture informatique, notamment l'imaginaire d'une société constituée d'individus souverains coordonnés par un système autonome, ainsi que son corollaire : chaque membre de ce corps social est un ennemi en puissance qui doit être agencé par le protocole de consensus vu comme mécanisme de coordination de l'ensemble.

Chapitre 1. Mystique du protocole : calculer sans connaître

Le prolongement de cet imaginaire apparaît dans l'examen que fait Vitalik Buterin du concept de décentralisation, « *the raison d'être* » des blockchains, dans un article intitulé « *The Meaning of Decentralization* » (Buterin 2017a). Le créateur d'Ethereum proposait de clarifier ce que « ce mot [décentralisation] signifie réellement ». La décentralisation articule l'imaginaire de Bitcoin avec celui repris pour Ethereum. Elle qualifie le calcul, non plus pour mettre à jour des unités de compte, mais pour produire une relation numérique au sens d'inscription dans une base de données elle-même décentralisée. À l'époque, Buterin participait sur le ton de l'essai à une controverse qui opposait des promoteurs de différentes cryptomonnaies s'accusant mutuellement de « centralisation ». L'opposition la plus nette, sur laquelle je reviendrai au Chapitre 4, opposait les promoteurs de Bitcoin et d'Ethereum. Elle participa à une scission d'Ethereum en deux infrastructures distinctes.

Buterin distinguait « trois types » ou « trois axes séparés » de décentralisation dans l'opération de calcul informatique. La (dé)centralisation « architecturale » pose les questions du nombre total d'ordinateurs physiques composant un système et du nombre d'ordinateurs en panne simultanée que le système peut tolérer pour produire un calcul correct. La (dé)centralisation « politique » pose la question du nombre d'individus ou d'organisations contrôlant les ordinateurs constituant le système calculateur. La (dé)centralisation « logique » pose la question de la forme des structures de données et des interfaces que le système présente et maintient, selon un spectre d'un « objet monolithique » (centralisé) à « essaim amorphe » (décentralisation). Pour ce dernier axe, Buterin propose de tester l'« heuristique » suivante : si le système est coupé en deux parties incluant chacune des fournisseurs (calculateurs) et des utilisateurs (calculés), est-ce que chacune des deux parties continuera d'opérer comme des unités indépendantes ? Cette proposition conceptuelle est illustrée par tableau à trois entrées, pour chacun de ces trois axes, reproduit en Figure 4.

Chapitre 1. Mystique du protocole : calculer sans connaître

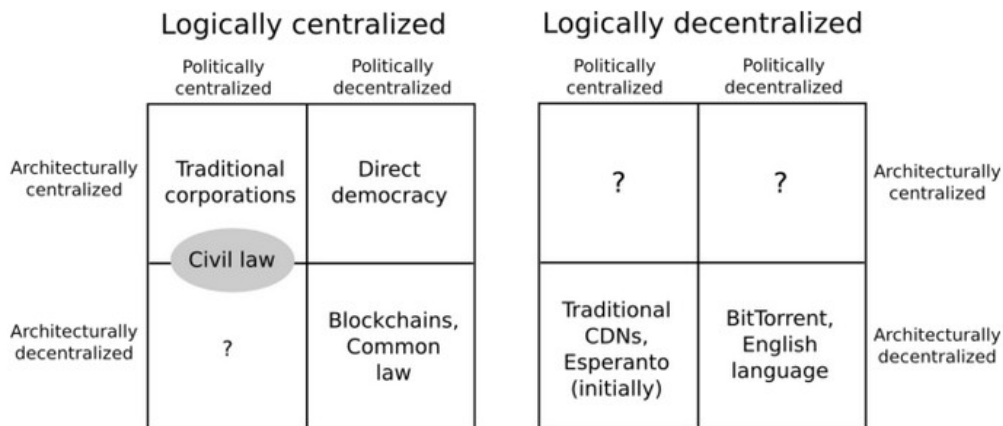


Figure 4 : Reproduction de la représentation des trois axes de la (dé)centralisation selon Buterin (2017a)

Buterin compare, pêle-mêle et comme des « systèmes » : des langues, des protocoles informatiques, des formes juridiques, des régimes politiques, des formes d'entreprises. Par exemple, les « entreprises traditionnelles » sont politiquement centralisées, car elles ont « un PDG » ; architecturalement centralisées, car elles ont « un siège social » ; et logiquement décentralisées, car « on ne peut pas vraiment les couper en deux », écrit Buterin. À l'inverse, les langues vivantes sont logiquement décentralisées, car l'anglais parlé par deux personnes « n'a pas besoin d'être en accord » avec l'anglais parlé par deux autres personnes ; elles sont décentralisées architecturalement dans la mesure où elles n'ont « pas besoin d'une infrastructure centralisée pour que le langage existe » ; elles sont enfin politiquement décentralisées, car aucune personne ne peut, seule, les contrôler. Voici l'interprétation que donne Buterin pour les blockchains :

*Blockchains are **politically decentralized** (no one controls them) and **architecturally decentralized** (no infrastructural central point of failure) but they are **logically centralized** (there is one commonly agreed state and the system behaves like a single computer) (Buterin 2017a)*

Pour Buterin, le protocole inspiré de Bitcoin (repris par les blockchains, dont Ethereum) répond à un objectif essentiel : sécuriser n'importe quel calcul contre tout événement possible du monde. Pour cela, une multitude d'acteurs calculent de manière déterministe (centralisation logique) en évitant toute dépendance vis-à-vis d'une autre entité qui dicterait

Chapitre 1. Mystique du protocole : calculer sans connaître

comment calculer (décentralisation politique) ou contrainte par la forme de l'infrastructure lie ces acteurs ensemble (décentralisation architecturale). La décentralisation (à la fois architecturale et politique) prévient ainsi tout événement vu comme menace pour l'opération de calcul : pannes, attaques, collusions.

Premièrement, le calcul est sécurisé s'il est « tolérant aux pannes », comme le sont les hôpitaux avec les groupes électrogènes ou les portefeuilles financiers par la diversification des actifs pour Buterin. Mais de telles stratégies ne préviennent pas le risque de « *common mode failure* », un principe d'ingénierie qui prévient l'origine commune de pannes dans des systèmes indépendants. Par exemple, un employé véreux peut introduire une faille de panne dans chacun des groupes électrogènes. La tolérance aux pannes suppose donc non seulement de se prémunir de défaillance technique, mais aussi de la communauté qui « gouverne le protocole dans son développement », elle-même sujette au risque de « panne ». Buterin identifie différents stratégies pour se prémunir de ce risque : se prémunir de bugs introduits par une équipe de développement (ou de recherche) travaillant à faire évoluer l'infrastructure en multipliant les logiciels permettant d'administrer les nœuds des *miners* et démocratiser la connaissance technique ; bâtir des algorithmes de consensus évitant la centralisation du minage qui pourrait conduire un gouvernement à mettre le réseau en péril pour des motifs de sécurité nationale ; diversifier les fournisseurs de matériel utilisés par les *miners* pour éviter que leur matériel soit contraint ou soudoyé pour insérer une porte dérobée ; et éviter de concentrer les coins (bitcoins, ethers, etc.) sur une même plan d'échange qui pourrait les détourner.

Deuxièmement, le calcul est sécurisé s'il « résiste aux attaques ». Ce critère suit un raisonnement économique en deux étapes. D'abord, et comme cela a été discuté à la section précédente, les *miners* ont « intérêt » à valider les transactions de manière conforme au protocole, quel que soit leur membre. Mais Buterin, qui raisonne selon des principes de théories des jeux, remarque que ce raisonnement théorique ne tient pas compte de risques pesant sur les personnes elles-mêmes : s'il était menacé de mort, est-ce qu'un *miner* préférerait mourir ou perdre de l'argent ? La décentralisation, en dispersant les différents participant au réseau, le sécuriserait. Au contraire, la concentration favorise les attaques.

Chapitre 1. Mystique du protocole : calculer sans connaître

Buterin remarque une « asymétrie attaque/défense » en faveur de l'attaquant dans le « monde moderne » en général : bâtir un immeuble peut coûter 10M\$ à construire et seulement 100k\$ à détruire. Selon ce raisonnement, éviter les attaques impose de bâtir des protocoles de consensus détectant les concentrations matérielles, de distribuer les équipes de développement y compris géographiquement, et les protocoles de consensus doivent intégrer des modèles économiques et de résistance aux pannes dès leur conception⁷⁶.

Troisièmement, le calcul est sécurisé s'il « résiste aux collusions », au sens de « coordinations qu'on n'aime pas » (Buterin 2017b), ou situations particulièrement dangereuses quand un sous-groupe est capable de se coordonner alors que les autres sont dans l'incapacité de le faire. Le concepteur donne des exemples de « coordinations non désirées », pour souligner que ce danger est intégré par des « institutions sophistiquées », comme les lois instaurant la concurrence ou la limite du nombre de parties que deux joueurs d'échecs sont autorisés à jouer ensemble. Les protocoles blockchain inspirés de Bitcoin supposent que les acteurs sont en situation de jeu, et que leurs décisions sont prises indépendamment les uns des autres⁷⁷. Buterin met en garde : le système pourrait agir comme un monopole guidé par un seul intérêt propre. Par exemple, en 2017, plus de 90 % de la puissance de calcul totale de Bitcoin était concentrée entre huit *miners*⁷⁸. Qu'ils se coordonnent explicitement ou pas, ces huit dirigeants étaient susceptibles de s'organiser, d'avoir un intérêt commun. Un autre exemple indiqué par Buterin : les développeurs d'un protocole de consensus pourraient tous être employés par la même entreprise, être de la même famille ou être assis dans la même pièce. Pour éviter ce type d'écueil, Buterin invite à développer des techniques pour répondre à ce qu'il voit comme un « paradoxe » : se coordonner en « communauté » en évitant les « mauvaises coordinations ». Il suggère de se fier aux utilisateurs, seul groupe qui est « décentralisé dans les règles » à ses yeux⁷⁹. Il

76 Je reviendrai au Chapitre 4 sur la traduction pratique de ce raisonnement dans l'organisation de la « communauté Ethereum ».

77 Avec le vocabulaire de la théorie des jeux, l'auteur parle d' « *uncoordinated choice model* ».

78 Ces *miners* étaient des dirigeants de sociétés spécialisées dans le minage, disposant d'entrepôts construits souvent à proximité de lieux de production d'électricité pour optimiser la rentabilité de l'activité de minage à grande échelle. On parle alors de « fermes de minage ».

79 Buterin désigne cet objectif par « *undesired-coordination-avoidance* » en réponse à l' « *uncoordinated choice model* ».

insiste sur l'importance de bâtir des protocoles qui résistent à la coordination, tout en cherchant à identifier des moyens de favoriser suffisamment de coordination pour que le protocole puisse évoluer en distinguant les bonnes et les mauvaises formes de coordinations.

Ethereum : dispositif de sécurité pour le Web

La notion de « sécurité » est centrale dans la politique de Bitcoin comme dans celle d'Ethereum. Dans les deux cas, elle qualifie un objectif assigné au registre, objet qui donne une réalité contrôlable aux relations numériques (monétaires, ou traces d'exécutions de contrats). Ce terme est également employé par Foucault qui se consacre à des dispositifs de pouvoir d'un genre particulier, qu'il appelle « mécanismes de sécurité » dans *Sécurité, Territoire, Population*. L'auteur les voit comme mécanismes de contrôle social qui modifient le destin biologique de l'espèce humaine. Un enjeu de son analyse était de déterminer si l'économie générale de pouvoir était en train de devenir de l'ordre de la sécurité, c'est-à-dire si (et comment) nos sociétés étaient dominées par une technologie de pouvoir particulière qu'il appelait « technologie de sécurité ». Les paragraphes qui suivent confrontent cette thèse et cette notion à celle de technologie de pouvoir d'inscrire, proposée à la sous-section précédente.

Foucault voit l'estimation de probabilités portant sur une population une caractéristique essentielle des mécanismes de sécurité. Le calcul de probabilité est central dans la sécurisation du registre de Bitcoin comme dans celle d'Ethereum : Buterin envisage différents événements probables (panne, attaque, collusion) susceptibles de menacer la sécurité du registre, et les situe par rapport à des estimations portant sur les individus (comme le niveau de concentration des *miners*, ou le taux de panne acceptable pour que le système tienne). Plus spécifiquement, Foucault distingue ces mécanismes de sécurité des mécanismes juridico-légaux et disciplinaires selon trois axes.

Premièrement, l'espace de la sécurité renvoie au temporel et à l'aléatoire, qu'il faut inscrire dans un espace où une circulation s'opère (comme des maladies, ou du grain) appelé un « milieu ». C'est à l'intérieur de ce milieu que « bouclent les effets et les causes » (Foucault

Chapitre 1. Mystique du protocole : calculer sans connaître

2004a) : le milieu est un champ d'intervention dans lequel on atteint une population. Ce rapport à l'espace se distingue du territoire, peuplé soit de sujets de droit capables d'actions volontaires ; c'est le cas des mécanismes juridiques avec l'exercice de la souveraineté, ou disciplinaires avec l'atteinte de corps capables de performances.

Ethereum fait du Web un milieu, un champ d'intervention sur des données qui circulent. Cette intervention prend une forme contractuelle. Ethereum fait compter ces données différemment pour chaque individu, en fonction des contrats passés par chacun. Ce milieu est un espace d'intervention dans lequel on atteint des personnes contractantes, individus ou institutions. Le cas fizzy montre qu'Ethereum s'appuie sur la circulation de ces données dans le futur en faisant des données de vol les éléments déterminants, par le déclenchement de contrats, de phénomènes aléatoires (les retards d'avion).

Ethereum is the foundation for a new era of the internet:

- An internet where money and payments are built in.
- An internet where users can own their data, and your apps don't spy and steal from you.
- An internet where everyone has access to an open financial system.
- An internet built on neutral, open-access infrastructure, controlled by no company or person.

Figure 5 : Impression écran d'une partie de la page web ethereum.org en mai 2020

Les concepteurs d'Ethereum annonçaient intervenir sur de larges pans du Web. La page web ethereum.org, portail de présentation d'Ethereum administré par l'Ethereum Foundation, indique en mai 2020 le texte reproduit sur la Figure 5. Ethereum « est la fondation » pour une « nouvelle ère d'Internet ». La monnaie et les paiements deviennent intégrés à Internet, non plus excluants. Le système financier n'aurait plus de barrières, il serait ouvert. Les données des Internautes ne seraient plus détachées mais possédées par les Internautes, les applications ne seraient plus des moyens de captation des données personnelles. L'infrastructure ne serait à la main de personne, elle serait neutre et ouverte.

Deuxièmement, Foucault voit un rapport particulier entre l'événement et le gouvernement ; il illustre ce rapport avec le cas de la disette. Des techniques de gouvernement juridico-

Chapitre 1. Mystique du protocole : calculer sans connaître

légales (agir sur les prix) ou disciplinaires (contraindre à ensemercer ou à arracher) ont engendré des révoltes paysannes au XVII^e siècle. La traduction des principes physiocratiques en gouvernement au XVIII^e siècle relevait du dispositif de sécurité : plutôt que de se concentrer sur la hantise de la disette, l'objectif du gouvernement était étendu à toute la réalité du grain (notamment à l'agriculture et au commerce). C'est sur cette réalité étendue que les physiocrates cherchaient à avoir prise pour éviter la famine, en postulant comme principe fondamental la liberté de commerce, dans la droite ligne du champ théorique duquel ils s'inspirent. Le mécanisme consistait à analyser ce qu'il se passait et à programmer ce qui devait se passer en tenant compte de l'état de la production et du comportement de la population, en élargissant le marché du grain. La disette vue comme un fléau disparaissait (mais pas la rareté du grain, qui continuait de faire mourir des gens). La population dans son ensemble devenait alors l'objectif du gouvernement plutôt que la multiplicité d'individus (qui pouvaient individuellement mourir de faim) ; elle était à la fois objet (des mécanismes) et sujet (dont on dirige la conduite).

Ethereum problématise l'implication d'institutions dans l'événement « formulation de relations *via* le Web » : elles les limitent, les censurent, les divulguent (Figure 5), ou encore les nient (exemple d'AXA). Plutôt que de se concentrer sur la hantise de ces événements, Ethereum remarque que la réalité des relations formulées par ces institutions est double : un calcul et l'inscription de ce calcul. C'est sur cette réalité qu'intervient Ethereum : le réseau est à la fois un dispositif de calcul (exécution des *smart contracts*) et d'inscription du résultat de ces calculs (inscription dans le registre). Le mécanisme vise à se prémunir de toute limite, censure, divulgation, ou négation du calcul et de ses résultats. Pour cela, Ethereum pose comme principe fondamental la liberté de calculer et d'inscrire tout en programmant comment doit se passer (être sécurisé) le calcul et sont inscription. Il permet à tous les acteurs du Web (et plus largement d'Internet) de participer au calcul tout en anticipant les comportements de cette population. D'une part, en cryptant les transactions, Ethereum limite les capacités de divulgation des termes aux parties impliquées dans le contrat. D'autre part, avec le principe de décentralisation du système calculeur (coordonné par le protocole) et comme indiqué dans les paragraphes précédents, Ethereum

Chapitre 1. Mystique du protocole : calculer sans connaître

prévient les comportements de sabotage du calcul qu'ils soient « attaques », « pannes » ou « collusions ».

Troisièmement, Foucault voit un rapport particulier des mécanismes de sécurité à la « réalité ». La discipline concentre, enferme, elle régleme et empêche même les détails, elle détermine ce qui doit être fait, le reste étant interdit. Le système légal, lui, détermine ce qui est interdit. Un dispositif de sécurité fait se développer des circuits plus larges, tout n'est pas autorisé mais le laisser-faire est indispensable (laisser monter les prix ou mourir de faim pour la disette) ; il prend appui sur des détails. Dans le système disciplinaire, ce dont il s'agit est de prendre suffisamment de recul pour saisir le point où vont se produire les choses, qu'elles soient souhaitables ou pas. Dans le mécanisme de sécurité, on ressaisit les choses dans leur nature, dans leur réalité effective, on prend appui dessus en faisant jouer les éléments les uns par rapport aux autres :

*Autrement dit, la loi interdit, la discipline prescrit et la sécurité, sans interdire ou sans prescrire, éventuellement cependant en se donnant quelques instruments du côté de l'interdiction et de la prescription, **la sécurité a essentiellement pour fonction de répondre à une réalité de manière à ce que cette réponse annule cette réalité à laquelle elle répond – l'annule, ou la limite ou la freine ou la règle.** C'est cette régulation dans l'élément de la réalité qui est, je crois, fondamental dans les dispositifs de la sécurité.* (Foucault 2004a : 48)

Selon Foucault, la loi travaille dans l'imaginaire, négativement ; la discipline travaille dans le complémentaire de la réalité ; la sécurité travaille dans la réalité. Foucault voit dans ce principe fondamental des dispositifs de sécurité, considérer que la technique politique ne doit « jamais décoller du jeu de la réalité avec elle-même », un lien profond entre gouvernement et le principe général de libéralisme. Laisser-faire suggère que la réalité se développe et suive son cours selon des lois, des principes et des mécanismes naturels. Cette liberté se comprend au sens moderne de « circulation ». Avec les physiocrates, on voit apparaître une physique du pouvoir, une action comme dans la nature, une régulation qui opère en prenant appui sur la liberté de chacun. Foucault indique que la liberté, plutôt qu'une « idéologie », est une condition du mode de gouvernement qui se déploie dans et par les dispositifs de sécurité.

Chapitre 1. Mystique du protocole : calculer sans connaître

Ethereum intervient sur toute la réalité de la circulation des données, sans la restreindre. La libre circulation des données est postulée et conservée. Mais dans le même temps, Ethereum agit sur cette réalité en instaurant un espace de contractualisation qui s'appuie sur cette circulation, en faisant participer les données aux calculs (mises à jour des contrats). Les données sont traduites en événements par les contrats eux-mêmes, c'est-à-dire par les règles de traitements fixées par les utilisateurs (individus et institutions) supposés avoir librement consenti à ces règles. Le vocabulaire des concepteurs rejoint là encore celui de Foucault : comme le travail des gouvernants inspirés des physiocrates qui « programmaient » ce qui devait se passer, les *smart contracts* « programment » les actions futures sur les parties liées contractuellement en fonction de données connues à l'avance mais selon des valeurs futures.

Ce sont bien de nouveaux « circuits » de données que câble Ethereum. Avec *fizzy*, les données produites par les utilisateurs sont d'abord combinées avec l'algorithme de pricing d'AXA pour établir un contrat qui en fige les termes, en définissant les circuits qui permettront de produire une nouvelle donnée, laquelle indiquera aux parties prenantes le résultat du calcul (l'exécution du contrat). Les données saisies au départ sont figées comme « réalité » du contrat dans la mesure où celui-ci devient impossible à modifier. Les données futures relèvent d'une « réalité future » : toute autre intervention (photo, témoignage, appel à la société d'assurance, etc.) ne sera qu'une fiction qui ne changera nullement la réalité de la (non-)décision de paiement. Les données « d'entrée » du *smart contract* deviennent l'image « naturelle » des phénomènes, et les données « produites » par le *smart contract* rendent réelle l'exécution du contrat. Dans ces deux cas, Ethereum fait prendre à ces « données » le sens « d'obtenues » (Latour 1993) légitimes pour les différents acteurs en présence ; d'abord en posant les sources qui feront foi, ensuite en instaurant le caractère « opposable » de l'information produite.

La centralisation du calcul dans la problématisation politique de l'informatisation

L'histoire de l'informatisation est marquée par des asymétries entre entités calculatrices et

Chapitre 1. Mystique du protocole : calculer sans connaître

entités sur lesquelles porte le calcul. Dans *Affaires privées. Aux sources du capitalisme de surveillance*, Christophe Masutti donne une version riche et récente de cette histoire, guidée par le problème de la surveillance⁸⁰ et de son rapport au développement du capitalisme par la valorisation des données (Masutti 2020 : 25). Masutti inscrit le « capitalisme de surveillance » contemporain dans une généalogie du processus d'informatisation qui se déploie depuis les années 1960. L'auteur voit différentes dynamiques qu'il décrypte en portant attention aux formes de circulation de l'information dans les réseaux informatiques. Comprendre ces formes permet d'identifier le sens que prend surveillance à différentes époques : « Faire une histoire de la surveillance suppose à un moment ou à un autre, de se demander à quel paradigme nous avons désormais affaire » (Masutti 2020 : 291). Les paragraphes qui suivent résument quelques épisodes de cette histoire pour faire apparaître un fil rouge lié à l'architecture à informatique, qu'il soit question de contrôle, de surveillance ou de gouvernement de l'État : l'asymétrie entre des calculateurs investis d'autorité institutionnelle et des fournisseurs d'informations numérique à ces calculateurs.

L'informatisation s'est d'abord développée avec l'ordinateur *mainframe*, ou ordinateur de grande puissance de traitement qui servait d'unité centrale à un réseau de terminaux, points d'accès au calculateur. Cet ordinateur peut se comprendre comme une bibliothèque de données consultable en continu par un très grand nombre d'utilisateurs. D'abord calculateurs scientifiques, ils commencèrent à entrer dans l'industrie en bouleversant l'organisation des entreprises à partir des années 1960 en offrant du « temps de calcul » à distance. Chacune des unités organisationnelles constituaient ce qui s'appellera plus tard un « système d'information ». Ce modèle d'une organisation calculant centralement pour des entités réparties fut interprétée comme contrôle d'un pouvoir central de l'organisation, et plus généralement comme une fin au niveau de la société entière avec le thème de la

⁸⁰ Masutti souligne, comme Alexandre Rios-Bordes qui prend pour objet la forme de surveillance particulière opérée par les administrations secrètes d'État (Rios-Bordes 2018), que la surveillance est un objet en vogue, regroupé sous le label « *surveillance studies* ». Pour ces deux auteurs, les *surveillance studies* font apparaître une systématisation et une routinisation des pratiques de surveillance tendant à participer à une « société de surveillance ». Masutti, qui regrette un biais cumulatif dans l'analyse de ces travaux, cible certaines pratiques de surveillance aux frontières troubles entre États et entreprises pour comprendre l'avènement du « capitalisme de surveillance ». Pour l'auteur, ce dernier se nourrit de traces pour donner corps à l'économie, aux techniques, à la société. Cet ouvrage offre un parcours détaillé des questions organisationnelles mais aussi infrastructurelles et matérielles qui permettent de comprendre la « surveillance » dans et par les systèmes informatiques comme un problème historique.

Chapitre 1. Mystique du protocole : calculer sans connaître

« société de contrôle ». Ce type de critique représente la société selon les transformations successives liées à sa soumission aux techniques de l'information et au postulat que l'information est le pivot du contrôle⁸¹. L'informatique au service de l'homme imaginé à la fin des années 1950 et rêvée par les cybernéticiens laissait alors la place à une informatique productiviste qui reprenait les avantages opérationnels de l'automatisation. Dans le même temps, la décision économique devenait dépendante des techniques de contrôle par et avec lesquelles les décisions étaient prises.

Ainsi dès les débuts de l'informatisation, le calcul signifiait relation de contrôle entre l'utilisateur du système (fournisseur d'informations) et le calculateur lui-même qui prenait des décisions (notamment économiques) pour un ensemble englobant le fournisseur d'informations (entreprises). Le thème du contrôle par une entité centrale calculatrice se prolonge avec l'échec d'instruments cybernétiques de gouvernement d'États. Masutti cite par exemple le projet Cybersyn, envisagé comme un système planifiant le gouvernement sous forme semi-automatique de manière à rationaliser la décision en contournant les « difficultés locales » propres aux fournisseurs d'informations⁸². Ce projet mettait en application des connaissances développées en recherche opérationnelle, une discipline croisant économie et informatique, visant à proposer des décisions à partir d'informations assemblées dans un calculateur. Pour Andrew Pickering qui s'est intéressé en détail à cet épisode, ces acteurs étaient animés par l'idée qu'il était impossible de connaître le monde mais qu'il était possible d'expérimenter en temps réel dans son émergence (Pickering 2009). Bien que ces ambitions de contrôle dans de grandes bases de données finirent par s'étioler, Masutti voit un prolongement avec le développement d'une science des organisations « justifiant parfois d'elle-même son existence » (Masutti 2020 : 104).

Du thème du contrôle, Masutti voit un basculement pour la surveillance avec le développement des réseaux interconnectés. Masutti explique que l'échec de ces outils tient au fait qu'ils prétendaient donner à la décision une rationalité qu'ils étaient incapables de

81 Beniger a nuancé ces critiques ; en montrant que la « société de l'information » et « société de contrôle », se sont mutuellement consolidés (Beniger 1986).

82 Ce projet porté par le gouvernement Allende portait l'idéal socialiste de l'économie en traduisant les formes classiques de planification par une réappropriation populaire des outils de production.

Chapitre 1. Mystique du protocole : calculer sans connaître

produire. Dans les entreprises, les ordinateurs *mainframe* permirent à des entreprises, en particulier dans le secteur financier, d'augmenter leur productivité. Avec la transmission de données par paquets, l'architecture des systèmes se décentralisa : les données produites localement étaient ensuite centralisées pour produire des décisions. Les modes de production tayloristes de l'information firent place à des modes de production collaboratifs. L'enjeu n'était alors plus tant de contrôler que de prendre les bons choix économiques ou gestionnaires. Au lieu d'une société de contrôle qui était anticipée avec les tentatives technologiques qui confondaient information et décision dans des mécanismes technocratiques comme Cybersyn, c'est l'économie de la surveillance qui s'est développée. À la différence du contrôle, la surveillance consiste à comprendre et influencer les choix (Masutti 2020 : 131).

Dans les années 1970, les données personnelles devinrent des objets concrets : on commença à associer l'agrégation d'informations à des « faits ». Les enjeux de la construction d'un individu « informatisé » (*computerized man*) a été déclenchée par un projet à l'échelle fédérale des États-Unis, le National Data Center. Le danger sur la vie privée devenait alors un enjeu juridique et civique, pas seulement intellectuel. La critique portait notamment sur le fait que le gouvernement pourrait tirer des « faits choisis » par la construction de bases de données centralisées, en opposition aux discours promouvant ces dispositifs pour des raisons budgétaires. Masutti analyse cet épisode comme une tentative étatique de se prémunir contre la multiplication de bases de données sur lesquels le gouvernement n'avait alors que peu de prises. C'est finalement la mise en réseau des institutions et l'émergence d'Internet qui finirent par répondre au « manque » d'une base centrale en interconnectant les banques de données des différents services d'État (Masutti 2020 : 199).

Dans tous ces épisodes et quelle que soit sa formulation, le problème politique est posé par une asymétrie du calcul (ou des manières de calculer) entre des institutions et des utilisateurs (employés, citoyens, ou consommateurs). Les ordinateurs *mainframe* commençaient par louer du temps de calcul sur un ordinateur partagé, puis progressivement, le calcul est devenu accessible à différentes entités avec les micro-

Chapitre 1. Mystique du protocole : calculer sans connaître

ordinateurs mais aux méthodes standardisées par la diffusion de logiciels standards dans chacune de ces entités. Le « système » se comprenait alors de plus en plus comme un réseau. La centralisation de l'information et de son traitement relevaient de postures stratégiques pour des États comme pour des entreprises qui cherchaient à prendre des décisions.

Avec Ethereum, le « système » est un « réseau » qui produit des calculs, lesquels ne relèvent pas de la responsabilité d'un acteur en particulier. Ajar décrit Ethereum comme « un gros ordinateur », un « ordinateur monde ». Le calcul ne produit plus une information dans une base de données d'une entité donnée, entreprise ou État. L'information produite, qu'elle soit « donnée » ou « décision », est l'exécution d'un contrat, formalisé dans du code antérieurement au calcul lui-même, par des contractants libérés au moment où le contrat est signé. Ethereum propose un modèle de base de données où une forme de « temps de calcul », en termes d'exécution de *smart contracts* et de mise à jour du registre, est là aussi partagé.

Conclusion du chapitre

L'organisation d'une rupture épistémique entre inscription et signification d'un calcul est la qualité politique centrale dont Ethereum hérite de Bitcoin. Elle est le résultat de l'agencement produit par le protocole, sécurisant le registre et neutralisant toute forme de pouvoir susceptible de s'exercer sur lui. En mobilisant cet objet technique, les concepteurs d'Ethereum font du protocole de Bitcoin un modèle pour une nouvelle organisation politique du Web. Ils renversent la notion de contrôle, comme l'ont fait avant eux les concepteurs de Bitcoin : au contrôle exercé par des institutions sur les relations est substitué le contrôle individuel sur les relations comprises comme résultats de calculs. Cette organisation de l'ignorance des sujets des relations mobilise des connaissances en informatique et l'hypothèse d'un monde peuplé d'entités qui ont la liberté individuelle radicale et la capacité à entrer en compétition comme qualités anthropologiques premières. Les paragraphes qui suivent proposent quelques remarques conclusives.

Premièrement, cette filiation fait de la transaction l'objet à partir duquel un monde est imaginé, substituant le calcul au contrôle des institutions (monétaires comme aux fournisseurs de services du Web). Ainsi, pour Ethereum et le Web, le paradigme relationnel tient dans le couple transaction et contrat plutôt que donnée et service. La notion de contrat dans « *smart contract* » rejoint celle des approches contractuelles de la firme en économie. Elle semble vouloir prouver qu'il existe un espace dans lequel l'incomplétude des contrats (Hart et Moore 1990) peut être dépassée : dès la rédaction (programmation) de ses termes (son code), le contrat (*smart contract*) suppose que l'information (les données) est (sont) parfaite(s). Le réseau lui-même est chargé de vérifier, en toute indépendance car ignorant de la nature du contrat passé par les entités, l'état de l'information nécessaire à la réalisation ultérieure du contrat.

Deuxièmement, la rupture épistémique opérée par la transaction est une politique du calcul. Ce « jeu politique » tient moins d'une quantification à partir de laquelle une action politique peut être envisagée dans ou à côté des institutions (Demortain 2019) que dans la manière

Chapitre 1. Mystique du protocole : calculer sans connaître

d'inscrire le résultat d'un calcul pensé comme état d'une relation entre acteurs contractants librement. Par extension et analogie, l'action publique avec Ethereum serait l'inscription de transactions au registre. Ce chapitre a proposé de comprendre le gouvernement en termes de sécurité plutôt que de discipline, ce que font différentes analyses de l'action publique qui s'appuient sur le vocabulaire de Michel Foucault. Néanmoins, toute comparaison avec la perspective d'une action publique serait hâtive après une analyse restreinte à la « mystique » du protocole. Les prochains chapitres s'intéresseront plus avant à la constitution de coalitions, à l'expertise et aux pratiques partagées à partir et avec les dispositifs qui ont été présentés en termes théoriques dans ce chapitre.

Troisièmement, cette politique du calcul introduite dans l'intime de l'opération de calcul problématise non seulement les institutions, mais plus généralement ce que calculer signifie. Rappelons-nous comment Alan Turing conçoit le calcul mécanisé dans son modèle de « machine » conceptuelle inventée pour définir mathématiquement un système formel (Turing 1936). Cette conception imagée du calcul représente un dispositif qui comporte un ruban, le long duquel se déplace une tête de lecture-effacement-écriture. Chaque case de ce ruban représente une opération ; la tête de lecture lit ce qui est inscrit sur cette case, efface et écrit ou ne fait rien, avant de se déplacer à la case suivante, en fonction des règles. Selon ce modèle, toute règle de calcul peut être réduite à une suite de règles élémentaires. À partir d'une (re)lecture de Ludwig Wittgenstein qui s'était intéressé à la modélisation de son ancien élève Turing, l'historien et philosophe des sciences et des techniques Pierre Wagner rappelle que cette modélisation n'est autre qu'une image conceptuelle traduisant ce que fait un humain devant une feuille de papier quand on dit qu'il « calcule » : examiner un signe, appliquer des règles sur ce signe, puis passer au signe suivant (Wagner 2005). Wagner soutient que le modèle de la machine de Turing ne doit pas être assimilé à une réduction du calcul humain au calcul mécanisé, mais plutôt que les machines qui calculent « sont les hommes » en train de calculer.

Par conséquent, faire calculer un réseau décentralisé et désintéressé par la signification du calcul pose une question démocratique pour les blockchains : quels « sont les hommes » en train de calculer au travers de ces réseaux décentralisés ? L'observation de Wagner

Chapitre 1. Mystique du protocole : calculer sans connaître

transforme les termes dans lesquels la question de la calculabilité est souvent posée, notamment face à l'émergence de technologies comme l'ordinateur ou l'intelligence artificielle. Plutôt que de demander si une machine peut penser ou si elle est intelligente, la question devient celle de la possibilité du calcul par une machine. En l'espèce, la question pour Ethereum présenté comme un « gros ordinateur » pourrait être : un réseau décentralisé peut-il calculer ? Dire qu'une machine calcule, c'est dire qu'une machine suit des règles. Poser la question de la possibilité pour une machine de calculer revient à distinguer, selon Wittgenstein, le suivi de règles et un processus physique (comme le déplacement de la tête de lecture de la machine de Turing, ou l'écriture de l'humain) : dire qu'une personne a obtenu un résultat en suivant une règle n'est pas dire qu'un dispositif physique a permis la production du même résultat par un enchaînement causal (Wagner 2005 : 193)⁸³.

Quatrièmement et en conséquence, l'analyse proposée dans ce chapitre doit être située comme une tentative d'éclairage historique de ce que j'ai appelé la « mystique » du protocole plutôt qu'une analyse « de » la politique de Bitcoin et d'Ethereum. En particulier, les distinctions des deux paragraphes précédents visent à éviter de naturaliser la notion de calcul, et à être attentif à l'interprétation des états physiques du système que l'on considère : aucun dispositif physique n'est en lui-même une machine à calculer. Les trois chapitres suivants analyseront selon des angles différents les interprétations des états physiques du système (du registre). Ce chapitre cherchait à identifier les hypothèses et les visions du monde posées par les concepteurs d'Ethereum dans leur réutilisation du protocole de Bitcoin pour affirmer la fiabilité du calcul en toute situation. Ce faisant, ils font de l'inscription « sécurisée » une loi naturelle, aux résultats prédictibles : en payant la commission adéquate, toute transaction est inscrite. Le système s'adapte pour que cette loi générale soit respectée quel que soit le calcul « toutes choses égales par ailleurs ». En ce sens, le protocole peut être compris comme une *nomological machine* (Cartwright 1999) : il fait répéter des opérations au réseau (exécuter l'algorithme de hachage en guise de compétition matérielle) pour produire un comportement régulier (les validations de

83 Par exemple, dire qu'un panier est composé de sept denrées, car on a acheté trois légumes et quatre fruits au marché, n'a pas la même signification que si un chat produisait la combinaison « $3+4=7$ » sur une calculatrice. On ne dira pas que la machine a calculé le nombre de denrées en suivant les règles du chat.

Chapitre 1. Mystique du protocole : calculer sans connaître

transactions en toutes circonstances) quels que soit le nombre de *miners* ou de transactions à inscrire.

Chapitre 2. Les modes des jetons : instituer par les *smart contracts*

Introduction : l'institutionnalisation des cryptoactifs et le problème de leurs significations

[L]e bitcoin n'est en rien une monnaie, ou même une crypto monnaie. C'est un actif spéculatif. Sa valeur et sa forte volatilité ne correspondent à aucun sous-jacent économique et ne sont la responsabilité de personne. La Banque de France tient à rappeler que ceux qui investissent en bitcoin le font totalement à leurs risques et périls. (Villeroy de Galhau 2017)

Sur le plan juridique, une crypto-monnaie n'est pas une monnaie : elle ne dépend d'aucune institution, ne bénéficie d'aucun cours légal dans aucun pays ce qui rend l'évaluation de sa valeur difficile et ne peut être épargnée donc constituer une valeur de réserve. (Bercy Infos 2022)

Des investissements, mais ni monnaies ni instruments financiers : voilà comment les crypto-monnaies ou cryptoactifs comme le bitcoin et l'ether étaient définis, pêle-mêle, par le Ministère de l'Économie et des Finances français (MEFF) à la suite du régulateur des marchés financiers, l'Autorité des Marchés Financiers (AMF)⁸⁴, en 2022. Ce cadrage était cohérent avec celui de la Banque de France⁸⁵ : cinq ans plus tôt, le gouverneur de la banque centrale François Villeroy de Galhau indiquait déjà que le bitcoin était un « actif spéculatif ». Étiquetée « Épargne et investissements mobiliers », la publication du MEFF était accompagnée de mises en garde : les cryptoactifs présentaient des risques de « bulles spéculatives », de « piratages informatiques » et de « blanchiment des capitaux ». Pourtant

84 Le MEFF indiquait : « Selon l'Autorité des Marchés Financiers (AMF), les « crypto-monnaies » ou « cryptoactifs » désignent « des actifs numériques virtuels qui reposent sur la technologie de la blockchain (chaîne de bloc) à travers un registre décentralisé et un protocole informatique crypté ». » (Bercy Infos 2022)

85 A une approximation sémantique près, qui relevait d'un jeu discursif : le gouverneur de la Banque de France refusait au bitcoin le statut de cryptomonnaie, concept qui n'était pas défini au sens commun que par l'utilisation de la technologie issue de Bitcoin, et qui n'avait aucune définition juridique en 2017. Ce discours doit être situé : François Villeroy de Galhau exprimait une distance ferme de la Banque de France vis-à-vis de Bitcoin à une période d'explosion du cours du bitcoin et des autres cryptomonnaies évalué en monnaies ayant cours légal, comme l'euro ou le dollar, alors que les positions des banques centrales sur les cryptoactifs étaient particulièrement scrutées.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

et dans le même temps, ces institutions publiques chargées de la réglementation financière et monétaire n'intervenaient pas sur ces objets financiers. Elles justifiaient cette position paradoxale par leur mandat, limité à des transferts d'argent comme « instruments financiers » (titres et contrats financiers⁸⁶), qualité qu'elles n'accordaient pas aux cryptoactifs :

En droit français, les crypto-monnaies n'ont pas de statut juridique clair et ne sont pas reconnues comme des instruments financiers. De ce fait, les crypto-monnaies ne sont pour l'heure pas réglementées. (Bercy Infos 2022)

Ces positions illustrent une tendance dans les discussions sur les cryptoactifs : les appréhender et les comme des objets cotés sur des marchés financiers. Cette tendance est au cœur du débat public sur l'institutionnalisation de ces objets, des interrogations sur l'opportunité qu'un État (comme le Salvador) fasse d'un cryptoactif (trop « volatile ») une monnaie légale aux analyses de leur « potentiel », évalué à l'aune de leur cours ou de leur capitalisation de marché⁸⁷. Institutions publiques, promoteurs comme détracteurs des cryptoactifs équipent leurs analyses de chiffres issus d'outils de mesure, de comparaison, de classement des différents cryptoactifs conçus par des acteurs de leur développement qui en font un marché financier cohérent. La Figure 6 représente une vue d'un agrégateur de différentes « places d'échanges » couramment dites « *exchanges* »⁸⁸ (comme Binance, Coinbase, Kraken ou FTX qui a connu une faillite spectaculaire fin 2022). Ces sites web permettent d'acheter et de vendre des cryptoactifs à la manière de bourses d'échanges, les agrégateurs donnent une vue « de marché » consolidée des échanges sur différents *exchanges*.

Comment comprendre l'institutionnalisation des cryptoactifs ? Ce chapitre interroge la réduction des cryptoactifs à des objets cotés sur des marchés financiers. Elle pose deux ensembles de problèmes : elle ignore la diversité des acteurs participant à les constituer et

86 Dans son article L211-1, le Code monétaire et financier indique : « Les instruments financiers sont les titres financiers et les contrats financiers », c'est-à-dire exhaustivement : les titres de capital émis par les sociétés par actions, les titres de créance, les parts ou actions d'organismes de placement collectif.

87 Respectivement, valorisation sur un marché d'une unité et de la somme de toutes les unités émises.

88 Terme vernaculaire que je conserve.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

lisse les multiples significations dont ces objets sont investis. Ce chapitre propose de la dépasser en étant attentif à la pluralité de processus de valorisation dans lesquels ils sont engagés pour saisir leurs dimensions sociales et politiques.

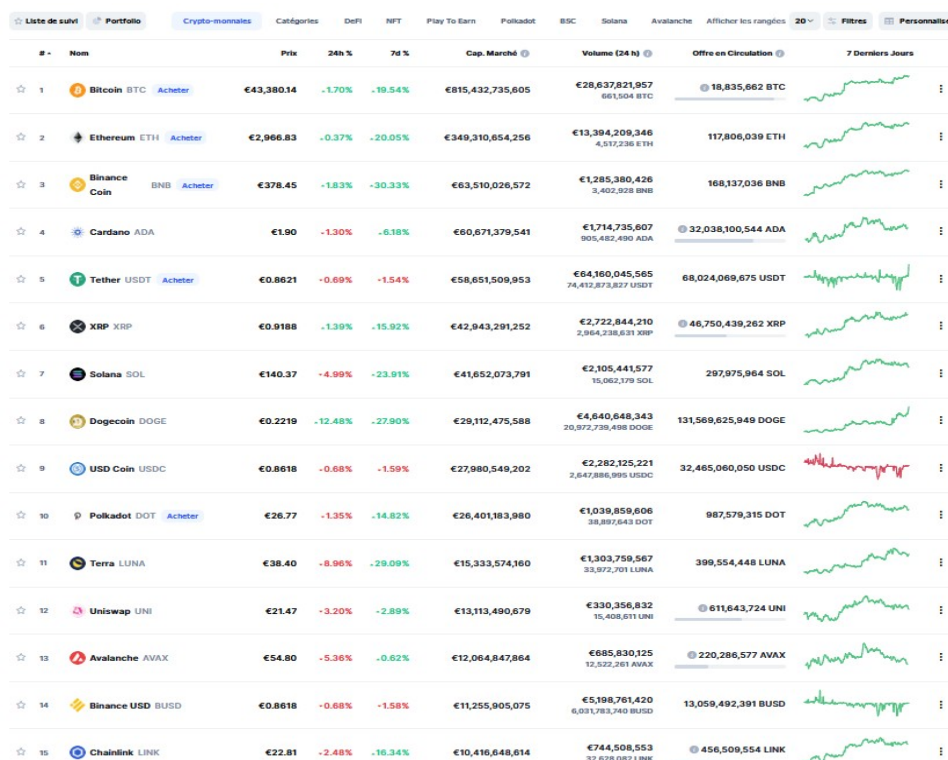


Figure 6 : Page d'accueil du site coinmarketcap.com, octobre 2021

Les cryptoactifs et l'argent : institutions, significations

Les cryptoactifs ne sont pas des monnaies (Tadjeddine 2021), mais ils ont une dimension institutionnelle. Selon le cabinet d'audit et de conseil KPMG et l'Association pour le Développement des Actifs Numériques (ADAN), principale association de promotion des cryptoactifs et de représentation du secteur en France, 8% des Françaises et Français possédaient des cryptoactifs en 2022 (ADAN et KPMG 2022). Une part importante de la population fait confiance à différents acteurs qui assurent la distribution et l'échange d'objets d'un casino géant à en croire les institutions publiques : les cryptoactifs ne

Chapitre 2. Les modes des jetons : instituer par les smart contracts

correspondraient à aucun « sous-jacent économique » (au contraire d'un titre ou un contrat), ne seraient de « la responsabilité de personne » ou « ne dépend[raient] d'aucune institution » (typiquement une société, cotée dans le cas d'actions ou endettée dans le cas d'obligations). Mais dans le même temps, ces institutions leur reconnaissent un caractère institutionnel : en mettant en garde contre la confiance que tout investisseur pourrait accorder à l'achat et la vente de ces objets, elles désignent des réseaux de confiance.

La dimension institutionnelle de l'argent est centrale dans les pistes analytiques développées par la sociologie de l'argent. Cette tradition acte que les relations sont constituées par l'argent, sans que celles-ci puissent être réduites à un cadrage économique : saisir l'argent « dans toute son épaisseur », dans ses dimensions politiques, institutionnelles et morales (De Blic & Lazarus 2021a : 108). À la suite de Viviana Zelizer (1994), elle s'oppose à deux positions opposées qui ont en commun de faire de l'argent un artefact extérieur aux relations : l'argent les corrompt (une condamnation morale de l'argent relayée par des sociologues comme Georg Simmel) ou les faciliteraient (un éloge de l'argent comme facilitateur des échanges, notamment par un large pan de l'économie). Au contraire, l'argent est l'expression d'une puissance politique qui est incarnée dans les institutions en lesquelles celles et ceux qui le manipule accordent leur confiance. Étudier ces institutions permet d'analyser les contours de la puissance politique qu'elles incarnent.

Résumer les cryptoactifs à un marché qui les naturalise en objets disponibles à des investisseurs fait l'économie des longues chaînes de relations entre de multiples acteurs qui instituent les cryptoactifs. Ces chaînes instituantes, qui s'étendent des *miners* récipiendaires des bitcoins ou ethers fraîchement émis jusqu'aux « investisseurs » mis en garde par les régulateurs, doivent être prises pour objet d'enquête pour analyser les dimensions politiques et sociales des cryptoactifs. Cette perspective résonne avec celles proposées par une littérature à la croisée des STS et de la sociologie économique qui substitue à l'étude du « marché » les agencements dont ils résultent (Muniesa et al. 2007 ; Callon et al. 2013 ; Callon 2015). L'étude de ces assemblages matériels et discursifs comme production sans cesse renouvelée des entités semblant *in fine* relever du domaine authentique de l'économie, appelée en général « *economization* » (Caliskan and Callon 2009, 2010) ou

Chapitre 2. Les modes des jetons : instituer par les smart contracts

« *marketization* » pour l'étude des marchés, permet de montrer leur caractère politique. La faillite de la plateforme d'échanges FTX a récemment illustré la fragilité de ces assemblages⁸⁹.

Dès lors, l'argent n'est plus appréhendé comme un fluide qui circule dans une tuyauterie monétaire ou financière institutionnelle posée *a priori*. En particulier, il évite la dichotomie entre finance « traditionnelle » et « alternative », qui suppose que la finance est une institution percutée par des externalités qui feraient bouger ses frontières ; la finance alternative ferait de ces externalités des opportunités, la finance traditionnelle les verrait comme des menaces. La numérisation de l'industrie financière, « *finnovation* » ou « *fintech* » (Zavolokina et al. 2016), suggère notamment que le développement des réseaux et technologies numériques pose des défis à une industrie financière contrainte de se réinventer⁹⁰. Au contraire, l'argent a une « vie sociale » en permanence inventée par ses utilisateurs, individus et groupes autres que les institutions traditionnellement au centre de l'analyse (Dodd 2014). La confiance dans l'argent est constituée en même temps qu'une multitude d'usages et d'une connaissance partagée de ces usages : l'argent est un processus plutôt qu'une chose, il mobilise des imaginaires politiques qui font dépasser les usages présents de l'argent (Dodd 2017 : 316, 320).

Ce point de vue institutionnel sur l'argent suppose d'être attentif à une pluralité de significations. Les travaux de Viviana Zelizer sont à ce titre une référence centrale (1994). La sociologue étatsunienne voit dans l'argent un lien qui prend un sens subjectif et se conjugue au pluriel (*monies*). L'argent est compris comme un objet moral qui forme des relations, modifiant les sujets et le sens que ces derniers lui donne dans des pratiques quotidiennes et matérielles : une opération qu'elle appelle « marquage » (*earmarking*).

89 Sa faillite a entraîné des milliards de dollars de pertes pour les investisseurs lui ayant confié leurs cryptoactifs. Elle a affecté l'ensemble des prix des cryptoactifs, montrant que FTX était un élément central d'un vaste agencement. En outre, elle a permis de révéler que FTX « agissait » directement, par ses dirigeants, sur les responsables politiques en lobbying et financement de campagne électorale, à une époque où se discutaient d'éventuelles futures réglementations des cryptoactifs aux États-Unis (Canton 2022).

90 Les cryptoactifs peuvent à ce titre être vus à la suite des systèmes de paiements en ligne développés depuis le pionnier Paypal au tournant du millénaire, aux applications web et mobile de prêts de pair-à-pair, de micro-crédit, de financement participatif, ou encore aux néobanques.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Recevoir de l'argent implique des manières de dépenser spécifiques à la relation à l'origine de cet argent, y compris dans le cas d'une monnaie nationale, remettant ainsi en cause le principe de fongibilité de la monnaie. Cette intuition a été prolongée par Jérôme Blanc, économiste qui cherche à systématiser la « piste zélizérienne » par l'analyse des « qualités de la monnaie » (2013), un cadre visant à enrichir une théorie socio-économique de la monnaie en donnant aux procédures de conversion de l'argent un sens anthropologique de transformation de ses significations sociales⁹¹.

Je propose de distinguer deux niveaux d'analyse pour saisir l'ampleur des significations des cryptoactifs. D'une part, un même cryptoactif peut prendre différentes significations en fonction des différents marquages dont il peut être l'objet. Par exemple, un cryptoactif peut être un investissement, rémunération, ou participation à un projet politique. D'autre part, les différents cryptoactifs sont marqués de manière spécifique, dès leur émission, c'est-à-dire dans le processus de conception. Les différents cryptoactifs n'ont pas tous les mêmes significations bien qu'ils soient souvent assimilés en une même « classe d'actifs financiers ». La diversité des désignations vernaculaire en témoigne : on les désigne comme « utilitaires » (*utility tokens*), titres financiers (*security tokens*), « stables » (*stablecoins*), unités « non fongibles » (*Non Fungible Tokens* ou *NFT*) ou encore « de gouvernance » (*governance tokens*).

Pour cela, je porte attention aux formes technologiques qui participent directement au marquage. Des anthropologues de l'argent montrent que les technologies participent à former les usages de l'argent, participant à la diversité de pratiques faisant sa « vie sociale ». Bitcoin a été décrit comme « unité de compte » marqué par la technologie de registre distribué (Maurer 2017). L'intérêt pour les technologies comme participantes au marquage a été mis en évidence par des anthropologues qui les incluent dans l'institution des relations par l'argent (Maurer 2015) : les relations sociales et les infrastructures politiques sont configurées par l'argent. Cette littérature met en évidence des paradoxes politiques et éthiques dans la traduction pratique des imaginaires politiques motivant des

91 En supposant l'authenticité de la monnaie dans un corps social, la monnaie se distingue par ses formes, marqueurs socio-économiques qui lui donnent sa moralité, et l'univers symbolique dans lequel il est inséré (Blanc, 2013 : 685, 700).

Chapitre 2. Les modes des jetons : instituer par les smart contracts

innovations monétaires (Clarke et Tooker 2018), notamment concernant les cryptoactifs, en termes de conception monétaire (Maurer et al. 2013), de transformations des mécanismes économiques (Maurer, 2016), et d'accès aux systèmes de paiements (Nelms et al. 2018).

Institutionnalisation des cryptoactifs : enquête sur les significations des jetons

Ce chapitre analyse l'institutionnalisation des cryptoactifs dans leur processus de conception, à une période clé de leur développement, entre fin 2017 et début 2019. Les réseaux étendus d'acteurs participant au développement d'Ethereum à cette époque ont joué un rôle clé. L'importance d'Ethereum ne peut pas se comprendre par sa seule position dans le classement des cryptoactifs par capitalisation, que je propose de voir comme un résultat de l'activité distribuée des réseaux d'acteurs au cœur de ce chapitre. Son unité de compte, l'ether, est en effet un cryptoactif qui a connu une valorisation de marché importante, souvent comparée à celle du bitcoin. Ces deux cryptoactifs ont eux-mêmes participé au développement de l'ensemble des cryptoactifs, mais leur succès tient à une myriade d'autres objets qui leur ressemblent, appelés « jetons ».

Un jeton (ou *token*, souvent préféré à « jeton » en français) est une unité codée dans un *smart contract*. Les jetons ressemblent au bitcoin ou à l'ether, car ils sont transférables et échangeables sur les *exchanges*. Pourtant, ils diffèrent par leurs formes techniques et leurs significations politiques. Je les appellerai « *coins* », selon le vocabulaire des acteurs, comme toutes les unités produites et codées dans le protocole informatique exécuté par tous les participants du réseau physique (qui font « la blockchain »). Je les distingue des jetons, dont les qualités sont programmées unilatéralement par certains utilisateurs dans des *smart contracts*. Les jetons sont l'utilisation ultra-majoritaire des *smart contracts*. La plupart d'entre eux ont été créés sur Ethereum, bien que d'autres plateformes de *smart contracts* existent avec des *coins* spécifiques, comme Solana ou Avalanche (7^e et 13^e positions sur la Figure 6).

Tous les jetons ne sont pas des cryptoactifs. « Cryptoactif » assimile *coins* et jetons comme

Chapitre 2. Les modes des jetons : instituer par les smart contracts

objets marchands, au travers de dispositifs comme les *exchanges*, mais aussi par le langage. *Coins* et jetons sont désignés par des trigrammes. Sur la Figure 6 par exemple, les cryptoactifs BNB et UNI (respectivement Binance et Uniswap, en 3^e et 13^e positions sur la Figure 6) apparaissent côte à côte avec les *coins* BTC (bitcoin) et ETH (ether). Dans le même temps, les notions sont parfois interchangeées. Cette confusion témoigne du flou qui règne autour de ces objets⁹², mais aussi de tentatives de distinctions politiques⁹³ qui seront abordées dans ce chapitre.

Les jetons ont été développés et diffusés par modes. Ce chapitre se concentre sur la période dite des ICO pour « offre initiale de jetons » (*Initial Coin Offering*), un mouvement entrepreneurial qui a accompagné le développement des « jetons utilitaires » (*utility tokens*) notamment entre fin 2017 et début 2018. Les modes sont souvent associées à un type d'usage imaginé, comme les NFT en 2021 ou la finance décentralisée à partir de 2020 ; avec les ICO et les jetons utilitaires, les usages étaient définis à la lumière d'un « Web 3.0 » à faire advenir. Comme le montrera la section 2 de ce chapitre avec les *security tokens*, l'analyse de l'institutionnalisation des cryptoactifs gagne à articuler ces différentes modes.

Plan du chapitre

La première section analyse les jetons dits « utilitaires » (*utility tokens*) et l'opération dite ICO, particulièrement en vogue du deuxième semestre 2017 au premier semestre 2018. Je les analyse comme objets de valorisation dans une perspective pragmatiste (Muniesa 2011), c'est-à-dire : comprendre leur valeur comme le résultat d'actions objets de la description, plutôt que de réduire leur valeur à des qualités subjectives (par exemple comme actifs

92 C'est ainsi que je comprends l'assimilation par le MEFF des *coins* et des jetons, dans leur réponse à la question : « Qui crée les crypto-monnaies ? Elles sont créées par une communauté d'internautes, également appelés « mineurs » à partir d'un algorithme qui génère des « jetons » (ou tokens, en anglais) qui sont ensuite alloués à chaque « mineur » en récompense de sa participation au fonctionnement du système. » (MEFF 2022)

93 Deux exemples de jetons nommés « *coins* » : la catégorie vernaculaire de jetons « stablecoins », et le jeton BNB intitulé « Binance Coin » sur la Figure 1. Dans ces deux cas, les concepteurs des jetons cherchent à donner à leur jeton une force politique propre aux *coins*, conférée par leur émission sur une blockchain. C'est le cas de Binance avec le BNB, mais plus généralement avec les stablecoins qui sont construits pour être « stables » comme des monnaies d'État (qu'ils répliquent) et qui elles-mêmes incarnent la « stabilité ».

Chapitre 2. Les modes des jetons : instituer par les smart contracts

spéculatifs selon les institutions de régulation, ou comme pièces essentielles d'un « Web3 » pour les concepteurs d'Ethereum) ou objectives (par exemple leurs cours sur les *exchanges*). L'analyse de ces actions montre que différents types de jetons sont impliqués dans la mise en existence de ces jetons utilitaires. Alors que ces derniers problématisent l'économie numérique, différents jetons participent à cette problématisation en prenant des significations variées. Les jetons sont imaginés comme briques élémentaires d'une ingénierie relationnelle qui prend des formes non nécessairement monétaires. Ainsi, cette section nuance le rapport causal parfois signalé entre imaginaire des innovateurs et formes techniques en portant attention à la diversité des chaînes qui instituent ces jetons.

Les matériaux mobilisés dans ce chapitre ont été collectés entre février 2018 juin 2019. La section 1 s'appuie principalement sur de matériaux collectés à Singapour en février 2018. Dix des dix-huit entretiens réalisés sur place étaient avec des entrepreneurs ; les neuf autres étaient des cadres de grandes entreprises ou responsables d'administrations publiques. Parmi ces dix entrepreneurs, neuf construisaient des jetons utilitaires : je découvrais alors que les jetons utilitaires était une mode qui battait son plein. La section 2 s'appuie principalement sur des matériaux collectés en France à partir d'observations systématiques de meetups organisés par ConsenSys, une société d'incubation de startups, d'investissement et de conseil spécialisée dans les cryptomonnaies et fondée par un des cofondateurs d'Ethereum. Ces événements réunissaient différents acteurs constituant ce qu'ils appelaient un « écosystème ».

La section 2 analyse l'asymétrie entre, d'une part, un ensemble de concepteurs qui voient dans les cryptoactifs un foisonnement de significations, et d'autre part, leur diffusion comme des objets cotés sur de marchés financiers, comme un moteur de leur institutionnalisation. La conception des jetons n'était pas isolée d'une société qu'elle serait venue percuter pour le meilleur ou pour le pire. Elle se développait au travers de réseaux d'entrepreneurs et d'institutions publiques qui, à Singapour comme en France, voyaient ensemble ces objets comme des innovations ayant une dynamique propre, qu'il fallait encourager plutôt que problématiser, au risque d'en diminuer la vigueur et de « manquer le train » de cette innovation. Cette section lie une préoccupation méthodologique et

Chapitre 2. Les modes des jetons : instituer par les smart contracts

analytique. Je présente les meetups organisés par ConsenSys comme postes d'observation de l'institutionnalisation des cryptoactifs au long cours. Je mobilise certains de ces matériaux pour montrer qu'en réduisant la problématisation des jetons utilitaires à des objets marchands, les institutions publiques et différents portes-paroles du secteur des cryptoactifs en France favorisaient leur diffusion en laissant aux concepteurs le soin de définir leurs significations.

1. Les jetons : anatomie sémiotique de la conception du Web décentralisé

Les jetons dits « utilitaires » ont joué un rôle historique important dans la construction d'Ethereum, dans la popularisation des cryptoactifs au sens large, et dans l'engouement pour la « technologie blockchain » entre 2017 et 2018. La presse spécialisée s'est largement enthousiasmée en voyant dans leur émergence l'avènement du « Web 3.0 » annoncé depuis plusieurs années par les promoteurs d'Ethereum, alors que des critiques des cryptoactifs ont eu tendance à assimiler l'ensemble des cryptoactifs et la blockchain à un phénomène de spéculation douteuse illustré par des « arnaques » qui ont défrayé la chronique. Cette section propose une autre analyse du développement des jetons utilitaires. Je les analyse dans un processus de valorisation étendu aux significations multiples, en observant l'imagination financière comme un phénomène culturel et politique (Muniesa 2021). Cette section s'appuie sur des matériaux collectés à Singapour en février 2018, plus marginalement à Paris dans les mois qui suivirent, ainsi que sur des observations d'arènes de discussion et de publication en ligne.

Dans cette section, je considère les jetons utilitaires par les yeux de leurs concepteurs : des objets imaginés comme relations d'un Web en cours de « décentralisation ». Ces relations engagent des utilisateurs attendus de services Web, imaginés autour de « plateformes » qui seraient autonomes et décentralisées. La première sous-section analyse la vie imaginée des jetons utilitaires. Je suis les associations qu'ils forment, jusqu'aux « *exchanges* ». D'autres jetons entrent alors en scène. Ils témoignent d'une ingénierie socio-technique plus sophistiquée que l'imaginaire de plateformes et de marchés bifaces ; la notion d'agencement marchand (Callon et al. 2013) est plus juste empiriquement et plus riche analytiquement. Dans la deuxième sous-section, je montre que les jetons sont une technique entrepreneuriale générique qui ne se limite pas au télescopage des jetons utilitaires avec des dispositifs financiers comme l'ont relevé certaines études critiques de ces objets (Zook et Grote 2020). Les deux cas retenus témoignent plutôt d'une grande richesse de significations : la programmabilité des *smart contracts* permet de concevoir finement des

opérations de capitalisation (Muniesa et al. 2017), et parfois d'*assetization* (Birch & Muniesa 2020). Enfin, je prends différentes coupes de ce processus étendu de rencontres entre des entrepreneurs et des investisseurs pour souligner son caractère institutionnel, et par-là proposer une explication alternative à la stigmatisation de pratiques individuelles douteuses ou naïves.

1.1. Les jetons utilitaires : imaginaire d'autonomisation des plateformes du Web

Début 2018 : foisonnement de DApps

Au passage de 2017 à 2018, cryptoactifs et cryptomonnaies se popularisaient, passant des magazines spécialisés, des arènes de discussions de passionnés en ligne ou des salons de grandes banques aux conversations familiales des festivités de fin d'année. Le développement des jetons d'Ethereum tenaient un premier rôle, quoi que discret à l'époque, dans cette fièvre spéculative pour des objets financiers représentant pêle-mêle de nouvelles « monnaies » numériques, de nouveaux services Web, ou plus prosaïquement des perspectives de profits rapides et apparemment sans risque.

Cet engouement était contemporain de l'émergence d'un type d'application Web appelé « *decentralized autonomous application* » (DApp), promues comme briques élémentaires d'un nouveau Web, appelé « Web décentralisé », « Internet décentralisé » ou « Web 3.0 » à l'époque. Les DApps avaient la particularité de fonctionner avec des jetons construits avec des *smart contracts* d'Ethereum. Le nombre de ces applications s'est accéléré en 2017 pour atteindre un rythme de plus de 100 nouvelles DApps par mois selon le site « State of the DApps », référence des acteurs au moment de l'enquête (Figure 7). Selon ce site qui ambitionne de référencer les différentes DApps, 2803 étaient bâties sur Ethereum en mars 2020, soit plus de 80 % de toutes les applications décentralisées construites sur des blockchains comme Ethereum.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

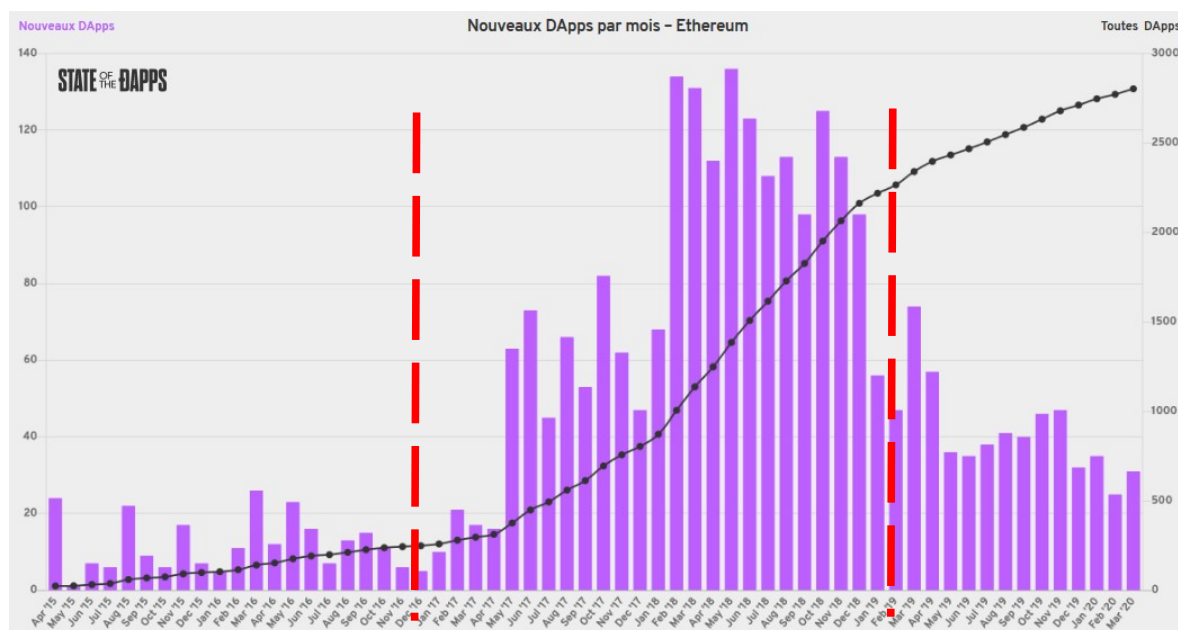


Figure 7 : Nombre de nouvelles DApp par mois (StateOfTheDApp 2020) – mes ajouts en rouge

Ce mouvement d'ampleur m'était inconnu quand j'arrivais à Singapour la première quinzaine de février 2018 pour explorer les développements de la blockchain dans la cité-État, connue comme haut lieu mondial de la technologie. Parmi les différents entretiens conduits sur place figuraient dix startups. Neuf d'entre elles avaient une activité centrée sur le développement d'applications sur Ethereum. J'ai fait ce constat sur place, sans m'être donné Ethereum comme objet central d'enquête à ce moment-là. Les contacts avaient été pris dans les semaines qui précédaient notre venue en fonction de la visibilité des acteurs dans la presse locale et spécialisée ainsi que de leur participation à des conférences locales sur le thème de la « blockchain ». Sur ces neuf startups, huit développaient des DApps, et une (sur laquelle je reviendrai en sous-section 1.3) proposait des services de développement de DApp pour d'autres startups.

Ces huit startups avaient en commun d'imaginer que des jetons représentent des objets physiques ou numériques. À la différence des premiers, ces derniers étaient vus comme facilitateurs d'échanges, notamment vis-à-vis d'acteurs « intermédiaires ». Ces startups et les objets correspondants sont résumés dans le Tableau 4. Averspace et Popety représentaient des biens immobiliers par des jetons, pour faciliter des ventes de pair-à-pair

Chapitre 2. Les modes des jetons : instituer par les smart contracts

ou pour améliorer le marché immobilier ; Bluzelle représentait du stockage informatique par des jetons ; Digix représentait des fragments de lingots d'or stockés dans des coffres par des jetons ; Indorse représentait des données personnelles liés à de parcours professionnels par des jetons ; Kyber Networks, LALA World et TenX représentaient des cryptoactifs⁹⁴ ou des monnaies bancaires par des jetons *ad hoc*.

| <i>Projet</i> | <i>Objet en jeton</i> | <i>Vision des fondateurs</i> |
|----------------|-----------------------|---|
| Averspace | Biens immobiliers | Négocier et conclure des ventes immobilières de pair à pair, sans agents immobiliers, et inscrire ces ventes sur la blockchain d'Ethereum. |
| Bluzelle | Stockage informatique | Bâtir une base de données décentralisée qui manque au web décentralisé que font advenir les blockchains. |
| Digix | Lingots d'or | Proposer un actif échangeable dans les mêmes conditions que tout cryptoactif, tout en ayant la « réalité » et la « stabilité » de l'or physique. |
| Indorse | Données personnelles | Rémunérer les individus publiant leurs compétences ou réussites professionnelles ou confirmant celles de leurs collègues sur un réseau social décentralisé. |
| Kyber Networks | Cryptoactifs | Échanger et convertir des jetons et des cryptomonnaies directement <i>via</i> la blockchain d'Ethereum, sans l'intermédiaire d' <i>exchanges</i> « centralisés ». |
| LALA World | Monnaies bancaires | Proposer aux « exclus » du système bancaire, en particulier les travailleurs migrants, des solutions de prêts et de paiement. |
| Popety | Biens immobiliers | Éliminer les fausses annonces sur les marchés de vente et de location de biens immobiliers en inscrivant les biens immobiliers sur la blockchain d'Ethereum. |
| TenX | Cryptoactifs | Permettre à quiconque du « monde réel » de dépenser des cryptoactifs grâce à des moyens de paiement traditionnels, comme une carte bancaire |

Tableau 4 : Visions des fondateurs de DApps rencontrés à Singapour en février 2018

Deux types de problématisations peuvent être distinguées parmi ces désignations systématiques d'acteurs « intermédiaires ». D'une part, des entrepreneurs problématisaient des institutions du monde contemporain : le marché immobilier de Singapour (agents immobiliers et plateformes de vente et de location), le système financier à l'échelle mondiale (en termes d'accès ou d'« inclusion » bancaire), ou les réseaux sociaux professionnels comme LinkedIn. D'autre part, des entrepreneurs problématisaient le

94 A l'époque, à Singapour, les acteurs désignaient généralement les cryptoactifs par « actifs numériques ». Par homogénéité et simplicité, je continue à employer « cryptoactif » dans le reste de ce document.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

développement des DApps et des cryptoactifs lui-même : il manquait un actif qui soit « réel » et « stable » en réponse à la volatilité des cryptoactifs, les services d'hébergement en nuage (*cloud*), d'un mécanisme d'échange de cryptoactifs sans l'intervention d'un *exchange* (qui contrevient au principe de décentralisation en détenant les cryptoactifs des deux parties d'un échange, à la manière d'un intermédiaire financier traditionnel), ou de systèmes permettant de faire des cryptoactifs des moyens de paiement.

Les paragraphes qui suivent se concentrent sur deux projets, Bluzelle et Digix, appartenant au deuxième ensemble de problématisations. Ces deux cas sont choisis, d'une part, parce qu'en problématisant le développement des cryptoactifs eux-mêmes ils informent à son sujet de manière réflexive, mais aussi d'autre part, car ils permettent de mettre en évidence différentes associations imaginées dans l'ingénierie des jetons et des *smart contracts*. Dans les paragraphes qui précède je parlais d' « imagination » car aucun des services imaginés par ces entrepreneurs était fonctionnel au moment de l'enquête.

Je m'appuie sur des entretiens avec des entrepreneurs de ces DApps ainsi que sur un document, produit par chaque startup, appelé *whitapeper*. Ce document, accessible en ligne (à l'époque), décrit le projet de construction d'une DApp en une dizaine à une cinquantaine de page, selon les cas. Ils ont une visée performative, descriptive et promotionnelle, de l'offre de service de la startup. Ils comportent, de manière variable selon les cas : des éléments décrivant l'implémentation technique, le problème que la startup entend résoudre, la composition et le parcours des (principaux) membres de l'équipe et de ses conseils externes, la vision des fondateurs, la stratégie marketing, des dispositions légales ainsi que des éléments sur sa (future) capitalisation financière.

Les smart contracts, plateformes dépouillées

Mon objectif dans les paragraphes qui suivent est de montrer qu'une même architecture logicielle traduit des objectifs politiques similaires. Le *smart contract*, codé comme un jeton, est un outil de comptabilisation de biens mis à disposition (capacité de calcul pour Bluzelle avec le jeton BNT, or physique avec la *Gold Asset Card* de Digix) et d'attribution

Chapitre 2. Les modes des jetons : instituer par les smart contracts

de ces mêmes biens. Dans les deux cas, la DApp est une plateforme qui met en relation des offreurs et des demandeurs de ces biens de manière décentralisée : les sociétés qui les développent n'ont pas de capacité d'intervention sur les relations formées entre les deux parties, inscrites sur Ethereum. Ces présentations montrent les plateformes de manière « dépouillée » : elles se concentrent sur le cœur de la DApp pour faire apparaître le mécanisme de comptabilisation sur Ethereum.

Selon son *whitepaper*, Bluzelle « remplirait un vide dans l'écosystème Internet décentralisé » (Bains 2018). En entretien, Peter, un des cofondateurs, détaillait :

*Blockchain builds a decentralized Internet. Ethereum can be the operating system of this Internet, just like Windows or Android. Filecoin replaces Amazon Services. And there was no service in the decentralized world to replace Oracle.*⁹⁵ (entretien avec Peter, février 2018)

Bluzelle serait la base de données d'un Internet imaginé comme un ordinateur dont le système d'opération serait Ethereum. La métaphore varie légèrement de celle rencontrée au Chapitre 1, plus habituelle, qui décrit Ethereum comme un « ordinateur mondial ». Ce décalage thématise la base de données comme un élément qui doit, pour les fondateurs de Bluzelle, être « décentralisée » au même titre que le calcul des états de l'ordinateur global (Ethereum). Les concepteurs de Bluzelle doublent la synecdoque habituelle : Internet est assimilé au Web, qui est lui-même assimilé à Ethereum dans sa nouvelle version dite « Web 3.0 » à l'époque (plus récemment, il est question de « Web3 »). Ce faisant, ils transfèrent les propriétés associées à l'architecture d'Ethereum à celle du service. Ce prolongement est établi en comparaison à d'autres projets qui participent au Web 3.0 (voir Figure 8), comme Filecoin, un dispositif de stockage décentralisé. Comme l'expliquent les entrepreneurs sur le blog de la startup, Bluzelle est une « base de données » (*database*) et non une « base de fichiers », ce qui suppose des différences en termes de performance dans l'accès aux informations (Muraka 2017).

Deux utilisateurs étaient imaginés. D'une part, un Internaute qui souhaite, selon les

⁹⁵ Notes prises à la volée pendant l'entretien. Si elles ne retranscrivent pas toutes les nuances de l'expression, les passages mobilisés sont ceux que j'ai jugés quasi littéraux immédiatement post-entretien. Le même principe vaut pour tous les entretiens conduits à Singapour en février 2018.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

principes de décentralisation des communications et d'utilisation des services Web promu avec Ethereum, disposer d'une base de données distante. Mais d'autre part et surtout, les développeurs de DApps eux-mêmes. Peter m'expliquait que toute DApp avait besoin d'une base de donnée pour fonctionner, mais qu'utiliser une base de donnée classique, c'est-à-dire « centralisée », comporte un risque de sécurité, un « *point of failure* ». Si Ethereum permet de calculer et d'inscrire les relations numériques de manière autonome et décentralisée, les données participant à la constitution de ces relations devraient elles aussi être tenues de manière décentralisée. Pensons par exemple au cas fizzy du Chapitre 1 : la bonne exécution des contrats d'assurance dépendait des données de vol de FlightStats. En d'autres termes, la blockchain n'était pas une technologie de base de données adaptée pour stocker des données volumineuses et accessibles dans des temps courts.

Cette base de données décentralisée serait assemblée comme une plateforme de mise en relation des clients avec une myriade de « fournisseurs » de stockage, les premiers rémunérant les seconds. Peter m'expliquait que Bluzelle fonctionnait comme une « place de marché » (*marketplace*), c'est-à-dire à première vue comme ce qui est communément un marché « biface » (Rochet et Tirolle 2003). Les relations entre l'offre et la demande de stockage sont formalisées par un jeton désigné par le trigramme BNT, géré par le *smart contract* de Bluzelle. Le *whitepaper* indique que le BNT abstrait les relations entre demandeurs et offreurs en capacité de stockage. Les clients se procurent des jetons BNT directement *via* l'application Web de Bluzelle. Une fois en possession de BNT, ils paient *via* l'application pour utiliser de la capacité de stockage. L'application verse les BNT aux fournisseurs de capacité de stockage. Lorsque ce dernier arrête de mettre de la capacité de stockage à disposition, il échange ses jetons BNT *via* la DApp. Ainsi, la DApp tient la comptabilité de l'offre de stockage disponible (jetons émis aux fournisseurs).

Chapitre 2. Les modes des jetons : instituer par les smart contracts

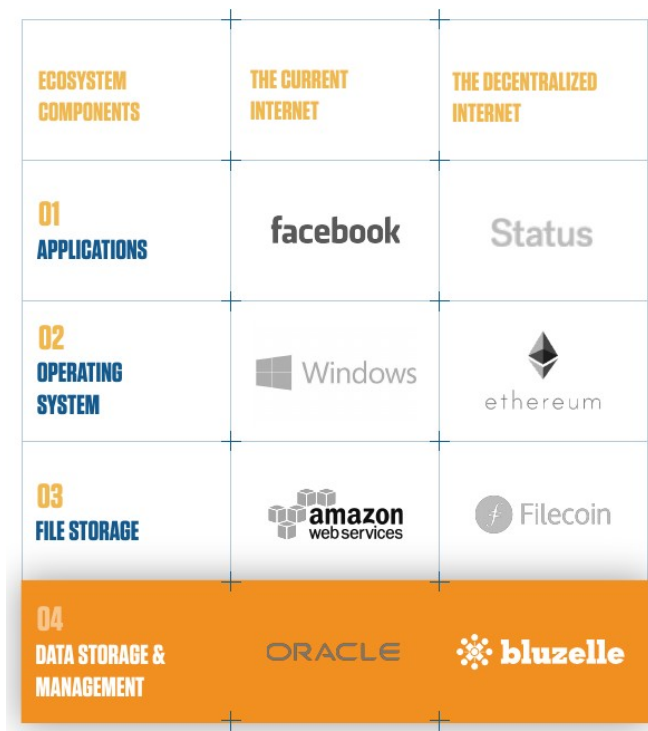


Figure 8 : Articulation de la promesse de service à l' « Internet décentralisé » (Bains 2018)

Avant de continuer à suivre les chaînes mettant en relation des clients et des fournisseurs, et répondre à la question de l'argent utilisé pour obtenir ou échanger les BNT, je présente le cas Digix pour mettre en évidence la ressemblance entre architecture logicielle et fonction du service.

Steve, cofondateur de Digix, présentait lui aussi la DApp comme participation au « Web 3.0 » : elle permettait à ses utilisateurs de détenir un « *smart gold* » sous forme de jetons appelés DGX, qui présente différentes qualités des cryptomonnaies, notamment la possibilité d'échange de pair-à-pair d'unités divisibles à l'envi, tout en évitant l'inconfortable volatilité de leurs cours (sur les *exchanges*). Steve m'expliquait que Digix s'adressait aussi bien aux individus qu'aux développeurs de DApps qui souhaitent avoir une « réserve de valeur » en cryptoactifs, en particulier lorsque les marchés sont en repli. Le choix de l'or comme collatéral tenait aux propriétés physique et réglementaires du métal, notamment vis-à-vis d'autres matières précieuses comme les diamants :

Chapitre 2. Les modes des jetons : instituer par les smart contracts

We need something real and stable. Diamonds are too controlled, with regulatory issues. Stone? You can have different stones at different prices. It is not very easy to fix. Gold is fungible, divisible. And we need the production to be standardized. (entretien avec Steve, février 2018)

Le *whitepaper* renseigne en détails sur cette « production standardisée » de « *smart gold* » dans le *smart contract* associé à la DApp. Elle implique différents acteurs extérieurs à l'application : un fournisseur d'or, un auditeur, et un entrepôt de stockage de l'or. Le *whitepaper* donne des garanties de confiance sur ces acteurs : le fournisseur (ValueMax Singapore) est une entreprise listée sur les marchés financiers, fournisseur de la London Bullion Market Association⁹⁶ ; l'auditeur « indépendant » (Bureau Veritas Inspectorate), qui vérifie la qualité et la quantité d'or fournie, est présenté comme une multinationale proposant une vaste étendue de service aux méthodes avancées d'audit (notamment, non destructrices) ; l'entrepôt de stockage « *state of the art* » (Malca-Amit) est décrit par sa situation géographique (près de l'aéroport de Singapour), par sa surface (25 000 m²), et comme un lieu hautement sécurisé et climatisé par des technologies de dernière génération et une construction écologique. Pour assurer une stabilité du prix d'achat de l'or et la transparence du processus de production, Steve m'expliquait que l'activité de Digix était limitée à Singapour.

A la différence du *whitepaper* de Bluzelle, rédigé dans des termes et une forme qui vulgarise la proposition pour un public large, celui de Digix détaille le fonctionnement de la DApp de manière plus sobre, technique et détaillée. La Figure 9, extraite du *whitepaper*, schématise le fonctionnement de la DApp. Chaque boîte verte correspond à un algorithme, détaillés là aussi sous formes de schémas, qui constitue la DApp. Au coeur de la DApp et au centre de l'image figure un jeton appelé « *Gold Asset Card* ». Ce jeton représente, sur Ethereum, chaque lingot d'or. Le *smart contract* prévoit différentes étapes de vérification d'acquisition, de stockage et de certification d'or avant qu'une *Gold Asset Card* soit créée. La certification est obtenue en fonction des actions des trois prestataires précédemment présentés. Elle est inscrite, avec différentes caractéristiques dans la « carte » du lingot :

96 « *The London bullion market* est un marché de gros de gré à gré pour le commerce de l'or et de l'argent. Les transactions se font entre les membres de la London Bullion Market Association (LBMA), sous la supervision de la Banque d'Angleterre. La plupart des membres sont de grandes banques internationales ou des négociants en lingots et des raffineurs. » (Wikipedia 2023, ma traduction)

Chapitre 2. Les modes des jetons : instituer par les smart contracts

heure d'enregistrement, numéro d'identification du lingot d'or, numéro de série, signatures des parties prenantes de la chaîne logistique (fournisseur, entrepôt, auditeur), facture d'achat, documentation de l'audit, facture de dépôt, coûts de stockages dus. En plus de ce processus d'enregistrement de l'or physique, trois autres processus sont codés dans le smart contrat : l'émission (*minting*) qui consiste à transformer l'enregistrement de l'or en un jeton propriété des utilisateurs de DGX, un processus de refonte de ces derniers (*recast*), et un dernier de rachat (*redemption*).

La Gold Asset Card et le jeton BNT de Bluzelle comptabilisent la mise à disposition d'un bien (or physique, capacité de stockage) par des fournisseurs à des clients. Ces deux objets, créés par des *smart contracts* dont le code fixe les termes sur Ethereum, sont le cœur d'un dispositif imaginé comme une plateforme. Les *smart contracts* sont mobilisés comme dispositifs de mise en relation automatique d'offreurs et de demandeurs de services, selon le principe de décentralisation qui anime les promoteurs d'Ethereum : les règles d'échanges étant codées en dur, la startup est privée d'action sur la mise en relation. La même propriété a été soulignée au Chapitre 1 avec le cas fizzy : le service était conçu pour qu'AXA, développant le service, n'intervienne pas sur les termes du contrat après sa signature. Bluzelle et Digix imaginent des plateformes de mise en relation qui soient elles-mêmes privées de capacité d'intervention sur des relations bilatérales.

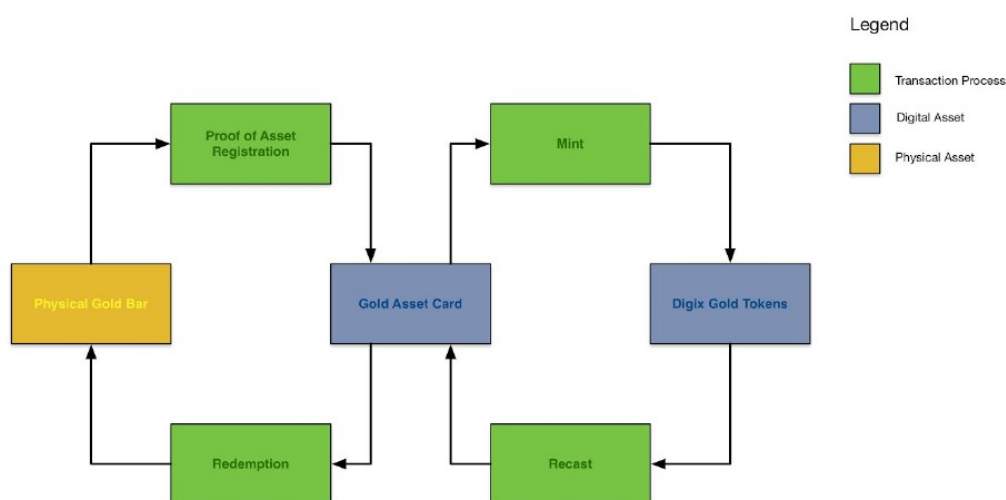


Figure 9 : « Cycle de vie du produit » (Eufemio et al. 2016)

La plateforme garnie : les jetons utilitaires

De la comptabilisation d'un bien (mise à disposition et attribution) à sa marchandisation, il n'y a qu'un jeton. À la similarité des objectifs politiques peut être ajoutée une similarité dans l'organisation de la rencontre entre clients et fournisseurs du bien. Dans les deux cas, cette rencontre est organisée par un jeton, différent de ceux rencontrés aux paragraphes précédents.

Mes deux interlocuteurs décrivaient leurs DApps comme des « places de marchés » (*marketplaces*), expression à comprendre au sens de « marché biface » entre des offreurs de biens et des demandeurs de ces biens. Dans la vue dépouillée de la plateforme, le jeton est un traducteur : il matérialise, dans la DApp, la mise à disposition d'un bien et son éventuelle utilisation par un client. Mais rien n'indique comment cette utilisation se manifeste, et en échange de quoi la DApp la prend en compte.

Dans le cas de Digix, nous avons vu que la création d'une Gold Asset Card était doublée de « l'émission » (*minting*) d'un jeton DGX. La startup prévoyait de mettre ce jeton en vente et de collecter un « *premium* », rémunération de Digix ainsi que des prestataires impliqués dans la mise à disposition de l'or dans les coffres-forts. Steve m'expliquait :

The price of the [DGX] token represents the spot price of the gold market value with an additional premium. For example 50 US dollars in the real world, 52 in the marketplace. It depends on the vault and some parameters. (entretien avec Steve, février 2018)

Ainsi, le jeton DGX était valorisé par un mécanisme de marché qui lui donnait son prix, au contraire de la Gold Asset Card qui tenait les comptes de l'or disponible. Dans le même temps, le jeton DGX était dit « utilitaire » (*utility token*), car il était littéralement « utile » : il donnait un droit d'accès à un service. Les jetons utilitaires peuvent se comprendre comme des bons d'utilisation. Un DGX donne droit à la détention d'un gramme d'or physique. Mais dans le même temps, le jeton DGX avait un prix fixé à l'émission, et étaient ensuite échangés sur un marché secondaire au travers des différents *exchanges* qui proposaient des cotations en continu des jetons DGX (parmi de nombreux autres jetons et *coins*).

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Avec Bluzelle également, un jeton utilitaire permettait d'utiliser le service : les clients dépensaient leurs jetons BLZ sur l'interface Web de Bluzelle, mais les acquéraient sur des *exchanges* externes à la DApp. Comme le DGX, le BLZ était conçu pour être échangeable et valorisable sur les *exchanges*, alors que les jetons « internes » aux plateformes, BNT ou *Gold Asset Card*, avaient une vocation purement comptable. Intrigué par l'existence de ces deux jetons, j'interrogeais Peter qui m'a expliqué que les deux jetons BNT et BLZ répondaient à deux temporalités. Le BLZ suivait une temporalité bien plus rapide de celle du BNT : les transactions en BLZ (les ordres d'achat et de vente) devaient pouvoir être passés indépendamment, et dans des temps bien plus courts que les transactions en BNT (spécifiques à l'usage ou la mise à disposition de la capacité de stockage).

Ainsi, chaque DApp articulait deux jetons qui représentaient respectivement des relations « internes » de type « plateforme » de mise en relation, et des relations « externes » de valorisation marchande et d'échange (de pair-à-pair ou *via* un *exchange*) imaginées comme indépendantes du niveau de production du service. Dans le cas de Digix, cette articulation passait par les processus dit d'émission (*minting*) et de refonte (*recast*). Dans le cas de Bluzelle, le *whitepaper* indiquait que le BLZ était un « un jeton externe-échangeable qui fait un pont entre le jeton natif de Bluzelle (BNT) avec le propre jeton ETH natif d'Ethereum », alors que le BNT était décrit comme un « jeton interne limité à Bluzelle qui permet la crypto-économie de Bluzelle, où les consommateurs paient et les producteurs gagnent » (Bains 2018 : 19, mes traductions). Le BNT était limité à l'« intérieur » de la DApp, assurant les mécanismes comptables de rémunération des fournisseurs et de paiement par les clients. La Figure 10 issue du *whitepaper* fait apparaître cette différence de périmètre. La DApp tenait une comptabilité automatique entre les BNT et les BLZ, à un taux de un pour un. En recevant un montant de BNT, la DApp considérait que l'« offre » de stockage du fournisseur prenait fin. Dans le même temps, un montant équivalent de BLZ était émis vers le *wallet* « extérieur » de ce (désormais ancien) fournisseur. Ces jetons BLZ nouvellement acquis par cet ancien fournisseur pouvait alors servir soit à constituer une « demande » de stockage, soit à être vendus sur une plateforme d'échange.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

When a producer wishes to "withdraw" their BNT tokens, they use the following steps:

1. Send the BNT tokens to the special Bluzelle gateway.
2. The gateway converts the BNT tokens at a 1:1 ratio to BLZ tokens, and sends these BLZ tokens to the producer's registered Ethereum wallet.
3. The producer now has the BLZ tokens, and is free to transact with them on the Ethereum network.

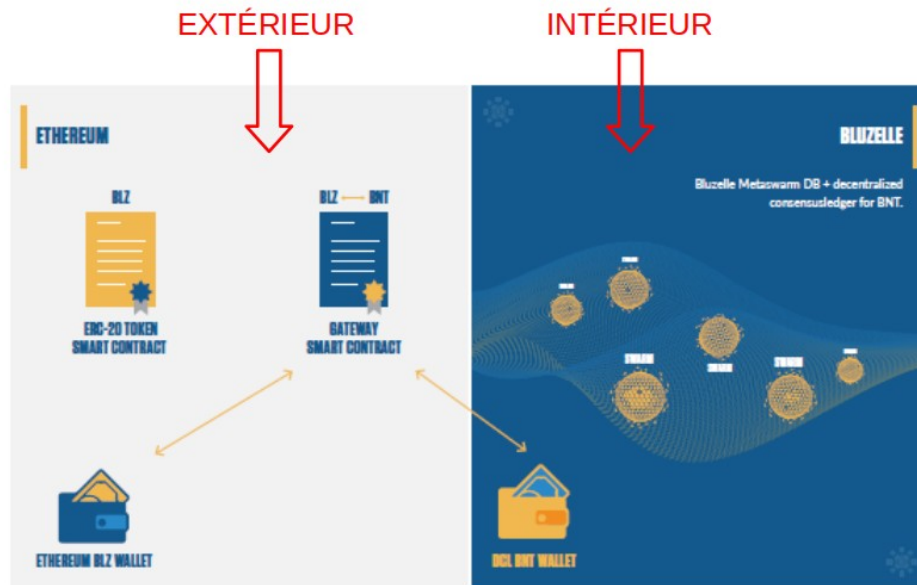


Figure 10 : Extrait de Bains (2018 : 20) – mes ajouts en rouge

Ces éléments montrent que les jetons utilitaires lient différentes entités : la DApp elle-même, les clients de la DApp, les fournisseurs de la DApp, les *exchanges*. Le modèle de la plateforme est utile pour décrire l'imaginaire qui guide le travail des concepteurs : une mise en relation automatisée, « autonome » et « décentralisée ». Il montre que les biens (or, stockage) sont qualifiés au travers de jetons « internes » qui en fixent les propriétés. Mais ce modèle ne tient pas dès lors qu'est posée la question de la mise en relation effective entre offre et demande sur ce marché biface : les jetons internes ne suffisent pas pour décrire l'établissement des transactions bilatérales entre clients et fournisseurs qui supposent que les bons d'utilisation aient un prix.

Ces différentes entités forment ce que Michel Callon appelle un « agencement marchand » (Callon 2013) : une action collective structurée par différents dispositifs socio-techniques destinés à établir des transactions commerciales bilatérales fructueuses et à promouvoir leur

prolifération. Le chaînage des jetons matérialise la transaction bilatérale entre des fournisseurs (qui reçoivent des jetons) et des clients (qui paient en jetons). Dans ce chaînage, chaque type de jeton a un rôle spécifique : les uns qualifient les biens échangés, les autres calculent le prix de marché des biens. À la différence de la notion de marché biface (ou plus généralement, multi-faces), l'agencement marchand oriente l'analyse des marchés sur leur processus d'établissement, sans cesse renouvelé et jamais acquis : « marché » se confond avec « *marketization* ». La section suivante part de ce cadrage pour analyser le rôle que les entrepreneurs donnent à la firme dans ces agencements.

1.2. Les jetons, ingénierie de relations entrepreneuriales

A firm's commercial activity must be analysed as an aggregation of a varying number of bilateral transactions, each of which link the firm to each of its customers. (Callon 2015 : 11-12)

Selon le modèle de la DApp comme plateforme vu à la sous-section précédente, la firme disparaît au profit des chaînes de jetons qui lient les fournisseurs aux clients. L'activité de la firme est de développer et de maintenir les jetons, tout en collectant des frais prélevés sur l'utilisation du service (en jetons, qu'elle est ensuite libre d'échanger sur les *exchanges*). La DApp formule à la place de la firme ce que Michel Callon appelle des « transactions bilatérales », directement entre les fournisseurs et les clients selon le principe de relations de pair-à-pair « sans intermédiaires ». Dans cet agencement, les *exchanges* agissent comme institution monétaire : ils permettent d'envisager les jetons comme de l'argent, en garantissant à tous leur convertibilité dans une unité comme le bitcoin ou l'ether, et par ricochets, en euros ou en dollars étatsuniens.

Cette sous-section montre que les jetons forment non seulement des relations commerciales (ou de production et d'utilisation du service) mais aussi entrepreneuriales. La place de la « firme » est variable en fonction des cas. Les matériaux collectés au début de 2018 (alors que les services présentés à la section précédente étaient des projets) et mobilisés dans cette sous-section permettent d'analyser comment les firmes envisageaient leur rôle et ceux des autres acteurs en présence, à partir de la manière dont ils imaginaient

Chapitre 2. Les modes des jetons : instituer par les smart contracts

les relations formées par les jetons. Les paragraphes qui suivent présentent successivement deux scénarii en fonction du sens que les firmes donnaient aux porteurs de jetons qu'elles créaient pour se financer. À la lumière de ces deux cas, je propose de comprendre les jetons comme des dispositifs d'enrôlement et des opérations matérielles de capitalisation.

Cas Digix : le financement par l'émission de jetons de gouvernance

Steve et trois associés imaginaient le service Digix entre fin 2015 et début 2016. Deux organisations ont vu le jour pour faire advenir le service Digix. D'une part, une startup nommée DigixGlobal était cofondée par Steve et ses associés. Au départ, cette société était chargée de l'ensemble du travail de développement entrepreneurial, technologique et promotionnel du service. Mais rapidement et d'autre part, une deuxième organisation entrait en jeu : DigixDAO devait devenir l'organe décisionnaire de Digix. L'acronyme « DAO » signifie « organisation autonome décentralisée (« *Decentralized Autonomous Organisation* »), une forme organisationnelle émergente en 2016 qui connu depuis un certain engouement. Une DAO est un groupement d'entités réduites à leur détention de jetons dits « de gouvernance ». Ces jetons permettent à leurs porteurs de s'exprimer sur des orientations d'un projet collectif ; typiquement, voter ou proposer de nouvelles orientations à l'ensemble des porteurs de jetons. Cette gouvernance est formalisée dans des *smart contracts* : les propositions sont codées, les votes sont des transactions en jetons vers ce *smart contract*, pondérés en fonction du nombre de jetons. Vis-à-vis de DigixDAO, DigixGlobal était imaginé comme un prestataire de service. Ainsi, DigixGlobal pouvait, à terme, être concurrencé par d'autres organisations.

DigixDAO a été créée le 30 mars 2016 par un processus appelé « *Initial Coin Offering* » (ICO). L'ICO est un processus de levée de fonds participatif. Typiquement, une startup organise une « pré-vente » d'un jeton ou d'un coin en échange de fonds (en général, bitcoins et ethers). Au moment de l'ICO, les *coins* ou jetons (en fonction de l'ICO, financement d'un réseau ou d'une DApp) peuvent être des promesses : auquel cas, ils sont créés plus tard, typiquement avec les fonds collectés par la startup. Steve était fier de m'expliquer que Digix était le premier service financé par ICO sur Ethereum.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Historiquement, avant d'être largement mobilisé pour le financement de DApps, l'ICO a permis de financer des projets alternatifs ou complémentaires à Bitcoin. C'est le cas de Mastercoin, présenté au Chapitre 1 dans la filiation entre Bitcoin et Ethereum, dont le créateur aurait inventé l'ICO (Apautes 2018). C'est également le cas d'Ethereum. En 2014, Vitalik Buterin et ses associés mettaient en vente, contre des bitcoins, 60 millions d'ethers qui ne seront créés et attribués qu'en 2015. En six semaines, l'équipe collectait l'équivalent de 18 millions de dollars étatsuniens (Eudes 2014).

Deux nouveaux jetons articulaient financement et gouvernance de Digix, « pré-vendus » par DigixGlobal pour constituer et capitaliser DigixDAO. L'ICO a été conclue en moins de 24 heures, le 30 mars 2016. 466 648 ethers ont été collectés, total alors valorisé à 5,5 millions de dollars étatsuniens sur les *exchanges* (Ward 2018). Au moment de l'entretien avec Steve en février 2018, cette capitalisation était estimée à 400 millions de dollars étatsuniens. Contre leurs ethers, les investisseurs recevraient des jetons DGD en proportion de leurs contributions. Parmi eux, les investisseurs ayant contribué au-delà de l'équivalent de 15 000 dollars étatsuniens se voyaient attribuer un jeton DGB appelé « badge » (*badge* en anglais). 385 investisseurs ont reçu ce badge. Les détenteurs de jetons DGD et DGB étaient investis de différents niveaux de décision. À l'origine⁹⁷, les détenteurs de DGB pouvaient soumettre des propositions (ils étaient dits *Proposers*) à l'approbation des autres détenteurs de jetons DGB ; en cas d'accord d'une majorité de détenteurs de jetons DGB, les propositions étaient soumises au vote de l'ensemble des porteurs de jetons DGD. Les cofondateurs de Digix disposaient en outre d'un privilège supplémentaire : ils pouvaient soumettre des propositions directement à l'ensemble des porteurs de jetons DGD, sans passer par le vote des *Proposers*. Cette hiérarchie est résumée sur la Figure 11, elle-même issue d'un document précisant le mécanisme de gouvernance imaginé quelques semaines après l'ICO (Digix Writer 2016a).

Ainsi, la distribution de ces jetons articulait pouvoir de décision et investissement financier préalable de chacun. Mais avant que l'organisation décentralisée soit tout opérationnelle,

⁹⁷ L'organisation des modalités de gouvernance a elle-même évolué voir par exemple Digix Writer (2018). Les éléments qui suivent sont donnés comme illustration du type de mécanisme imaginés par des jetons de gouvernance.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

les fondateurs à la tête de DigixGlobal jouaient un rôle central d'animation. Dans les mois qui suivirent et avant qu'une interface Web permette à chaque porteur de jetons DGD et DGB d'exercer les pouvoirs de proposition et de vote, l'administration était assurée par DigixGlobal en lien avec les porteurs de jetons. Par exemple, des votes *ad hoc* étaient organisés *via* une application tierce appelée CarbonVote, permettant d'organiser des scrutins dans lesquels les porteurs d'un jeton donné « bloquent » leurs jetons le temps du vote (pour éviter que les jetons soient utilisés pour voter plusieurs fois) en associant à ce blocage le contenu du vote. Nous verrons au Chapitre 4 que ce mécanisme a été utilisé dans un autre cas important dans l'histoire d'Ethereum.

| Badge Type | Can directly submit proposals? | Can submit proposals for vetting? | Can vet on proposals? | Can pledge on proposals? |
|--------------|--------------------------------|-----------------------------------|-----------------------|--------------------------|
| Founder | ✓ | ✓ | ✓ | ✓ |
| Proposer | ✗ | ✓ | ✓ | ✓ |
| Token Holder | ✗ | ✗ | ✗ | ✓ |

Figure 11 : Hiérarchie des pouvoirs de décision dans DigixDAO

La nature et l'origine de l'argent utilisé pour les développements du service et des outils permettant à DigixDAO de fonctionner témoigne de la volonté de dissocier les actions initiées collectivement dans un fonctionnement « normal » et futur (par DigixDAO) des actions de construction transitoires (à l'initiative de DigixGlobal). Les ethers collectés durant l'ICO étaient toujours bloqués lorsque je m'entretenais avec Steve, en février 2018. Steve et ses associés étaient financés par des financements privés. En novembre 2017, DigixGlobal annonçait le financement de deux fonds de capital-risque, à hauteur de 1,25 million de dollars étatsuniens (Digix Writer 2017). Premièrement, Global Brain était annoncé comme « l'une des plus grandes sociétés de capital-risque du Japon ». Le fonds inaugurerait deux mois plus tôt un « *Blokchain Lab* », manière d'annoncer une spécialisation dans l'investissement dans les projets de cryptomonnaies. Deuxièmement, Fenbushi Capital était connu comme l'un des investisseurs de premier plan dans les projets de DApp, société

Chapitre 2. Les modes des jetons : instituer par les smart contracts

à laquelle était associé le cofondateur d'Ethereum, Vitalik Buterin.

Toutefois, les fondateurs de DigixGlobal s'étaient réservé un rôle important dans la gestion future de Digix *via* DigixDAO. Lors de l'ICO, les fondateurs se sont octroyés 15 % du total des jetons DGD émis (300 000 sur 2 millions), soit 15 % du pouvoir de décision « décentralisé », en plus du pouvoir particulier de proposition directe auprès des porteurs de DGD (badge de fondateur). Cette pratique d' « auto-attribution » était courant lors des ICO. Par exemple, les cofondateurs d'Ethereum s'étaient auto-attribués 12 millions d'ethers sur les 60 millions mis en « pré-vente ». Ce rapport entre investissement initial et pouvoir de décision n'était bien entendu pas figé une fois pour toutes. DigixGlobal a par exemple suggéré en 2016 que DigixDAO organise un vote tous les deux ans pour décider si de nouveaux DGD devaient être émis afin de reconstituer les réserves de la DAO. De cette manière, la répartition du pouvoir de décision pouvait être diluée (ou renforcée) en fonction de l'arrivée de nouveaux investisseurs.

Le cas de Digix montre que l'ingénierie des jetons mêle formulation de relations entrepreneuriales, en distribuant le pouvoir de décision sur la construction et la maintenance du service Digix, et d'investissement dans une DApp dont les bénéfices sont produits en jetons DGX et alloués à DigixDAO. Les jetons de « gouvernance » DGD et DGB ressemblent respectivement à des actions et à des droits, le rôle des porteurs des jetons étant proche de celui d'actionnaires dans des sociétés par actions. En filant la comparaison, les ethers collectés lors de l'ICO s'apparente à un « capital social » de la société DigixDAO, réduite à son conseil d'administration qui décide, notamment, de la répartition des bénéfices générés par le service Digix en jetons DGX (prélevé sur les transactions commerciales de la DApp). DigixGlobal ressemble à un bureau exécutif dont les membres ont des droits de direction particuliers en raison de leur statut de cofondateurs qui ne se limitent pas à leurs parts de capital social.

Cas Bluzelle : le financement par l'émission de jetons utilitaires

La firme Bluzelle était au centre d'une toile de relations constituée avec un seul jeton. Dans cette toile, la firme devait jouer un rôle central, en conservant formellement le pouvoir de décision et le financement du développement du service. Bluzelle a obtenu deux sources de financement. D'une part, Bluzelle a été capitalisée par des fonds de capital-risque, parmi lesquels Kenetic Capital (Hong Kong), Kryptoni 1 (Royaume-Uni), Hashed (Corée du Sud), ainsi que Fenbushi Capital (également investisseur dans DigixGlobal). D'autre part, Bluzelle a recouru à l'émission de jetons. Entre le 17 et le 26 janvier 2018, la pré-vente de 165 millions de jetons BLZ a permis aux cofondateurs de Bluzelle de collecter en ethers l'équivalent de 19,5 millions de dollars étatsuniens à l'époque. Cet objectif était celui annoncé par les cofondateurs dans le *whitepaper*, qui détaillait le processus d'émission du jeton BLZ, vendus à certains, donné à d'autres. Le Tableau 5, construite à partir du *whitepaper* et de l'entretien avec Peter, récapitule la distribution du jeton utilitaire comme opération de financement en fonction des différentes catégories d'acteurs (en lignes).

Premièrement, 165 millions de jeton BLZ étaient « pré-vendus » selon un mécanisme d'ICO formellement similaire à celui de Digix. Mais ici, le jeton BLZ, imaginé pour former les relations « externes » à la DApp (valorisation marchande et échange) avait une signification préalable : celle d'instrument de levée de fonds. Autrement dit, le premier destin du jeton BLZ était d'être vendu à des investisseurs avant de pouvoir servir à utiliser un service qui n'existait pas au moment de son émission. Les fonds collectés lors de l'émission des jetons BLZ permirent d'obtenir les financements présentés comme nécessaires au développement du service.

Le *whitepaper* spécifiait ces utilisations futures (Bains 2018 : 30). 50 % étaient destinés à la recherche et au développement du produit, de manière à « développer le produit de manière continue et faire croître l'équipe au niveau mondial » ; 10 % étaient associés à des coûts de réseau, un « capital initial nécessaire à l'alimentation du réseau et ses nœuds, et au lancement du service décentralisé » ; 20 % étaient consacrés aux ventes et au marketing à destination des personnes ordinaires (« *grass-root* ») au départ, puis « à étendre aux

Chapitre 2. Les modes des jetons : instituer par les smart contracts

conférences, partenariats, et publicité » ; 10 % étaient consacrés à la conduite des opérations, leur « supervision générale et l'administration des coûts pour conduire les affaires à l'échelle mondiale » ; enfin, 5 % étaient dédiés aux aspects légaux et comptables, « importants pour que Bluzelle maintienne de hauts niveaux d'exigences pour ses opérations et agisse de manière transparente ».

| <i>Postes de l'émission de jetons BLZ</i> | <i>%</i> | <i>Destinataires des jetons</i> | <i>Jetons offerts en échange de</i> | <i>Effets attendus pour Bluzelle</i> |
|---|----------|---------------------------------|--|---|
| <i>Initial Coin Offering (ICO)</i> | 33 | « Public » | ethers | Enrôlement de futurs consommateurs et producteurs Des ressources en ethers |
| Auto-attribution | 27 | Bluzelle | Promesse de développement d'un service | Enrôlement continu de l'équipe future de Bluzelle Des ressources pour de futurs développements |
| <i>Developers fund</i> | 10 | Bluzelle | Développements futurs du service | Enrôlement des développeurs Développement de la communauté |
| Equipe fondatrice | 15 | Cofondateurs | Travaux précédant l'émission de jetons | Enrôlement des cofondateurs Publicité (sérieux du projet) |
| <i>Early Backers, Equity Investors and Advisors</i> | 15 | <i>Early Backers</i> | Soutiens matériels ou financiers | Rétribution de tiers |
| | | <i>Equity Investors</i> | Part du passif comptable de Bluzelle | Augmentation de la part des fondateurs dans le capital social |
| | | <i>Advisors</i> | Conseils, publicité, mise en réseau | Rétribution de tiers |

Tableau 5 : Émission des jetons BLZ et effets attendus pour la firme

Deuxièmement, le *whitepaper* indiquait que 335 millions de jetons BLZ étaient distribués à différents groupes d'acteurs qui participaient ou avaient participé au développement du service. 27 % de l'ensemble de jetons émis étaient « conservés par Bluzelle » de manière à être « utilisés pour des offres additionnelles de futurs développements et pour des 'staff incentives' ». 10 % capitalisent un « fonds pour développeurs » (*developers fund*), utilisés comme des « incitations, récompenses et des moyens d'attirer des développeurs pour construire des projets, des intégrations, des partenariats, des hackatons et pour l'implication de la communauté [de manière à] faire grandir l'écosystème ». 15 % étaient

Chapitre 2. Les modes des jetons : instituer par les smart contracts

directement destinés à l'équipe fondatrice, car « les fondateurs de Bluzelle ont travaillé sur cette affaire pendant trois ans », tout en précisant que « leurs jetons BLZ ser[aient] bloqués [vested] pendant trois ans ». Enfin, 15 % étaient attribués aux « *Early Backers, Equity Investors and Advisors* » pour leur « aide dans le développement de la technologie » et dont « une partie des investissements » en fonds propres (*equity*) a été « convertie en jetons ».

Dans les deux cas, vente comme don, les jetons BLZ forment des relations entre les cofondateurs et les tiers qui concourent au développement de Bluzelle. Premièrement dans le cas de la vente, les jetons BLZ signifient financement pour Bluzelle, investissement pour les utilisateurs. Le jeton ne signifie ni rémunération future ni droit de vote : il articule une possibilité d'utilisation du service future (le jeton est dit « utilitaire ») à une dimension spéculative (le jeton étant coté dès son émission sur des *exchanges*). Deuxièmement dans le cas du don, les jetons BLZ signifient soit rétribution de tiers et libération d'obligations (la firme vis-à-vis de l'équipe fondatrice⁹⁸, des *Early Backers* et des *Advisors* pour leurs actions passées, de développeurs pour de futurs travaux), sinon capitalisation de la firme et renforcement de la capacité d'action des cofondateurs (auto-attribution pour de futurs travaux, changement de la forme du capital social par le rachat en jetons de parts correspondant aux financements en capital-risque).

Les jetons : dispositifs d' enrôlement et opérations de capitalisation

Les cas de Bluzelle et Digix montrent que les firmes imaginent des relations multiples avec les acteurs en présence dans le développement des DApp. Avec Bluzelle, la firme conçoit son propre rôle de manière centrale dans le développement du service. L'émission des jetons lui permet d'organiser ses relations et de se donner des moyens pour développer le service : capitalisation de la société en ethers, rétribution de tiers, renforcement du contrôle des cofondateurs sur le capital social. Avec Digix, la firme (DigixGlobal) est imaginée comme prestataire privilégié d'une assemblée « décentralisée » de décideurs (DigixDAO). L'émission de jetons permet de constituer cette assemblée d'investisseurs tout en lui

98 Cette rémunération ressemble à une *stock-option*, mais ici, la rémunération versée n'est pas une option d'achat de l'action de la firme (qui n'est pas cotée), mais le jeton lui-même.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

donnant un objet de décision : l'allocation des ethers que ces derniers ont payé en échange des jetons de gouvernance.

| <i>Usages imaginés des jetons</i> | <i>Bluzelle</i> | <i>Digix</i> |
|---|-----------------|-----------------|
| Interne à la DApp | BNT | Gold Asset Card |
| Jeton « utilitaire » : usage du service | <u>BLZ</u> | <u>DGX</u> |
| Gouvernance de la DApp | (cofondateurs) | <u>DGD, DGB</u> |
| <i>Légende :</i> | | |
| <ul style="list-style-type: none"> • <u>Souligné</u> : ont des valorisations de marché (exchanges) • Gras : opérations de capitalisation | | |

Tableau 6 : Récapitulatif des usages imaginés des jetons, cas Bluzelle et Digix

Ainsi, les jetons forment des manières de participer au développement (entrepreneurial, technologique, financier) de la DApp. Ces participations articulent utilisation du service et investissement d'une part, et détention présente et future d'autre part. Dans le cas de Digix, l'investissement (c'est-à-dire la détention de jetons DGD et/ou DGB) a une signification comparable à l'actionnariat : les porteurs de jetons disposent de droits de gouvernance qui orientent les futurs développements du service, ainsi que la distribution des profits générés par l'utilisation de la DApp (via le jeton DGX). Dans le cas de Bluzelle, l'investissement (le jeton BLZ) initialement valorisé par la firme qui a la main sur l'émission, donne droit au présent à une revente au prix de marché (exchanges) et à l'utilisation future d'un service inexistant.

Les émetteurs font des différents jetons des dispositifs d'enrôlement (Callon 1984) : ils nouent des alliances entre des acteurs préalablement intéressés (par les cryptoactifs) à l'extérieur de la firme et (plus spécifiquement par le projet de DApp en question) à l'intérieur de la firme. Avec Digix, le jeton DGD constitue un intérieur de la firme intéressé par le développement entrepreneurial et financier de la DApp dont la performance est mesurée par la création et l'utilisation du jeton DGX. Avec Bluzelle l'enrôlement par don

Chapitre 2. Les modes des jetons : instituer par les smart contracts

de jetons à l'intérieur de la firme participe directement à l'enrôlement des investisseurs et utilisateurs à l'extérieur. En effet, le *whitepaper* valorise ces dons comme des gages de sérieux du projet des cofondateurs : les jetons attribués à l'équipe de cofondateurs sont bloqués pendant trois ans, pour les motiver à s'impliquer au maximum dans le développement du service ; les fonds alloués au « fonds pour développeurs » visent à « inciter » des développeurs à participer à des projets ou partenariats pour faire « grandir l'écosystème » ; les *Advisors* sont des personnalités qui ont travaillé pour les grands noms de la Silicon Valley ou de la naissante galaxie de sociétés crypto⁹⁹. Ces gages de sérieux sont directement destinés aux porteurs de jetons BLZ, investisseurs et éventuellement futurs utilisateurs ; le *whitepaper* précise que ces jetons sont « mis en vente aux consommateurs et producteurs de manière à ce qu'ils prennent part à l'écosystème ».

L'agentivité des jetons dans le processus d'émission s'observe aussi, par contraste, avec les deux cas de mon échantillon de huit startups rencontrés à Singapour qui n'ont pas eu recours à l'émission de jetons pour financer leur projet de DApps. Premièrement, Averspace s'est financé par des partenariats avec des institutions préalablement enrôlées pour l'utilisation du service imaginé. Comme me l'expliquait son fondateur, la startup de mise en relation de pair-à-pair de vendeurs et d'acheteurs de biens immobiliers (sans agents immobiliers) prévoyait de diriger le trafic d'un de ses partenaires, City Development Limited, l'un des plus grands conglomérats immobiliers de Singapour, vers sa plateforme. Deuxièmement, Popety était déjà une entreprise profitable en 2018 et travaillait à l'analyse prédictive des biens immobiliers sur les six à douze mois à venir. Face au manque de fiabilité des listings de biens immobiliers en vente, son *Chief Operating Officer* voyait dans la blockchain Ethereum une opportunité de nouveau service : un *listing* fiable (au sens d'incorrupible avec Ethereum) des biens immobiliers en vente. Dans ces deux cas, aucun

99 Le *whitepaper* indique : « *Bluzelle has put together a specialized unit of advisors to guide the growth of the business. Each person is a technology heavyweight contributing to companies like Facebook, PayPal, LinkedIn, Ethereum and more* ». Parmi eux figurent un développeur du protocole d'Ethereum (*core developer*) ou un grand investisseur (*super-angel*) dans Ripple (cryptomonnaie qui a connu une forte capitalisation et soutenue par des banques). Un informateur rencontré plus tard en meetup me confirmait une intuition issue de la lecture de différents *whitepapers* : ce que Bluzelle appelle « *Advisors* » sont généralement des personnes reconnues dans le milieu des cryptoactifs (souvent Vitalik Buterin) ou de l'investissement qui prêtent leurs noms et leur image à des startups construisant DApps pour participer à la crédibilisation de leur projet.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

besoin d'enrôlement d'acteur « extérieur » à la firme n'était pensé comme un élément clé de la réussite du service, que ce soit en termes d'usages futurs ou de financement présent.

L'émission des jetons (BLZ, DGD, DGB) montre que les *smart contracts* permettent de réaliser des opérations de capitalisation (Muniesa et al. 2017) : ces jetons sont vus par des investisseurs comme des objets susceptibles de générer des revenus futurs. La diversité de leurs significations témoigne de la pluralité de la notion « investisseur » (Ortiz 2014) dont le sens est ici le résultat d'un travail entrepreneurial et d'ingénierie : un décideur doté de différents niveaux de décision (avec ou sans « badge », DGB) en fonction du montant d'ethers investi (Digix), ou un futur utilisateur misant sur l'appréciation de son bon d'utilisation par une valorisation de marché (Bluzelle). Ainsi, les *smart contracts* apparaissent comme un langage pour formuler la transformation de choses en actifs, ce qui peut être vu comme un langage du phénomène décrit comme « *assetization* » (Birch et Muniesa 2020) : ici ces choses sont la participation à une « organisation décentralisée » et le bon d'utilisation d'un service qui n'existe pas encore.

Ainsi, la programmabilité des *smart contracts* confère à l'ICO une grande diversité de significations qui la distingue de l'*Initial Public Offering* (IPO) ou introduction en bourse dont elle est inspirée. L'IPO consiste à échanger des parts de société sous la forme d'actions ouvrant droit à des dividendes annuels ou des droits de vote en assemblée générale, contre des capitaux. D'un point de vue de gouvernance d'entreprise et nonobstant les questions pratiques d'organisation des DAO qui seront abordées au Chapitre 4, l'ICO de Digix via DigixDAO ressemble à une IPO. Au contraire dans le cas de Bluzelle, les jetons partagent avec les actions le caractère échangeable sur des marchés côtés. Mais à la différence des actions, les jetons « utilitaires » ne représentent aucune participation formelle à la gouvernance de la firme.

1.3. Gestation d'un agencement marchand : quelques plans de coupe

Plutôt qu'une multitude de marchés, les jetons côtés sur les *exchanges* participent d'un

Chapitre 2. Les modes des jetons : instituer par les smart contracts

agencement marchand étendu. Les entités qui concourent à la construction des DApp sont multiples mais interdépendantes. D'une part, la valorisation marchande des uns est articulée aux autres *via* des objets communs comme le bitcoin et l'ether ; d'autre part, les différents acteurs participant à construire les DApp, qu'ils soient investisseurs, utilisateurs ou entrepreneurs, voient dans les DApp et les processus d'émission des jetons des pratiques communes.

Cette sous-section s'arrête sur un objet et un phénomène qui ont été centraux dans la gestation de ce que je propose de comprendre comme un agencement marchand étendu. Par gestation, je désigne le processus de rencontres entre des entrepreneurs et des investisseurs qui se déployait alors que les DApps étaient des services imaginés. Premièrement, les *whitepapers* sont analysés comme dispositifs de valorisation des projets de DApp et de capitalisation, au sens d'objets dans la rencontre, essentiellement en ligne, entre des investisseurs et des entrepreneurs. Deuxièmement, je contextualise le mécanisme d'ICO comme phénomène central dans la fièvre mondiale pour les cryptoactifs en 2018. Je pointe le rôle d'acteurs influents pour montrer un autre aspect d'un phénomène trop souvent résumé à des arnaques en série ou relevant de la naïveté d'investisseurs individuels. Je présente également l'activité d'un intermédiaire financier qui témoigne de la structuration des pratiques de ce secteur et du rôle qu'ont pris des *exchanges* dans ce phénomène, révélant la fragilité de ce modèle entrepreneurial.

Le whitepaper : dispositif de valorisation et de capitalisation

Les participants en devenir, enrôlés comme futurs utilisateurs ou investisseurs par les entrepreneurs, étaient prioritairement des utilisateurs de cryptoactifs. À Singapour comme à Paris, les rencontres physiques avaient typiquement lieu lors de « meetups », du nom de la plateforme Web permettant d'annoncer des réunions physiques sur des thèmes particuliers. Ces événements rassemblaient régulièrement et dans un même espace des entrepreneurs et des utilisateurs, investisseurs, ou plus largement des curieux de cette industrie naissante. Ils étaient des lieux de réseautage, des espaces de publicisation des projets auprès de ces publics ainsi que de partage des nouveautés commerciales et technologiques, en particulier

Chapitre 2. Les modes des jetons : instituer par les smart contracts

concernant Ethereum, dans ce qui était communément appelé un « écosystème ». Je reviendrai sur les meetups à la section 2 de ce chapitre.

Dans le même temps, les rencontres se passaient en ligne. La publicisation des projets prenait la forme de posts de blogs sur des sites généralistes comme Medium, ou de manière plus informelle sur Reddit ou Quora, sur des forums spécialisés comme BitcoinTalk, ainsi que *via* des sites de presse spécialisée dans les cryptoactifs. Ces derniers participaient activement à la promotion et à la crédibilisation des cryptoactifs. Ils étaient souvent détenus par des investisseurs, des fonds de capital-risque et des gestionnaires de (crypto)actifs. Parmi les plus consultés selon mon expérience de navigation sur le Web et dans les groupes Telegram d'utilisateurs et d'investisseurs de cryptoactifs figuraient CoinDesk et le Coin Telegraph en anglais, ou le Journal du Coin en français. Le site CoinDesk était détenu par le groupe Digital Currency Group depuis 2015. Ce groupe, dirigé par l'investisseur et activiste pro-Bitcoin Barry Silbert, détenait l'équivalent de 50 milliards de dollars étatsuniens en gestion. Le site Coin Telegraph indiquait que son *Chief Executive Officer* était George Givishvili, lequel est *Chief Marketing Officer* chez BitFury Group, une société d'investissement dans le secteur des cryptoactifs, notamment dans l'industrie du « minage ». Le site du Journal du Coin indique explicitement participer à la promotion des cryptoactifs, notamment pour favoriser les intérêts du secteur face aux réglementations émergentes. Malgré une formulation alambiquée mais comme l'a montré le journal Warning Trading, le Journal du Coin appartenait à une société d'investissement dans les cryptoactifs de droit estonien, appelée Coincorp, et dirigée par un mystérieux résident russe qui avançait sous pseudonyme (Miller 2022).

Dans ces différentes arènes, le *whitepaper* était un objet central de promotion des projets de DApps. Il était repris par bouts, mis en circulation dans les présentations des entrepreneurs en meetups et les posts de blogs sur les plateformes comme Medium et Reddit, mais aussi souvent *in extenso* dans les articles de la presse spécialisée. Le *whitepaper* était un « dispositif de valorisation », au sens d'assemblage matériel et discursif qui intervient dans le processus de valorisation (Doganova 2011) des projets de DApps. Cette généralisation du *whitepaper* s'est affirmée comme un standard de valorisation des coins et des jetons, au

Chapitre 2. Les modes des jetons : instituer par les smart contracts

point que des chercheurs le voit comme un élément empirique pour fonder une taxonomie des blockchains et de leurs acteurs selon leurs propres termes (Caliskan 2020). Le *whitepaper* m'a servi de ressource pour la constitution des matériaux d'enquête, notamment la préparation des entretiens avec les entrepreneurs, ainsi que pour l'analyse. Dans la première sous-section (1.1), le *whitepaper* est ma principale ressource pour analyser les services imaginés par les entrepreneurs comme des plateformes articulées au projet collectif de construction d'un Web 3.0.

Le *whitepaper* était également un objet clé d'un « dispositif de capitalisation » selon la définition qu'ont donné Liliana Doganova et Fabian Muniesa pour les modèles d'affaires (2015) : il participe à valoriser le projet de DApp comme un objet d'investissement en participant à former la rencontre entre des entrepreneurs et des investisseurs dont ils stimulent l'imagination, et par là, ont des capacités performatives. Cette dimension est évidente à la lecture du *whitepaper* de Bluzelle qui consacre une partie détaillée à l'émission des jetons, en indiquant les classes de récipiendaires et les quantités de jetons associées à chacune (sous-section 1.2). En revanche, elle est moins évidente dans le cas de Digix. Les jetons DGD et DGB, matérialisant les opérations de capitalisation, n'y sont pas évoqués ; ce *whitepaper* est un document austère, qui décrit le service de manière technique et algorithmique (fonctions, arbres de décisions, schémas d'architecture logicielle). Ce choix doit être situé : Digix était, selon ses cofondateurs qui étaient très fiers de l'annoncer en entretien comme sur Medium, le premier projet à se financer par émission de jetons sur Ethereum. Au contraire, l'émission de jetons de Bluzelle, deux ans plus tard, est contemporain de ce que certains ont qualifié de « mania des ICO ». Mais dans le même temps, les extraits du *whitepaper* de Digix étaient mobilisés dans différents supports de communication, notamment sur Medium.

ICO mania : valorisation des jetons et commerce de l'influence

Arnaud faisait de l'organisation de la rencontre entre entrepreneurs et investisseurs son activité professionnelle. J'ai rencontré Arnaud lors du traditionnel pot de fin du meetup #16 (septembre 2019). Pour lui, les meetups faisaient partie des lieux où on se montre et où on

Chapitre 2. Les modes des jetons : instituer par les smart contracts

créé des relations. Arnaud avait cofondé sa société avec quelques amis au début de 2018. Cette société articulait services d'investissements et prestations de service marketing, dans des proportions variables selon les clients. Ces clients étaient des « projets » dans le vocabulaire d'Arnaud : les entrepreneurs porteurs d'un projet de DApp cherchant à obtenir des financements par une ICO.

Pour Arnaud, les jetons dignes d'intérêt devaient être conçus pour avoir une utilité « réelle ». Cette assertion peut paraître évidente du point de vue d'un utilisateur de services ; mais pour Arnaud, cette utilité future participait à la valorisation des jetons pour les investisseurs. Cette utilité réelle signifiait que les jetons ne devaient pas être créés dans le seul but de lever des fonds en vantant des retours sur investissement mirobolants. Arnaud m'expliquait que, sinon, leurs valorisations marchandes s'effondraient systématiquement. Arnaud pointait un hiatus entre la valorisation d'un jeton (sur les *exchanges*) et la valorisation des sociétés qui cherchaient à obtenir des capitaux :

Le principal, pour moi, c'est quelle est l'utilité du token. En fait le truc déjà, et ça c'est un problème cœur vraiment dans les cryptos, c'est la valuation d'une boîte. Le market cap¹⁰⁰, donc tu as le supply multiplié par le prix du token, ne représente pas forcément la valeur de la boîte qui va être représentée par l'equity. [...] Sur la vingtaine de projets [pour lesquels Arnaud a levé des fonds], ben t'en as deux qui vont être géniaux, t'en as seize qui vont être à chier et t'en as deux qui seront peut-être moyens. [...] Et en fait il n'y a pas d'utilité autre que lever des fonds, et essayer de créer une communauté pour incentivizer les gens ensuite vu qu'ils ont un bout de ton truc, à faire de la pub pour toi, à en parler autour... ce qu'ils auraient aussi pu faire s'il y avait de l'equity. Donc c'est juste, les gens créent leur token comme ça parce que tout le monde créé leur token et ils ne réfléchissent pas trop, et en fait ben ils se plantent après, tout simplement quoi. (entretien avec Arnaud, septembre 2019, mes ajouts entre crochets)

Arnaud déplorait les pratiques qui avaient conduit à l'explosion du nombre de jetons émis par ICO entre 2017 et 2018 avec le développement des DApps (voir Figure 7) : à cette période il était en effet « facile » de lever beaucoup d'argent à partir d'un *whitepaper* décrivant un projet de DApp. Tous les moyens étaient alors bons. Bien avant que les influenceurs de tous poils s'emparent des cryptoactifs comme tout autre produit

100 Par « market cap », Arnaud désignait la « capitalisation de marché », discutée en introduction de ce Chapitre.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

publicitaire, certains « influenceurs des cryptos » avaient fait une spécialité de cette pratique en jouant de leur réputation dans le milieu des cryptoactifs. Des Youtubers, comme l’influent Ivan On Tech, facturaient des vidéos promotionnelles de quelques dizaines de minutes pour des dizaines de milliers de dollars étatsuniens pièce. John McAfee, sulfureux fondateur du célèbre antivirus éponyme, s’était distingué en se targuant de facturer 105 000 dollars étatsuniens par tweet promotionnel pour un projet d’ICO (Liao 2018). Il avait par ailleurs monté de toute pièce une équipe de rédaction de *whitepapers* pour entrepreneurs peu scrupuleux (Figure 12).



Figure 12 : Tweet de John McAfee faisant la publicité d'un service de rédaction de whitepapers

L'ampleur des montants de ces services de marketing fondées sur la réputation de leurs auteurs étaient tellement élevés que de nombreux « crypto arnaqueurs » (*crypto scammers*) usurpaient l'identité de ces personnalités pour extorquer des bitcoins ou des ethers à des entrepreneurs soucieux de faire connaître leur projet : en se faisant passer pour ces personnalités, ils promettaient à des entrepreneurs repérés sur les réseaux sociaux ou sur les groupes Telegram de passionnés et d'investisseurs en cryptoactifs une publicité qui serait utile à leur ICO. Ce phénomène était si généralisé que certains luttèrent directement contre ces arnaqueurs, par exemple en les dénonçant ou en tentant de les piéger (Sanders 2018). Pour Arnaud, ces pratiques traduisaient une tendance généralisée à la déconnexion entre les prix des prestations promotionnelles et la valeur des services proposés dans ce milieu.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Arnaud me confiait que la déconnexion était telle qu'il arrivait que des arnaqueurs soient démasqués, car les montants qu'ils demandaient étaient trop faibles par rapport aux montants mirobolants demandés par les personnalités dont ils usurpaient l'identité.

Intéresser d'abord, monnayer l' enrôlement ensuite

Arnaud pratiquait lui aussi l'influence pour, en ses termes, « créer de la hype » pour un jeton. Mais Arnaud influençait des « membres » d'une communauté d'individus intéressées par les cryptoactifs qu'il avait lui-même constituée. La société d'Arnaud articulait deux activités auprès de sa communauté, constituée sur des groupes Telegram et sur Discord. D'une part, la société assurait la mise en visibilité du jeton et du projet d'entrepreneurs clients auprès de cette communauté (marketing), et d'autre part, elle investissait dans des jetons avant ou après l'émission (investissement). Cette communauté de membres était sa ressource essentielle : elle lui permettait d'attirer ses clients (services marketing) et lui permettait de négocier des prix de jetons intéressants (investissement). Plus sa communauté était grande, plus il pouvait espérer attirer des projets de « bonne qualité ». Un enjeu important d'Arnaud était donc d'attirer le maximum de membres dans ses différents groupes, mais aussi de protéger ses membres de sollicitations extérieures :

En effet, le cœur du business en tous cas pour ce qu'on fait, notre groupe, à la fois donc les pools, la levée de fonds ou juste les communautés pour le marketing, c'est avoir une communauté active, de qualité, et la plus grosse possible en fait. Si t'as ça, ben tu peux faire payer plus les projets, tu peux demander plus, tu as des projets de meilleure qualité qui voudront travailler avec toi. Donc c'est vraiment un business de communauté. Et encore une fois, on était très naïf au début quand on a commencé et pas du tout assez agressifs. Ce que plein de nos concurrents ont fait c'est qu'ils avaient des bots pour spam en fait. Et ils envoyaient des milliers de MP [messages privés] très facilement à tous les autres membres des groupes de pools. Ils étaient un peu idiots parce qu'ils n'avaient pas pensé que leurs scripts envoyaient les messages aux admins parfois, donc on s'en rendait compte et on recevait nous aussi les messages « oh venez rejoindre notre groupe, c'est super voilà, on a travaillé avec tel projet, tel ROI [Retour Sur Investissement] ». Ou alors pour ceux qui arrivaient à ne pas target les admins, nos membres nous disaient parfois « tiens j'ai reçu 3 PM [private messages, anglais « message privés »] aujourd'hui, pour rejoindre tel groupe tel groupe et tel groupe », bref. (entretien avec Arnaud, septembre 2019)

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Pour recruter des membres, Arnaud employait différentes techniques. Il avait recours, comme les entrepreneurs, à des techniques publicitaires classiques comme l'achat d'espaces publicitaires sur des sites Internet spécialisés (typiquement, sur des sites listant les ICO comme ICObench ou de référencement des cryptoactifs comme CoinMarketCap). Arnaud m'expliquait que les techniques « côté clair de la force » prenaient du temps, ne payaient pas tout de suite, mais permettaient de construire une communauté de manière « organique ». Outre la publicité, Arnaud cherchait à « se faire remarquer » sur des arènes de discussion en ligne, comme Medium, Quora, BitcoinTalk ou Reddit : il s'agissait alors d'écrire « des choses intéressantes », quel que soit le format de la plateforme, mais toujours en veillant à ce que les informations professionnelles de son profil Telegram (son statut de cofondateur avec le nom de sa société et un lien vers son site Internet) soient bien visibles. Une « stratégie » consistait à répondre régulièrement à des questions en lien avec les cryptoactifs sur ces plateformes. Ces techniques s'opposent au « côté obscur de la force », comme le « *spam marketing* » qui consistait à créer de faux profils et à les ajouter massivement dans son groupe pour le faire grandir artificiellement. Bien que ces techniques soient très peu coûteuses auprès de prestataires spécialisés (15 dollars les 1000 membres), il les jugeait dangereuses car elles faisaient peser un risque de crédibilité et de réputation à son groupe si des membres authentiques remarquaient ces faux profils qui mécaniquement apparaissaient comme « supprimés » au bout de six mois.

Arnaud intéressait ses membres en permanence en animant le groupe, notamment en diffusant quotidiennement un résumé des nouvelles du jour dans le secteur des cryptoactifs (actualités financières, réglementaires, nouveaux projets, annonces de développement d'infrastructures). Il organisait les discussions avec les membres sur les groupes de discussion. Arnaud m'expliquait passer beaucoup de temps à expliquer le mode de fonctionnement du groupe aux nouveaux arrivants, de manière à les « gagner un par un ». Ce lien régulier avec les membres lui permettait de vendre cet espace de discussion à ses clients, dans le cadre de prestations de marketing.

La Figure 13 illustre une situation que j'ai observée sur le groupe, avec à droite le verbatim que me donnait Arnaud en entretien pour décrire sa technique d'intéressement. La

Chapitre 2. Les modes des jetons : instituer par les smart contracts

prestation de service consistait à annoncer aux membres une séance d'échanges avec un entrepreneur client qui ferait la promotion de son jeton, et de monter cet échange comme un concours : les membres qui posaient les « meilleures » questions obtenaient une « récompense » en jetons de la startup. Arnaud prévoyait un court moment (deux ou trois minutes) pendant lequel les membres étaient autorisés à poser leurs questions à cet entrepreneur. Ce faisant, Arnaud concentrait l'attention de ses membres vers le projet, chacun observant les questions que les autres posaient. Mais dans le même temps, Arnaud capitalisait sur la séquence qui était enregistrée, puis intégrée à un montage vidéo diffusé sur Youtube pour vanter l'enthousiasme que le projet avait généré dans les communautés d'investisseurs, « preuve » vidéo à l'appui.

Rendre visibles des projets auprès de ses membres permettait non seulement à Arnaud de proposer des prestations de marketing aux « projets », mais aussi de valoriser sa propre activité. Sa communauté était un public « capté », le groupe Telegram opérait comme un « dispositif de captation » (Cochoy 2004). Plus les projets qu'Arnaud valorisait réussissaient, plus il pouvait « monter dans l'échelle des projets avec qui [il] travaill[ait] », et viser ces projets qu'il appelait les « *top tiers* ». La qualité d'un projet d'ICO s'appréciait, pour lui aussi, à la « hype » dont chacun bénéficiait, c'est-à-dire au nombre de personnes qui en parlait. Arnaud m'expliquait que la mesure de la hype était difficile. De nombreux projets créaient de faux comptes pour vanter les mérites de leurs projets dans des groupes Telegram publics, parfois avec habileté. Certains commençaient par ne pas parler de leur projet, puis glissaient des liens ou des commentaires élogieux une fois qu'une confiance a été construite. D'autres procèdent plus systématiquement en employant une ou deux dizaines de prestataires (rémunérés à la tâche) avec pour compétence minimale de savoir écrire, de manière à générer des « vagues » d'attention sur un projet donné dans différents groupes Telegram ou sur des forums et réseaux sociaux. Personnellement, j'ai souvent été sollicité par des comptes qui m'étaient inconnus, *via* des messages personnels indiquant ce type d'éléments promotionnels, alors que je ne m'exprimais pas sur les groupes.

Chapitre 2. Les modes des jetons : instituer par les smart contracts



Figure 13 : Exemple d'avalanche de questions à l'ouverture du chat – mes rajouts en rouge (concentration des messages) et gris (anonymisation)

« Et là, ce qu'on a fait récemment, c'est qu'on a fait un format beaucoup plus structuré, où **tu as une petite introduction au début** où le chat est muté en fait, **personne ne parle sauf nous, donc ça permet d'avoir une bonne idée de ce que le projet est**, ça dure 10-15 minutes, les gens se présentent. Et ensuite ce qu'on fait ensuite c'est exactement, c'est dans l'esprit pur crypto, c'est pour créer de la hype au maximum. Donc en gros, **on laisse le chat ouvert juste 2 ou 3 minutes**, et dans cette petite période de temps, les gens peuvent poster leurs questions. Donc comme la période de temps est très faible, et qu'il y a **des récompenses pour les meilleures questions**, tu vas avoir beaucoup de gens qui vont post dans un petit laps de temps. Et ce qu'on fait ensuite c'est qu'on record [enregistre] ça, **on record l'événement, et ensuite on édite la vidéo, et ça fait une petite vidéo qui va être un peu virale pour les projets**. Parce que quand tu vois la vidéo et tu vois qu'il y a 3 messages par secondes et que le chat défile super vite tu te dis « **mais c'est dingue, il y a plein de gens qui sont super intéressés par ce projet, ça vaut peut-être le coup que je regarde** ». » (entretien avec Arnaud, septembre 2019)

La taille de sa communauté, et par là sa « réputation », permettait également à Arnaud de négocier le tarif d'achat des jetons (typiquement auprès de projets qui étaient également ses clients dans le cadre de prestation marketing). Comme d'autres investisseurs aux capacités financières dépassant un certain seuil, Arnaud pouvait prétendre à des tarifs avantageux. Il avait accès aux « *private sale* » de jetons : des ventes organisées avant l'ICO ouverte au « public », restreintes à ces grands investisseurs, donnant droit à des tarifs négociés en fonction du montant investi. Ce tarif réduit lui permettait de proposer les jetons à ses membres à un prix réduit par rapport à la « *public sale* », tout en empochant une commission qu'Arnaud estimait à environ 15 % du prix du jeton pour le public. Toutefois, Arnaud ne prenait aucune commission sur les ventes auprès de ses plus gros investisseurs, appelés « *whales* » dans le milieu des cryptoactifs. Arnaud cherchait à créer un « climat de

confiance » pour ces gros poissons, autrement dit, à les maintenir captifs. Même s'ils ne rapportaient pas de revenus directs en achetant des jetons, ces investisseurs permettaient à Arnaud d'acheter de gros volumes lors des « *private sales* », et par conséquent d'obtenir des tarifs avantageux.

Les IEO, ou la fusion des valorisations marchandes et entrepreneuriales

A partir de 2019, les *exchanges* ont eux-mêmes joué le rôle d'assistance à l'émission de jetons, ou d'organisateur de la rencontre entre entrepreneurs et investisseurs, c'est-à-dire le rôle que jouaient des intermédiaires comme Arnaud. Ce dernier situait les *exchanges* comme des compétiteurs directs, mais dotés d'une force dont lui-même ne disposait pas, en raison de leur envergure financière, mais aussi du rôle institué des *exchanges* comme producteurs du prix des jetons. Cette cotation était essentielle pour les entrepreneurs, comme l'illustrent les cas Digix et Bluzelle : l'achat et la vente de jetons sur les *exchanges* permettait, d'une part d'articuler le service fonctionnant comme une plateforme « autonome » à ses utilisateurs (clients, fournisseurs), et d'autre part d'articuler investissement présent et utilité future (au sens d'utilisation ou de gouvernance du service).

Les ICO organisées par les *exchanges* étaient devenues si courantes qu'elles étaient nommées spécifiquement : « *Initial Exchange Offering* » (IEO). Comme Arnaud, les *exchanges* valorisaient le public utilisateur de leurs sites web ou applications mobiles. Mais les *exchanges* disposaient d'un argument supplémentaire : rendre le jeton directement achetable sur leur interface, et publiciser la vente à une audience très large, par exemple en mettant le jeton « à la une ».

En retour, les *exchanges* étaient très exigeants, me racontait Arnaud. Deux types de rémunérations peuvent être distingués. D'une part, ils exigeaient des rémunérations directes aux entrepreneurs : une commission pré-IEO, à laquelle s'ajoutait un pourcentage sur les fonds levés post-IEO ainsi qu'un pourcentage des jetons émis eux-mêmes. D'autre part, l'*exchange* se rémunérait indirectement en imposant l'unité de change du jeton émis ;

Chapitre 2. Les modes des jetons : instituer par les smart contracts

typiquement, cette unité était un jeton dont ils maîtrisaient eux-mêmes l'émission et le taux de change dans les autres devises génériques comme le bitcoin ou l'ether. Ce mode d'émission, s'il était favorable à la mise en visibilité des projets, impliquait des coûts variables selon l'*exchange*. Tous les entrepreneurs ne pouvaient pas s'y conformer, au risque de tuer leurs projets dans l'œuf.

L'exemple le plus célèbre de ce type de rémunération indirecte par un jeton *ad hoc* est Binance, fondé à Hong Kong en 2017. Binance était réputé comme *exchange* le plus important en termes de volume de transactions en 2019 et inventeur des IEO. Binance disposait de son propre jeton émis sur Ethereum, le BNB, créé au départ pour fidéliser les utilisateurs en divisant les frais de transaction en BNB par deux : les utilisateurs étaient incités à conserver un montant de BNB, donc à rester sur Binance.

Ainsi avec les IEO, les *exchanges* attiraient et fidélisaient des utilisateurs contraints d'acquérir leurs jetons pour pouvoir investir dans d'autres jetons dont l'émission était exclusivement assurée par un *exchange* donné. Ce mécanisme a été radicalisé suite au succès des premiers IEO début 2019 : Binance a décidé de limiter l'accès aux IEO aux utilisateurs qui avaient préalablement « gagé » (*stake*) un montant de BNB sur Binance plusieurs jours ou semaines préalablement à l'IEO.

Cette promotion du jeton de l'*exchange* via les IEO avaient deux avantages supplémentaires pour les *exchanges*. D'une part, les *exchanges* s'assuraient un afflux régulier d'actifs fraîchement apportés par ses utilisateurs, actifs à la totale disposition de l'*exchange* pour toutes ses activités commerciales et financières (change, investissement) avec un horizon de temps garanti (car « gagés »). D'autre part, en contraignant les possibles investisseurs à utiliser son jeton, les *exchanges* amélioraient la valorisation de marché de leurs jetons, c'est-à-dire leurs prix en ethers ou en bitcoins, en stimulant le volume d'échange global.

Du fait des relations établies avec des entrepreneurs ayant été contraints de faire ce type de compromis, Arnaud m'a rapporté des pratiques qu'il qualifiait de « manipulations » de marché. En voici deux exemples. Premièrement et au moment de l'émission, dans les cas

Chapitre 2. Les modes des jetons : instituer par les smart contracts

où l'objectif de vente des jetons n'était pas atteint, certains *exchanges* faisaient croire que la vente avait bien eu lieu à 100 %, de manière à « garder un semblant de hype ». Deuxièmement et après l'émission, des *exchanges* exigeaient des entrepreneurs qu'ils engagent eux-mêmes des « animateurs de marché » (*market makers*), c'est-à-dire des sociétés qui passent des ordres sur l'*exchange* pour former et orienter le prix du jeton tout juste émis. D'une part, l'animateur de marché passait des ordres d'achat et de vente simultanément, de manière à assurer qu'un prix « de marché » existe bien, c'est-à-dire garantisse un volume minimum d'échanges. L'objectif était d'éviter que le nombre de transactions soit insuffisant, et que la différence entre le prix d'achat et le prix de vente soit importante, signes de désintérêt des investisseurs pour ce jeton. D'autre part, l'animateur de marché pouvait aider à atteindre des retours sur investissements hebdomadaires, eux-mêmes imposés à l'avance aux entrepreneurs. Par exemple, l'*exchange* pouvait exiger que le prix du jeton ai progressé de 20 % au bout d'une semaine, de 50 % au bout de deux semaines. Pour tenir ces objectifs, les animateurs de marché pouvaient, à un moment jugé opportun, décider d'acheter massivement le jeton (on parlait alors de stratégie de « *buy wall* ») pour provoquer un pic d'intérêt pour ce jeton.

Dans cette section, j'ai considéré les jetons utilitaires par les yeux de leurs concepteurs. Dans la section suivante, j'analyse leur institutionnalisation.

2. La conception institutionnelle des jetons

La section précédente pourrait laisser penser que les espaces de développement et de circulation des jetons sont séparés du reste du monde : sur leurs sites web, des forums ou des groupes Telegram, des entrepreneurs diffuseraient une idée *via* un *whitepaper*, semblent discuter et lever des fonds *via* un réseau décentralisé et des *exchanges* accessibles eux aussi depuis n'importe quelle machine connectée à Internet. Cette lecture renforce l'autonomie accordée à ces objets par leurs concepteurs et dénoncée par leurs rares critiques. En France, le groupe de réflexion Institut Rousseau était l'organisation critique la plus audible. Une tribune signée par 170 économistes, informaticiens, experts et personnalités scientifiques en février 2022, titrée « Il est urgent d'agir face au développement du marché des cryptoactifs et de séparer le bon grain de l'ivraie » (Institut Rousseau 2022), plaidait pour une intégration des cryptoactifs dans la réglementation. Les auteurs listaient des « craintes légitimes » face à des objets qui « bousculent » le « monde monétaire et financier », et appelaient à une coopération internationale « avant que la situation ne soit hors de contrôle ».

Le développement des cryptoactifs est institutionnel, ses espaces de conception sont articulés au reste de la société. Une première sous-section identifie deux points d'articulation : les réseaux entrepreneuriaux dans lesquels sont impliqués des institutions publiques, et les *exchanges* qui garantissent la convertibilité entre jetons et argent de ces espaces (ethers, bitcoins) ou du reste du monde (typiquement en dollar étatsunien). Ainsi, le développement des cryptoactifs que je propose de comprendre comme institutionnalisation doit être distingué des analyses sociales et économiques qui font de ces objets des institutions en elles-mêmes (« technologies institutionnelles »). Une seconde sous-section présente un pan d'enquête à la fois utile dans ce chapitre et fil rouge empirique de l'ensemble de la thèse : les meetups organisés par ConsenSys. Je les comprends comme sites de problématisation (Callon 2012) des cryptoactifs, comme espaces donnant accès aux significations que les acteurs de leur institutionnalisation leur donnent. En particulier, je montre que ces acteurs problématisent les jetons utilitaires comme des objets marchands, et

ce faisant, limitent les incertitudes pesant sur leur prolifération. Dans une dernière sous-section, je montre que ces mêmes réseaux d'acteurs confirment cette délégation aux concepteurs. Investis de la légitimité institutionnelle de définition de la signification des jetons qu'ils créent, ces derniers étendent la prolifération des jetons à des acteurs qui leur étaient *a priori* opposés : les institutions financières privées.

2.1. Un processus de conception institutionnel

Pratiques de conception : standardisation et réseaux de proximités

Les pratiques partagées de conception et de financement des jetons utilitaires (section précédente) n'étaient pas confinées à des entrepreneurs et investisseurs qui travailleraient indépendamment du reste du monde. Les paragraphes qui suivent indiquent deux articulations. Premièrement, elles étaient inscrites dans des formes standardisées des *smart contracts*, participant à leur diffusion rapide. Deuxièmement, le développement des jetons utilitaires était une activité de réseaux entrepreneuriaux soutenus par des administrations qui les voyaient par le prisme de politiques publiques favorisant les technologies émergentes en général.

Premièrement, un même standard de *smart contracts* appelé ERC-20 était utilisé dans tous les cas constituant mon sous-corpus d'enquête sur les entrepreneurs de DApps à Singapour (Tableau 4). Les *Ethereum Request for Comments* (ERC) étaient des standards informatiques de *smart contracts*. Ces ERC étaient des types particuliers des *Ethereum Improvement Proposals* (EIP), lesquels décrivaient plus généralement les standards pour Ethereum couvrant les *smart contracts* ainsi que les spécifications du protocole réseau¹⁰¹. Les EIPs étaient des propositions d'amélioration d'Ethereum qui suivaient un processus de validation par les développeurs, similaire à celui d'autres communautés *open source*. Elles faisaient explicitement référence à la construction d'Internet : ERC était calqué sur RFC, les *Requests For Comments* qui avaient fait de TCP/IP un protocole standard, avant d'être

101 Les descriptions fonctionnelles des EIPs pouvaient être consultées à : <https://eips.ethereum.org/>. Les spécifications techniques pouvaient être consultées à : <https://github.com/ethereum/EIPs>.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

étendues comme un processus lui-même standard d'élaboration des différents protocoles d'Internet.

Le standard ERC-20 a directement participé à l'institutionnalisation des jetons en les rendant interopérables, notamment *via* les *exchanges*. Les standards de jetons ERC associaient une forme technique (des fonctions d'un *smart contract*) à un usage. L'ERC-20, norme technique définie en 2015 (Ethereum Foundation 2023), convenait à la fois pour l'émission de jetons d'ICO que pour les jetons utilitaires. L'utilisation de l'ERC-20 dans les cas de Digix et de Bluzelle montrent que le standard participait à associer ces projets à un phénomène d'ensemble ; autrement dit, à les institutionnaliser. Dans les deux cas, les jetons « internes » aux DApps (Gold Asset Card, BNT) étaient écrits selon des logiques spécifiques à ces plateformes, sans souci de standardisation. En revanche, les jetons « externes » aux plateformes (BLZ, DGX, DGD) qui liaient l'utilisation d'une DApp particulière à un ensemble social plus vaste étaient écrits dans le standard ERC-20.

Les jetons ERC-20 articulaient le foisonnement de jetons (avec leurs services imaginés et opérations de capitalisation) à des utilisateurs et investisseurs qui voyaient un même type d'objets accessibles et échangeables sur différentes places d'échanges. L'ERC-20 est un cas d'articulation entre des pratiques de conception et une classification des objets du monde (Bowker & Star 1998 : 234). Joseph Lubin, un des cofondateurs et protagonistes importants du développement d'Ethereum sur la période d'enquête, expliquait rétrospectivement que le standard ERC-20 a directement participé à rendre Ethereum et les jetons populaires :

*I think **one of the main reasons that Ethereum got so popular was because we de facto standardized on ERC-20**, making it easy for anybody to issue these tokens, making it easy for exchanges and wallets to deal with them, and for people who issued them to know that exchanges and wallets would deal with them. And so **we need to see so much more of that and we do, through the EIP process**, it's not a perfect process, but it's a pretty great process for achieving standardization. (Joseph Lubin, mars 2020, Ethereum Community Conference, Palais de la Mutualité à Paris)*

Deuxièmement, les différentes startups dont j'ai rencontré les cofondateurs en entretiens travaillaient en réseaux. D'une part, des entreprises se spécialisaient dans le développement

Chapitre 2. Les modes des jetons : instituer par les smart contracts

de DApp, de formes standards de jetons ou de développements spécifiques (notamment « internes » aux DApps). C'était le cas d'Attores, société qui a contribué au développement d'Averspace, de Digix et de Popety, et qui était fondée et dirigée par un des cofondateurs d'Indorse (cf Tableau 4). D'autre part, ces entrepreneurs imaginaient leurs services comme des composants d'un ensemble plus grand, le Web 3.0. Le « *developers fund* » imaginé par Bluzelle introduisait un caractère évolutif au service de stockage de données décentralisé, à la main de développeurs qui souhaiteraient s'engager à développer des API (*application programming interfaces*) avec d'autres services. Le cofondateur d'Indorse m'expliquait en entretien voir Bluzelle comme une solution de stockage possible pour le développement de son service de réseau social décentralisé. Digix voyait son service comme une couche à partir de laquelle d'autres développeurs pourraient bâtir « au-dessus » (*on top of*), par exemple des services qui représenteraient des valeurs stables car adossés à son « or numérique », le DGX.

Ces entrepreneurs avaient des relations de proximité topographiques et institutionnelles. Plusieurs d'entre eux occupaient les mêmes bâtiments ; souvent les mêmes collaboraient. Sur les six startups ayant eu recours à l'émission de jetons pour se financer, quatre avaient leurs bureaux dans le même bâtiment. Le cofondateur de Kyber Networks m'expliquait qu'il existait un lien direct entre la force d'Ethereum comme plateforme de développement et sa « communauté », observable dans des proximités et des collaborations étroites entre projets. Il soulignait, dès mon arrivée dans ses locaux pour l'entretien, que la pièce dans laquelle nous allions nous entretenir, qui était simplement séparée de l'espace de travail par une baie vitrée, était intéressante pour « partager des invités » avec d'autres startups aux bureaux proches. Il m'expliquait que la Fondation Ethereum, qui coordonne notamment la communauté de développeurs de l'infrastructure, avait des bureaux « de l'autre côté de la rue ». Il n'était pas question pour cet entrepreneur de participer au développement du protocole ; mais il lui était possible d'avoir des soutiens et de « demander » facilement des évolutions à la Fondation Ethereum.

Cette proximité physique et ces collaborations professionnelles étaient promues par des acteurs ayant pour mission de développer l'entrepreneuriat à Singapour en général, et le

Chapitre 2. Les modes des jetons : instituer par les smart contracts

développement des startups bâtissant des DApp sur Ethereum en particulier. SG Innovate se présentait comme une entreprise privée financée par le gouvernement qui avait « commencé comme une startup pour startups », par l'investissement. Cette entreprise participait à la constitution de « communautés » comme le *deep learning* ou la blockchain en nouant des partenariats spécifiques, par exemple avec Google, IBM, ou avec la Fondation Ethereum (SG Innovate 2017). Ces communautés répondaient à un objectif gouvernemental : favoriser l'émergence d'écosystèmes entrepreneuriaux en développant des technologies de pointe « pour Singapour et pour le monde », sélectionnés en fonction de l'impact espéré de ces choix en termes de développement entrepreneurial :

We focus on entrepreneurial drive and impactful solutions for Singapore and for the world. The question is which space is crucial? Fintech was the buzz of the day. But yet they have all been done and ecosystem is already there, very active and vibrant. We have then to focus on where it matters most. We want to focus on IA: there is a centric activity. There is hardly an AI community here and we want to focus on it and build companies, where the ecosystem is vibrant and active. Blockchain and medtechs are the next ones. Deep tech is our nexus strategy. We are currently working with eleven partners GSIC [Government of Singapore Investment Corporation]: Nvidia, IBM, GSEs... With them, we have a training curriculum, and a community activity. There is a lot of demand but there is no driving force. Community grown by 50% since November, that's why we know this is the right area. (entretien avec un responsable de SG Innovate, février 2018)

SG Innovate fédérait des « écosystèmes » orientés vers le développement de « cas d'usages », auxquels participaient des financeurs institutionnels privés et publics, de grandes entreprises, mais aussi des universités et des startups. Le cofondateur d'Attores m'indiquait avoir bénéficié de l'aide de SG Innovate, alors appelé Finlab, pour lancer son entreprise. Cette collaboration lui avait par exemple permis de trouver un premier débouché dès 2016 auprès de l'université Ngee Ann Polytechnic avec qui a été développée une application d'inscription des diplômes universitaires sur Ethereum, afin de réduire les risques de fraude. C'était également d'espaces de travail qu'ont Atttores, Digix et TenX, qui travaillaient côte-à-côte dans les locaux de SG Innovate quand ils lançaient leur affaire, avant de déménager chacun dans des bureaux à quelques minutes à pied les uns des autres. C'est aussi SG Innovate qui proposa des espaces pour la tenue de meetups, des événements rassemblant la « communauté Ethereum » pilotés par Steve, le cofondateur de Digix. C'est

encore SG Innovate qui offra régulièrement un lieu de résidence professionnelle à l'inventeur d'Ethereum Vitalik Buterin.

Les argents de la conception de DApps : ethers et bitcoin articulés au dollar étatsunien

Les jetons des concepteurs de DApps prenaient des significations spécifiques dès leurs émissions : leur attribution nouait des relations spécifiques avec différents acteurs du projet. Nous avons vu que les jetons BLZ crédibilisaient le projet entrepreneurial en associant différents participants passés et futurs, et enrôlaient des utilisateurs futurs en les faisant investisseurs au présent. Nous avons aussi vu que les jetons DGD signifiaient droits de gouvernance du service futur et investissements au présent. Ces jetons sont des opérations de marquage, parfois au sens matériel du terme. Par exemple, les jetons alloués aux cofondateurs de Bluzelle étaient bloqués dans un *smart contract* pour plusieurs années, signifiant que l'argent qu'ils représentaient *via* les *exchanges* ne pouvait être que futur, et qu'en attendant les bénéficiaires étaient incités à travailler pour que leur valorisation future s'apprécie. Les ethers obtenus par DigixGlobal étaient eux aussi bloqués dans un *smart contract*, contrôlé seulement par les détenteurs de DGD.

L'argent obtenu dans l'opération d'ICO était toujours de l'ether et des bitcoins sur mon échantillon de projets. Dans le même temps, les concepteurs disposaient aussi de monnaie ayant cours légal : si leurs *wallets* étaient constitués de bitcoins et d'ethers, leurs comptes bancaires étaient garnis de monnaies comme le dollar étatsunien ou de singapourien, provenant notamment des financements autres que les ICO (par exemple en capital-risque) et par la conversion de cryptoactifs *via* les *exchanges*. La convertibilité permettait aux entrepreneurs de payer le travail de construction des DApps ainsi que les frais liés à l'activité entrepreneuriale plus généralement.

Les *exchanges* avaient un rôle central. Ils articulaient deux vues en permettant l'achat et la vente des cryptoactifs : d'une part celle des concepteurs et des ceux qui voyaient dans les jetons des usages comme un « Web 3.0 » (plus tard une « finance décentralisée ») et dans

Chapitre 2. Les modes des jetons : instituer par les smart contracts

l'ether et le bitcoin de l'argent, et d'autre part celle des investisseurs ou utilisateurs qui voyaient dans ces objets des objets financiers classés selon des profils de risque ou de rentabilité. Ces derniers étaient listés les uns à la suite des autres : les investisseurs ou futurs utilisateurs pouvaient choisir les cryptoactifs comme dans un catalogue, selon leurs cours en bitcoins ou en ethers ou selon l'évolution de ces cours, ou encore selon leurs capitalisations.

Ce rôle central de passerelle conférait aux *exchanges* une position stratégique. Avec les IEO, les *exchanges* ont tiré directement profit de leur rôle central dans la réussite d'une ICO. En les organisant eux-mêmes, ils imposaient l'achat des jetons qu'ils avaient eux-mêmes créés, comme le BNB pour Binance (voir section précédente). Cette position stratégique peut plus récemment s'observer dans la devise proposée par défaut par l'agrégateur et fournisseur de données sur les cryptoactifs CoinMarketCap (Figure 6), le plus populaire au moment de l'enquête. Aujourd'hui, et suite à son rachat par le chinois Binance, ce site étatsunien propose par défaut d'analyser les différents cryptoactifs (cours, capitalisation) en BNB, participant à imposer Binance comme un acteur central de l'agencement étendu décrit à la section précédente.

Le dollar étatsunien était l'unité de référence pour les *exchanges*, pour les entrepreneurs et pour les investisseurs. Les classements des cryptoactifs en termes de cours et de capitalisations étaient généralement, par défaut, en dollars étatsuniens. Les entrepreneurs que j'ai rencontrés à Singapour donnaient les chiffres de leur ICO en dollars étatsuniens à la date à laquelle ils me parlaient. Selon les chiffres donnés plus haut pour Digix, les fonds collectés durant l'ICO ont été multipliés par plus de 70 en dollars étatsuniens à la date de l'entretien, soit en 23 mois. Les investisseurs raisonnaient également en monnaie légale : les retours sur investissements clamés par les influenceurs de tout poil étaient formulés en dollars étatsuniens ou en euros.

Les cours en dollar étatsunien fournis par les *exchanges* servaient également de référence aux investisseurs. Ci-après je présente un exemple d'indicateur construit par un fonds de capital-risque qui tentait d'évaluer la pertinence d'Ethereum comme une « plateforme de

Chapitre 2. Les modes des jetons : instituer par les smart contracts

smart contracts », c'est-à-dire comme autre chose que l'unité propre à un réseau comme le bitcoin. Cet indicateur, appelé l'ETH NVTV, pour « *Ethereum Network Value / Token Value* »¹⁰², était construit à partir des données de capitalisations de marché de l'ether et des jetons disponibles sur les agrégateurs comme CoinMarketCap. Cet indicateur était le résultat du calcul, à une date donnée, du ratio entre la capitalisation de l'ether (numérateur) et la somme des capitalisations de tous les jetons sur Ethereum (dénominateur). Il était utilisé par des analystes qui publiaient sur des sites spécialisés.

*The [NVTV] metric compares the market capitalization of Ether to that of all the tokens launched on the network. **This network value to token value ratio evaluates the health of Ethereum's token ecosystem.** A value of one indicates that Ether's market cap and the aggregated market capitalization of the tokens it hosts are equivalent. That implies a healthy, possibly undervalued smart contract platform. (De Havilland 2019)*

Ce ratio cherchait à mesurer la « santé » de « l'écosystème de jetons », jugée d'autant meilleure que la capitalisation de l'ether était proche de la somme de l'ensemble des capitalisations des jetons. Dans les deux cas, les données utilisées supposaient que l'unité commune d'évaluation de l'ether et des jetons est le dollar étatsunien. La capitalisation de marché de l'ether traduisait la « valeur du réseau » (le même raisonnement pourrait être appliqué à Bitcoin). En indiquant que la valorisation totale de l'ether devait correspondre aux valorisations des jetons, l'ether était cadré comme l'argent des ICO et représentatif de la valeur intrinsèque du réseau, plutôt que comme un moyen de paiement pour l'exécution des *smart contracts*.

Selon cette dernière vue, l'ether était une ressource pour le fonctionnement d'Ethereum, une marchandise, qualification retenue par l'agence fédérale américaine de régulation des bourses et matières premières qui l'avait qualifié de « *commodity* » (CFTC 2019) comme elle le fit pour le bitcoin : un produit de base, standardisé, aux qualités définies et connues des acheteurs qui se l'approprient *via* un marché. Au contraire, les investisseurs ayant élaboré l'ETH NVTV voyaient l'ether, au même titre que le bitcoin, comme de l'argent : une valeur de référence, ou un or numérique dans le langage des promoteurs de Bitcoin

¹⁰² Cet indicateur était calculé par l'analyste Coin Metrics selon la méthode développée par Chris Burniske de Placeholder, un fonds de capital-risque : <https://www.placeholder.vc/>.

(Chapitre 1) plutôt qu'un « combustible » (*gas*) qui sert à l'utilisation des Dapp.

Institutionnalisation d'objets technologiques plutôt que technologie institutionnelle

Avec les éléments des paragraphes précédents, je cherche à montrer que le processus de développement des jetons engageait des acteurs autres que leurs concepteurs. Je cherche ainsi et dans la suite de la thèse à étendre l'analyse des significations politiques et sociales associées à processus de conception, comme un processus d'institutionnalisation. Cette approche se distingue de celle développée par des économistes qui lisent l'imaginaire des concepteurs par le prisme de leurs théories. Les paragraphes qui suivent résument leurs propositions.

Une technologie institutionnelle, génératrice d'institutions économiques : voilà comment des chercheurs se réclamant de la nouvelle économie institutionnelle¹⁰³ décrivent les blockchains en général et Ethereum en particulier. Plusieurs sont affiliés au *Blockchain Innovation Hub* de l'Institut Royal de Technologie de Melbourne (RMIT University) : soit des économistes qui y sont attachés institutionnellement, soit des auteurs comme la chercheuse CNRS et entrepreneure Primavera De Filippi, très citée internationalement pour ses analyses sociales et juridiques des blockchains. Ces auteurs analysent la technologie blockchain comme une révolution des organisations économiques (Davidson et al. 2016a, 2016b, 2018).

Selon ces auteurs, cette technologie est « institutionnelle » car elle produit des faits, objets essentiels à la coordination économique. Ils distinguent la blockchain d'autres technologies de l'information comme les transistors, les ordinateurs, ou Internet. Au contraire, les blockchains seraient de nouvelles institutions économiques du capitalisme que ne seraient pas capables d'instituer les gouvernements, les marchés, ou les relations contractuelles. Les auteurs préfèrent comparer cette technologie à l'invention de la société anonyme plutôt qu'à

103 La nouvelle économie institutionnelle est un ensemble de courants de pensée qui a contribué au renouvellement de l'analyse économique des institutions dans les années 1970 en s'interrogeant sur leur rôle dans la coordination économique.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

l'invention d'Internet. Ces innovations seraient permises par la production de faits sur un registre de manière décentralisée. De ce fait, les blockchains seraient en compétition directe avec les institutions qui organisent le capitalisme contemporain de manière centralisée, les grandes entreprises et les États.

Selon cette approche, la blockchain serait une technologie sociale comparable aux firmes et aux entreprises. Les auteurs la distinguent de la technologie dans l'approche néoclassique : un facteur de production qui cadre les coûts de production. Il ne s'agit pas de voir la blockchain comme une technologie qui permettrait de faire plus (de produits ou services) avec moins (de facteur de production). L'économie néoinstitutionnelle voit les institutions et les organisations comme des technologies sociales productrices de « transactions » entre agents. Son analyse porte sur les coûts de ces transactions. L'intérêt pour les coûts de transaction dans la coordination économique, initialement proposé par Ronald Coase (1937) pour expliquer l'existence des firmes, fut repris par la nouvelle économie institutionnelle à la suite d'Oliver Williamson (1979). Le problème central était alors de comprendre pourquoi les transactions étaient formées par des firmes plutôt que par des marchés. Ces derniers étaient vus comme des organisations nécessairement plus efficaces car décentralisés ; les premières, au contraire, étaient réputées coûteuses en raison de leurs structures hiérarchiques.

La réponse de cette tradition économique passe par la notion d'incomplétude des contrats dans la production de biens ou de services. D'une part, les contrats ne peuvent pas tout stipuler en raison de la « rationalité limitée » des acteurs économiques. D'autre part, du fait de l'impératif pour une firme de coordonner différentes ressources pour assurer sa production, les contrats peuvent être déformés par des comportements « opportunistes » du fait de l'importance de la valeur de la transaction pour le maintien de la production, par exemple en produisant des biens de mauvaise qualité ou en livrant en retard. Traduits en termes économiques, la production engendre des investissements dont les coûts lui sont spécifiques, et par là différents de la valeur que les choses pourraient prendre dans d'autres transactions : la production d'un produit nécessite d'investir dans une pièce spécifique nécessaire à la chaîne de production, ou la fourniture d'un service peut dépendre de

Chapitre 2. Les modes des jetons : instituer par les smart contracts

compétences et savoir-faire spécifiques. Ce problème est appelé « *asset specificity* ». La coordination économique par des firmes permettrait de contrôler cet « opportunisme », par des relations de confiance.

La blockchain et les *smart contracts* apporteraient une réponse originale pour l'organisation de la production, surpassant les marchés et les firmes hiérarchiques, que cette tradition analyse comme une forme institutionnelle de compromis au problème de l'opportunisme. En décentralisant la tenue de registre, la blockchain apporterait une transparence absolue sur le contenu des contrats et sur leur exécution de manière « complète », répondant au problème de « rationalité limitée » jusque-là pris en charge par la firme ; et en raison du caractère « *trustless* » de la technologie, la blockchain permettrait d'établir des relations bilatérales à moindre coût que ne le permettent les marchés qui obligent à traduire les relations de production dans les termes d'un échange.

But the valuable prospect of blockchain, when operationalized with smart contracts and distributed autonomous organizations, is precisely to eliminate opportunism by cryptoeconomic mechanisms. This works by enabling a spot market exchange to carry forward indefinitely a pure promise; in other words, it returns the transaction to a market-like context, but with fewer of the costs of a market. This is revolutionary because it undermines the strong case for the economic efficiency of hierarchies (which exploits incomplete contracts) and relational contracting (which requires trust between parties) over markets. (Davidson et al. 2016b : 16)

L'argument de ces chercheurs est illustré par un « cas d'étude », Backfeed, une startup cofondée par Primavera De Filippi. Le jeton est imaginé comme un élément d'une organisation économique alternative, qui serait « méritocratique », produisant une « coordination stigmergique » inspirée des termites, fourmis ou oiseaux¹⁰⁴. Selon les auteurs, Backfeed pourrait être utilisé par les organisations décentralisées (les DAO comme DigixDAO) pour permettre des « contributions libres et spontanées dans des réseaux distribués ». À la manière des protocoles de consensus entre machines utilisées par Bitcoin et Ethereum, Backfeed permettrait à un réseau d'êtres humains d'atteindre un consensus

104 Un mécanisme de coordination indirecte, à travers l'environnement, selon le principe suivant : la trace laissée dans l'environnement par une action individuelle provoque une autre action, par le même agent ou par un agent différent.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

(Matan 2015) en tenant compte de leur mérite. Celui-ci était défini en fonction des contributions passées à des décisions collectives qui avaient été valorisées par les autres membres du groupe et de ses propres évaluations elles-mêmes évaluées par l'ensemble de ce groupe.

Selon eux, Backfeed permettrait de matérialiser des relations entre individus éloignés, chacun pouvant agir comme écrivain, assuré ou lecteur de journal, mais aussi participant comme éditeur, assureur ou journaliste dans des organisations décentralisées productrices. Les actions dans chacun des rôles seraient rémunérées par un jeton *ad hoc*, échangeable. Ainsi, les auteurs voient Backfeed comme une manière de faire passer la blockchain de « catallaxie » au sens hayekien (« une organisation spontanée dirigée seulement et exclusivement par des dynamiques de marché ») à une économie au sens d' « une organisation ouverte mais plus circonscrite, animée par une hiérarchie uniforme de finalités, et qui incorpore son propre système économique ou monétaire ».

2.2. Meetups de ConsenSys, sites de problématisation des jetons et des smart contracts

Rencontre avec une entreprise en mutation

Ma première discussion avec un employé de ConsenSys a eu lieu dans un café branché de Singapour, dans lequel le responsable pour la région Asie du Sud Est et Pacifique m'avait donné rendez-vous. Ce dernier connaissait tous les entrepreneurs de DApps que j'avais rencontré sur place. Il entretenait avec elles des rapports réguliers : il jouait un rôle d'animateur au sein d'un « *decentralized studio* » qui articulait développement de l'infrastructure Ethereum et des utilisations entrepreneuriales d'Ethereum par des activités d'incubation de startups et d'édition de logiciels :

*ConsenSys support the development of Ethereum with people working on the code of Ethereum at first. On a non for profit basis, for the community. We spent a year or so planning this **community role**. Then a lot of companies went out of ConsenSys, around 100 companies. Then, we wondered: **why not go to business?***

Chapitre 2. Les modes des jetons : instituer par les smart contracts

We launched foundation products. For examples, an identity management plugin called UPort, and a Chrome browser plugin, on top of the browser, called Metamask. (entretien avec le représentant de ConsenSys Asie du Sud Est et Pacifique, février 2018)

ConsenSys a été fondée en 2015 par Joseph Lubin, un des cofondateurs d'Ethereum et ancien membre de la Fondation Ethereum qui organisait les développements de l'infrastructure. Joseph Lubin a financé seul ConsenSys pendant plusieurs années ; cet entrepreneur disposait d'une fortune personnelle qui a été augmentée par sa participation à la fondation d'Ethereum et s'est appréciée au fil des années. L'ICO d'Ethereum permit non seulement de capitaliser la jeune Fondation Ethereum en bitcoins, en échange des éthers « pré-vendus », mais aussi de capitaliser ses cofondateurs de quelques milliers de bitcoins et de millions d'éthers. En raison de la hausse du cours du bitcoin et de l'ether entre 2014 et 2018, ces fonds atteignirent au fil des mois des montants importants en dollars. Fin 2022, Joseph Lubin dirigeait toujours ConsenSys.

Le début de mon enquête coïncidait avec une accélération de la croissance de ConsenSys. Adèle et Cécile, deux employées du bureau de Paris, m'expliquaient en novembre 2018 que la société avait plus que triplé son nombre d'employés au niveau mondial en un an, passant de 400 à la fin de 2017 à 1300 à la fin de 2018. L'activité de la société était divisée en « deux grands pôles ». Premièrement, une activité de « *startup studio* », incubation par les employés eux-mêmes qui développaient des « projets internes » à ConsenSys. D'une part, ces projets correspondaient à des DApps décrites comme des « plateformes », par exemple : de partage d'articles de journaux, de données de santé, d'instruments financiers, ou d'échanges de cryptoactifs. D'autre part, il s'agissait de « projets non pas pour développer des usages commerciaux mais pour développer l'infrastructure d'Ethereum » selon Cécile, comme le « *wallet* en ligne » Metamask dont me parlait déjà le responsable à Singapour. Deuxièmement, ConsenSys construisait un pôle dit « *Solutions* » (prononcé en anglais) pour les activités de conseil. Ces prestations pouvaient signifier développement de projets informatiques pour des entreprises, impliquant possiblement la commercialisation de « projets internes », mais aussi des missions d' « affaires publiques ». Le Ministère des Finances français a par exemple commandé un état de l'art sur la blockchain, la

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Commission européenne avait confié à ConsenSys le pilotage de son « Observatoire Européen de la Blockchain ».

ConsenSys faisait de sa participation au développement d'Ethereum entre 2014 et 2017 une expertise, vendue comme prestations de conseil du deuxième pôle, qui portaient plus largement sur « la blockchain ». J'interrogeais Cécile et Adèle sur les termes qu'elles employaient pour décrire l'activité de ce deuxième pôle : « blockchain » plutôt que « Ethereum ». Les employées m'expliquèrent que la technologie dépendait d'abord du souhait du client : certains clients, pour des raisons « politiques », préféraient par exemple travailler avec Hyperledger, la technologie d'IBM. Ethereum était alors non plus vu comme une infrastructure enregistrant des *smart contracts*, mais comme un logiciel qui était utilisable pour bâtir des infrastructures privées :

Cécile : ConsenSys même si c'est très associé à Ethereum, la position quand le client demande le développement d'une solution, nous on pousse Ethereum, bien sûr, parce qu'on pense que c'est le meilleur, mais on n'arrive pas en leur disant on fait que du Ethereum. Si jamais ils ont des requêtes spécifiques, on s'adapte.

Clément : Qu'est-ce qui vous fait penser que c'est la meilleure, Ethereum plutôt qu'une autre ?

Cécile : À l'heure actuelle ?

Clément : Oui.

Adèle : Ben la puissance d'Ethereum... Elle t'a parlé d'infrastructure tout à l'heure, en fait c'est le fait d'avoir un écosystème. Parce que d'avoir juste une blockchain, c'est une chose mais d'avoir un écosystème autour... Parce que toutes les briques dont tu as besoin pour qu'il y ait une application à la fin que quelqu'un puisse utiliser, un utilisateur qui voit ni clé privée, ni clé publique, que cela ne lui prenne pas trop de temps, que ceci que cela, pour qu'on en arrive là et qu'il y ait vraiment une adoption de ces applications par les utilisateurs, il faut derrière qu'il y ait des briques d'identification, des briques d'optimisation, des briques, etc. Donc ça, c'est vraiment, ce que je pense qu'à l'heure actuelle, je pense que cela est partagé comme avis, le plus important c'est l'écosystème qui a l'air de se développer... sur tous ces sujets en même temps, en parallèle.

(entretien Adèle et Cécile, novembre 2018)

Ce passage illustre l'intérêt de recherche que j'ai vu dans le suivi de l'activité de ConsenSys. L'entreprise occupait une position centrale dans les réseaux qui étaient en train

Chapitre 2. Les modes des jetons : instituer par les smart contracts

de faire d'Ethereum un phénomène mondial avec le développement des jetons utilitaires et des ICO (en investissant et en développant des logiciels), tout en articulant des activités présentées dans les discours publics comme deux mondes bien délimités : les crypto-monnaies avec leurs relents anti-État dans le sillon de Bitcoin, et les développements novateurs de la blockchain pour toutes sortes d'activités économiques. Les éléments ci-dessus montrent que ce travail d'articulation était inscrit dans l'organisation de l'entreprise, au moment où je commençais mon enquête. Je reviendrai au Chapitre 3 sur l'évolution des activités de ConsenSys.

Les meetups : fil rouge d'enquête sur un « écosystème »

Cet écosystème, principale « puissance » d'Ethereum selon Adèle, était constitué par ConsenSys dans les meetups. Ces événements étaient annoncés sur une page du site meetup.com, administrée par ConsenSys¹⁰⁵. Toute personne inscrite sur le site pouvait s'inscrire, dans la limite des places disponibles ; quelques dizaines, jauge variable selon les lieux. Ces événements prenaient la forme de conférences ou de tables-rondes durant lesquelles s'exprimaient différents acteurs du développement d'Ethereum ou des cryptoactifs. Les thèmes abordés étaient variés ; il s'agissait notamment de discuter du développement technologique d'Ethereum, de la manière de lancer une entreprise utilisant la technologie blockchain, des formes d'organisation du travail par des moyens numériques, de nouveaux logiciels ou architectures réseaux, de l'évolution de l'adoption d'Ethereum et des cryptoactifs, de techniques de développement, ou encore de la transformation des services financiers.

Les meetups étaient des espaces physiques, constitués d'un espace réservé à des orateurs (scène sans estrade) le plus souvent équipés d'un jeu de diapositives (« slides ») diffusé sur grand écran, face auquel des spectateurs, toujours très majoritairement des hommes, étaient assis. Après les présentations et tables-rondes, un moment de discussion et de réseautages était systématiquement proposé autour de victuailles et boissons offerts par les

105 La page « *ConsenSys Paris Ethereum & Blockchain Meetup* » listait les événements passés et présents organisés ou soutenus par ConsenSys : <https://www.meetup.com/fr-FR/ConsensysParis/events/past/>

Chapitre 2. Les modes des jetons : instituer par les smart contracts

organisateur. Les orateurs (le plus souvent entre deux et quatre) se succédaient, sinon discutaient autour d'une table ; à de plus rares occasions, les deux formats étaient enchaînés. Dans ces derniers cas, le premier orateur posait les termes du problème soumis à la table-ronde. Les organisateurs du meetup décidaient des orateurs, des lieux et de leurs agencements, ainsi que des victuailles et boissons qui évoluaient au gré des thèmes retenus et des publics attendus. Au départ limités à une discussion entre personnes présentes physiquement, les meetups ont commencé à être filmés en cours d'enquête (voir par exemple en Figure 14), et parmi eux, certains ont été diffusés en ligne.



Figure 14 : Photo prise lors de l'introduction du meetup #10 (mai 2019) à ConsenSys, rue Vauvilliers, Paris 1^{er} arrondissement

J'ai suivi les meetups comme des « sites de problématisation », au sens que donne Michel Callon à cette notion (2012 : 15-16) à la suite du travail de thèse de Brice Laurent (2011) sur les nanotechnologies : des sites où les objets qui prolifèrent dans le développement des blockchains sont définis, caractérisés, où des mondes sont produits et imaginés. La notion

Chapitre 2. Les modes des jetons : instituer par les smart contracts

de problématisation souligne que les questions ou préoccupations liés à ces objets sont propres à des groupes spécifiques ; celle de site souligne le caractère temporellement et spatialement situé de la problématisation. Les objets problématisés dans les meetups étaient en premier lieu les jetons et les *smart contracts*. La notion de site de problématisation me semble utile pour souligner le caractère exploratoire de ces réunions pour les acteurs en présence. D'une part, les orateurs rassemblés par ConsenSys formulaient un problème préalablement stabilisé, dont ils débattaient éventuellement ; d'autre part, les spectateurs participaient à problématiser ces objets en intervenant publiquement ou en tête-à-tête, lors des pots.

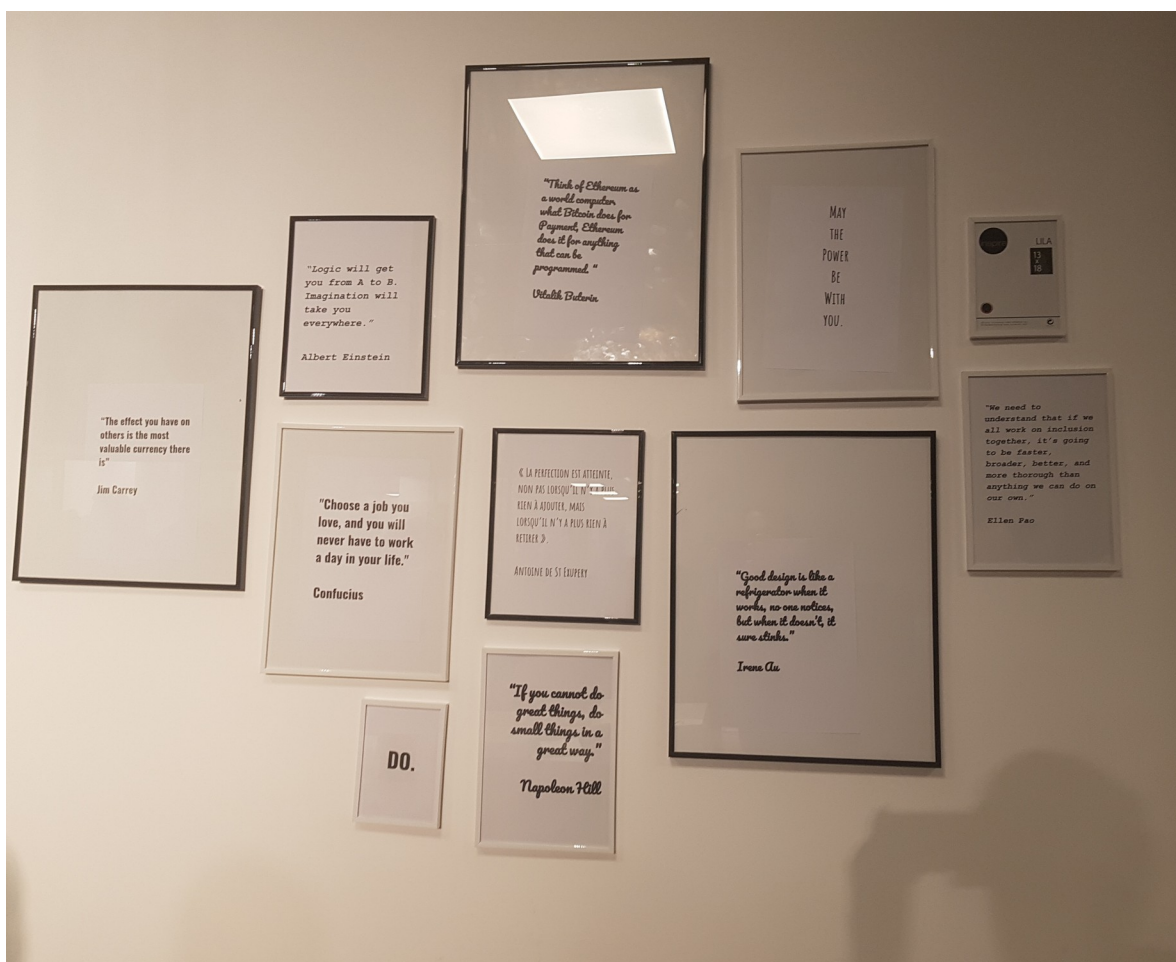


Figure 15 : Photo d'un mur des locaux de ConsenSys France couvert de citations, prise lors du meetup #10 (mai 2019)

Chapitre 2. Les modes des jetons : instituer par les smart contracts

La notion de problématisation m'a été utile pour enquêter au long cours sur des objets qui évoluaient rapidement ; souvent selon des « modes », terme employé par les acteurs et que j'ai repris dans le titre et l'introduction de ce chapitre. Au début de l'enquête, j'ai souvent eu l'impression que différents problèmes étaient entrelacés de manière originale et inattendue. Prendre les meetups de ConsenSys pour fil rouge d'enquête m'a permis d'obtenir une succession de problématizations des cryptoactifs et des *smart contracts* par une multiplicité d'acteurs réunis en écosystème que ConsenSys revendiquait de rassembler largement. Ainsi, les meetups me donnaient une vue de l'écosystème et de ses problèmes qui était empirique et située.

Mon corpus est constitué de 18 meetups que je liste en Annexe 2 selon le titre du meetup, sa date, son lieu, le format retenu et les différents orateurs. Le Tableau 7 synthétise ces meetups, chaque chiffre correspondant à un des meetups listés en Annexe 2. J'ai retenu deux axes : qui est orateur, et à qui ces orateurs entendaient parler. J'ai défini les catégories d'orateurs et de spectateurs à partir de mes observations ainsi que des descriptions écrites par ConsenSys sur le site meetup.com. « Utilisateurs de cryptoactifs » désigne des individus ou des entreprises détenant des cryptoactifs. « Entrepreneurs et startups » désigne les entreprises utilisant les cryptoactifs dans leurs activités commerciales ou leurs modèles d'affaires ainsi que les startups mobilisant la technologie blockchain plus généralement. « Développeurs et technophiles » désigne des développeurs et des personnes intéressées par les questions techniques autour d'Ethereum à titre privé ou professionnel. « Institutionnels privés » désigne des entreprises commerciales ou financières disposant de capitaux importants autres que des cryptoactifs, typiquement des entreprises du CAC40 et des institutions financières qui existaient avant l'apparition des cryptoactifs. « Régulateurs et juristes » désigne les régulateurs financiers français et européens ainsi que des juristes dont l'activité touchait aux cryptoactifs. « Gouvernements » désigne les responsables politiques élus et les représentants d'institutions publiques supranationales comme la direction générale du Trésor ou l'Union européenne, ainsi que leurs conseils.

Les entrepreneurs sont les acteurs qui s'exprimaient le plus souvent dans les meetups, et les

Chapitre 2. Les modes des jetons : instituer par les smart contracts

institutionnels privés étaient massivement attendus à partir du meetup #4¹⁰⁶. Il n'est pas question de chercher à essentialiser les positions des différents groupes, ni de limiter l'analyse à ces acteurs, d'autant plus que certains peuvent être associés à différentes catégories. Je souhaite seulement indiquer les grandes catégories d'orateurs et de spectateurs attendus par ConsenSys durant les meetups, et comment ces rencontres ont évolué dans le temps, la numérotation étant chronologique¹⁰⁷.

| Chaque chiffre correspond à un meetup (Annexe 2) | | ORATEURS INVITES | | | | | |
|--|------------------------------|------------------------------|--|----------------------------|------------------------------|-------------------------|---------------|
| | | Utilisateurs de cryptoactifs | Entrepreneurs, startups | Developpeurs, technophiles | Institutionnels privés | Régulateurs et juristes | Gouvernements |
| SPECTATEURS ATTENDUS | Utilisateurs de cryptoactifs | 9 | 8, 9 | 9 | | | |
| | Entrepreneurs, startups | 9 | 1, 4, 6, 9, 10, 16, 18 | 9 | 1, 4, 16, 18 | 1, 10 | |
| | Développeurs, Technophiles | 9 | 2, 3, 9, 10, 12, 18 | 2, 3, 9, 12 | 18 | 10 | |
| | Institutionnels privés | | 4, 5, 6, 7, 10, 11, 13, 14, 15, 16, 17, 18 | 5, 11 | 4, 5, 13, 14, 15, 16, 17, 18 | 5, 10, 11, 15, 17 | 5, 15, 17 |
| | Régulateurs et juristes | | 1, 11, 15, 17 | 11 | 1, 15, 17 | 1, 11, 15, 17 | 15, 17 |
| | Gouvernements | | 11, 15, 17 | 11 | 15, 17 | 11, 15, 17 | 15, 17 |

Tableau 7 : Correspondance entre catégories d'orateurs et de spectateurs attendus entre juin 2018 et mars 2020, selon la numérotation de l'Annexe 2

Le meetup #1 est un cas qui illustre l'intérêt de ces sites d'enquête tout en participant directement à l'argument de cette section. Ce meetup montre que la régulation des jetons utilitaires et des ICO était, en 2018, une manière de problématiser la prolifération des cryptoactifs par un large spectre d'acteurs : un membre d'une association internationale de promotion de la technologie blockchain auprès du secteur public, une représentante d'une startup proposant des solutions pour sécuriser les *wallets* de cryptoactifs, une porte-parole

¹⁰⁶ Cette numérotation fait référence à la liste récapitulant le corpus de meetups, en Annexe 2.

¹⁰⁷ En lien avec l'Annexe 2, ce tableau permet de mettre en relation des modes d'organisation des meetups avec les catégories d'orateurs ou de spectateurs : les événements organisés en matinée (meetups #11, 15) ou annoncés par emails et non sur meetup.com (meetups #15, 17) étaient principalement adressés aux institutionnels privés, régulateurs et juristes, et aux législateurs.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

d'un lobby des acteurs des marchés financiers, un représentant d'un courtier en cryptoactifs, un chercheur et consultant en droit, ainsi qu'une avocate spécialisée en droit financier. Tous ces acteurs définissaient, caractérisaient, et imaginaient des mondes avec et par les jetons en problématisant leur prolifération. L'existence, la légitimité, ou l'intérêt des jetons était supposée par ces différents acteurs. Les débats se cristallisaient plutôt sur la manière d'éliminer les incertitudes vis-à-vis du reste du monde pour faciliter leur diffusion ; autrement dit, sur la manière de favoriser leur institutionnalisation.

Problématisation des ICO : qualités du marché des jetons plutôt que l'ampleur de ses significations

Le premier meetup organisé par le bureau parisien de ConsenSys était aussi le mien. Il avait lieu quelques mois après l'explosion de la « bulle » des cryptoactifs, début 2018, alimentée par le développement des ICO. ConsenSys le co-organisait en partenariat avec la « *Government Blockchain Association* » (GBA) qui assurait l'animation de la table-ronde. L'association s'érigait en porte-parole de la « communauté blockchain » auprès des « institutions publiques » :

We trade the discussion between the institutions and the blockchain community, for them to understand the blockchain and also for them to understand that there's a lot of blockchain applications into the public sector [...]. And we also voice for the blockchain community to the public institutions because we want to, you know, push into the right direction for blockchain companies to thrive, because we really want technology to be fully adopted and just see a lot of things to be done. (animateur, meetup #1, juin 2018)

L'animateur demandait au tour de table quel était le « principal risque » que chacun associait aux ICO. Pour Mia, avocate spécialisée en droit financier, le principal risque pesait sur les investisseurs en raison de l'absence de réglementation. Elle dénonçait des excès dans le processus d'ICO, processus par lequel des individus peu scrupuleux promettaient des retours sur investissement mirobolants au travers des *whitepapers* qui n'avaient rien d'un projet entrepreneurial réel, et tout d'une « arnaque ». Elle expliquait que dans sa pratique d'avocate, elle conditionnait son accompagnement juridique aux

Chapitre 2. Les modes des jetons : instituer par les smart contracts

entrepreneurs qui lui semblait sérieux, principalement sur la base du *whitepaper* :

Basically we only take project we think are interesting and are not obviously fraudulent. So, what happens technically, we get the whitepaper, we read about what the project is about, we add all the legal disclaimers to the whitepaper and if the project is a real project then, there is no... the line is not hard to draw when the people behind the project know what they are doing. And they are doing an ICO precisely to raise for a specific project that is very well detailed including everything, for example, related to the valuation of the token, can be found in the whitepaper. They don't make crazy announcements in the whitepaper that "give us your money will quadruplate in two weeks" and I don't know what... a lot of whitepapers do that! (Mia, meetup #1, juin 2018)

Michel répondait à Mia. Il représentait CoinHouse (anciennement La Maison du Bitcoin), place d'échange en ligne (*exchange*) et en boutique (à Paris). Il partageait l'inquiétude de Mia pour les arnaques, mais il y voyait un reflet anthropologique : les arnaques étaient l'expression de la « cupidité » de certains individus. Michel voyait dans toute forme de réglementation spécifique une aventure onéreuse car bureaucratique. Il préférait fiabiliser le processus d'ICO en améliorant la procédure technique, sans intervention d'un régulateur. Autrement dit, la technologie pourrait servir d' « auto-régulation ». Michel évoquait une solution similaire à la DAO proposée par Digix : le processus d'ICO pourrait prévoir que les fonds collectés soient d'abord bloqués dans le *smart contract*, puis débloqués progressivement, au fur et à mesure des développements, de manière à donner aux « investisseurs » un rôle actif de contrôle des entrepreneurs, selon des règles de gouvernance codées directement dans le *smart contract*.

L'existence, la légitimité ou l'intérêt des ICO que je m'attendais à être des problèmes, c'est-à-dire mes problèmes, n'étaient pas ceux des orateurs au tour de table. Ces derniers problématisaient les ICO selon les incertitudes pesant sur leur « adoption », c'est-à-dire sur leur diffusion dans la société, ou encore : sur leur institutionnalisation. Pour Mia et Michel, la principale incertitude résidait dans les arnaques qui commençaient à être publicisées dans la presse généraliste. Pour Mia, les arnaques pouvaient être évitée par une forme de régulation. Pour Michel, les *smart contracts* eux-mêmes permettaient de les éviter, en donnant le contrôle aux investisseurs.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

L'autre ensemble d'incertitudes pesant sur l'institutionnalisation des jetons d'ICO relevait de la qualité de leur marché. Pour Florie, porte-parole de l'Association française des marchés financiers (AMAFI), lobby des acteurs des marchés financiers, le principal risque concernait le marché secondaire des jetons, organisé par les *exchanges* de manière « inefficace » et « non transparente » : il était très difficile pour un investisseur de savoir ce que représentaient les jetons sur ce marché. Ce problème de classification ou de qualification des jetons compromettait la possibilité d'attirer des investisseurs sur le marché primaire (émission des jetons d'ICO) et induisait des risques de sécurité et de volatilité des prix des jetons. Florie proposait de suivre de près une nouvelle agence de notation, spécialisée dans les jetons, qui aurait pu répondre à ces problèmes en proposant une forme d'auto-régulation en l'absence de positionnement des gouvernements. Pour cette ancienne de l'AMF¹⁰⁸, cette incertitude pouvait être résolue par des acteurs de leur développement. Il s'agissait pour elle d'un problème de fonctionnement de ces marchés, évalué comme les marchés financiers traditionnels ; comme pour ces derniers, une agence de notation pourrait permettre de résoudre une incertitude liée à un problème d'information.

Les régulateurs participaient à réduire l'incertitude sur les jetons à celle des qualités de leur marché. Aline était porte-parole de l'Autorité Européenne des Marchés Financiers (ESMA)¹⁰⁹. Le caractère non-régulé des *exchanges* conduisait pour elle à des « manipulations de marché », un problème qui s'ajoutait à celui de la diversité des jetons aussi bien pour les investisseurs que pour les régulateurs qui découvraient des « objets nouveaux ». Nadine était lobbyiste pour Ledger¹¹⁰, une startup française devenue « licorne » en 2021. Cette « *Head of Government Affairs and Central Banks* » était une ancienne jeune cadre de la Société Générale et investisseuse aux Émirats Arabes Unis. Nadine expliquait discuter régulièrement avec les gouvernements et les autorités de régulation à Paris et à Bruxelles. Elle confiait à l'assemblée que ses interlocuteurs ne « souhaitaient pas arrêter

108 L'AMF se définit comme « une autorité publique indépendante qui a pour mission de veiller à la protection de l'épargne investie en produits financiers, à l'information des investisseurs et au bon fonctionnement des marchés ».

109 L'European Securities and Markets Authority (ESMA) est une autorité de surveillance européenne indépendante installée à Paris.

110 Ledger était une start-up française qui concevait et commercialisait des portefeuilles matériels de cryptoactifs (*wallets*) destinés aux particuliers et aux entreprises.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

l'innovation », c'est-à-dire ne pas faire peser de contrainte légale ou réglementaire sur ces objets, mais craignaient que les ICO conduisent à des pratiques de blanchiment d'argent.

L'intervention des autorités publiques *via* une quelconque forme de régulation ne semblait pas être un problème pour les orateurs, qui ne semblaient pas l'envisager, sinon pour améliorer la qualité du marché des jetons. Elle représentait en revanche une incertitude qui inquiétait différents spectateurs présents dans la salle. Certains prirent la parole, en fin de table-ronde, pour interroger la pertinence de lancer une ICO en France. Ils pointaient une incertitude réglementaire française, qu'ils envisageaient comme possiblement restrictive face à la position du régulateur suisse, réputée au contraire *pro-business*. Mia prit plusieurs fois la parole pour insister sur la réglementation française en cours d'élaboration : selon elle, les entrepreneurs pouvaient s'attendre à une régulation française au moins aussi favorable pour les entrepreneurs que celle du régulateur suisse.

Ce meetup montre qu'un large ensemble de protagonistes problématise le développement des jetons, et participent à les instituer, comme des objets financiers. La sous-section suivante montre que ce type de problématisation confie aux concepteurs le monopole de leurs autres significations.

2.3. Incertitudes et significations : jetons utilitaires et security tokens

Cette sous-section se concentre sur le développement d'un type de jetons alternatif aux utilitaires et d'ICO : les « *security tokens* »¹¹¹. Ces jetons problématisaient les marchés financiers : ils étaient conçus comme des titres financiers. Mais cette problématisation en cachait une autre : elle répondait à une incertitude réglementaire pesant sur le développement des jetons utilitaires et d'ICO (sont-ils juridiquement des titres financiers ?). Les autorités de réglementation des marchés financiers distinguaient jetons utilitaires et

111 Je conserve la terminologie en langue anglaise « *security tokens* » pour ne pas introduire de distorsion analytique ; je présente des débats sur cette notion dans ce qui suit.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

security tokens comme leurs concepteurs ; les premiers voyaient les significations que les seconds imaginaient dans la conception de ces jetons, « eux-mêmes ». Je conclus cette sous-section en suivant le parcours de développement des *security tokens* via un produit que ConsenSys essayait de vendre à des institutions financières, c'est-à-dire à les mettre en position de conceptrices de jetons.

Problématisation de la finance institutionnelle

Le Tripot Régnier, Paris 15^{ème} arrondissement, un soir de décembre 2018

*Bonjour à tous. Merci d'être venus. Je m'appelle [Kean] et je suis responsable de ConsenSys en France. On est très heureux de vous accueillir en cette fin d'année pour **parler de tokenization en actifs financiers. Un sujet loin du passé sulfureux des cryptomonnaies ; quartier respectable, sujet respectable.** Donc l'idée c'est vraiment de parler de la transcription entre la technologie, technique, entre la blockchain, technologie de base de données décentralisée, et ses **applications aux actifs financiers pour les rendre plus faciles à émettre, et pour rendre liquides des marchés** qui jusqu'à présent étaient illiquides (Kean, meetup #5, décembre 2018)*

Ces mots du directeur de ConsenSys en France ouvrait le meetup #5, intitulé « Conférence : Blockchain & Numérisation des actifs » en décembre 2018. Kean annonçait que Michel Aglietta, qu'il présenta comme un « professeur émérite à l'université de Nanterre », allait introduire l'événement. Pour Kean, « recevoir Michel » sur la même scène qu'un porte-parole de la Société Générale signifiait « [une ouverture] à différents écosystèmes, à l'écosystème des économistes, à celui des banques également ». La première table-ronde proposait un « tour d'horizon » du « paysage mondial » et du « paysage réglementaire », la seconde devait avoir une « vocation beaucoup plus pratique », se pencher sur « la perspective des investisseurs, et la perspective des émetteurs », la réponse de « la blockchain » à « leurs besoins » et la manière de « lancer une opération », « concrètement ».

La finance de marchés institutionnelle était à l'honneur. Le buffet n'était cette fois pas constitué de pizzas et de bières, habitude des meetups où étaient attendus entrepreneurs et

Chapitre 2. Les modes des jetons : instituer par les smart contracts

développeurs, mais de petits fours et de champagne. Mais le ton était annoncé dès les premiers mots de Kean et l'introduction de Michel Aglietta, qui se présenta comme « quelqu'un d'extérieur ». Le professeur expliqua avoir été sollicité « par l'intermédiaire de l'Institut Louis Bachelier [pour] dire à quel point la finance était dangereuse ». Rires nerveux ou amusés dans la salle. Dans une présentation intitulée « les fintechs à l'épreuve de la fragilité de la finance de marché », Michel Aglietta décrivait les cycles financiers de différents pays pour montrer le lien entre libéralisation des marchés financiers et instabilité économique. Au bout d'une dizaine de minutes, une musique d'ambiance commença à se superposer à la voix de Michel Aglietta. Au départ impassible, jetant un coup d'œil aux organisateurs, il continua sa présentation. Puis la musique pris de plus en plus d'espace sonore, accompagnée par une rumeur venant d'une salle qui commençait à discuter. Le professeur s'étonna que son auditoire ne se sente pas aussi concerné qu'il le devrait, et pris quelques minutes pour terminer son exposé tandis que de nombreuses personnes présentes continuaient d'échanger des regards et des mots de manière entendue. Aucun doute, la finance ne semblait pas effrayante à une très large part de l'auditoire du professeur.

Ce meetup visait à faire exister un nouveau type de jeton appelé « *security tokens* » (ST) selon des perspectives réglementaires, financières, commerciales et techniques. À la différence du meetup #1 qui problématisait le développement des ICO, ce meetup problématisait les marchés financiers institutionnels. Alors que les ICO et les jetons utilitaires existaient depuis des années déjà en juin 2018, les ST étaient une forme tout juste émergente et explicitement destinée à des institutions financières. Pour ses organisateurs, l'objectif du meetup était d'enrôler ces institutions financières, leur montrer le potentiel des *security tokens*, et de marquer une différence avec un « passé sulfureux » (mots de Kean) auquel appartenaient les ICO et les jetons utilitaires.

En problématisant la finance institutionnelle, les dix orateurs du meetup tentaient d'éliminer les incertitudes percevaient les professionnels de la finance dans les jetons, *a priori* frileux face à une technologie qui héritait directement de Bitcoin.

Voici quelques exemples de problématisations de la finance institutionnelle évoquée durant

Chapitre 2. Les modes des jetons : instituer par les smart contracts

ce meetup. Pour Maurice, représentant d'une association d'entrepreneurs suisses, les ST permettaient de créer de « nouvelles façons de raisonner financier » en constituant des portefeuilles d'actifs auxquels des publics n'ont aujourd'hui pas accès. Il donnait l'exemple de biens immobiliers qu'il serait possible de rendre « liquides » en les représentant par des ST. Pour Arnold, avocat spécialisé en droit des affaires et du numérique, les ST permettaient d'améliorer les délais de règlement-livraison lors de transactions impliquant des titres d'entreprises (actions), passant de plusieurs jours à quelques secondes ; en conséquence, les droits de vote en assemblées générales d'actionnaires pourraient être redistribués quelques minutes avant leurs tenues. Les ST pourraient par ailleurs améliorer la vision de gestionnaires de fonds sur leur passif comptable, c'est-à-dire connaître les identités ou des catégories de porteurs des actifs qu'ils ont en gestion, de manière à éviter les « phénomènes de double imposition » qui seraient aujourd'hui conséquents de ces points aveugles. Maxence, avocat spécialisé en gestion d'actifs (« *asset management* »), voyait dans les ST des moyens de « créer un lien direct entre la société de gestion [d'actifs] et les investisseurs ». Il voyait également un moyen de transformer le marché secondaire de capital-investissement (« *private equity* »), organisé aujourd'hui de gré-à-gré, « chronophage et coûteux », car la blockchain permettrait de « capitaliser sur l'effet réseau qu'elle crée, et créer une communauté d'investisseurs-vendeurs et d'investisseurs-acheteurs qui va obéir à des standards prédéfinis et ce qui va permettre de fluidifier ces transactions et de les faciliter ». Sylvain, cofondateur d'« un projet qui était développé au sein de ConsenSys »¹¹², et président de la ChainTech¹¹³, voyait les ST comme des améliorations de la transparence et du contrôle des régulateurs, étant donné que le registre était numérique, et symétriquement, d'améliorer l'« efficacité de reporting et d'informations [des entreprises régulées] auprès des autorités réglementaires ».

112 Il s'agissait de ce qu'Adèle et Cécile appelaient un « projet interne » à ConsenSys, dans le premier pôle. Ce projet, appelé VariabL, visait à construire une « plateforme sécurisée de négociation de produits dérivés basée sur Ethereum ».

113 La ChainTech se définissait comme l'« association des professionnels de la blockchain et des cryptoactifs en France ». Depuis, cette association a été remplacée par l'« Association pour le Développement des Actifs Numériques » (ADAN), qui se dit « rassemble[r] les professionnels des cryptoactifs et des technologies blockchain en France et en Europe ».

D'une incertitude réglementaire à une innovation technologique

La promotion des ST participait à réduire l'incertitude réglementaire pesant sur l'institutionnalisation des jetons utilitaires. Cette incertitude était liée aux différences que prenait la notion de « *security* », ou de « titre financier », dans différentes juridictions. En particulier, les entrepreneurs qui se finançaient par ICO craignaient que leurs jetons soient qualifiés de « *security* » par le régulateur étatsunien, la SEC¹¹⁴, car cette qualification engendrait des obligations particulières et contraignantes. En associant la notion d'investissement à celle de ST, les concepteurs de jetons, typiquement entrepreneurs ou développeurs, prenaient la main sur cette qualification et la distinguaient des émissions de jetons utilitaires et des ICO.

La citation qui suit est longue mais intéressante pour observer le subtil renversement que je souhaite documenter dans ces paragraphes : promouvoir un nouveau type de jetons, les ST, pour résoudre une incertitude portant sur un type de jetons existant, les jetons utilitaires ou ICO.

Je l'ai divisée en trois paragraphes par souci de lisibilité et pour l'analyse qui suit, mais Sylvain a énoncé l'ensemble sans s'arrêter, en réponse à Kean qui lui donnait la parole pour définir ce qu'étaient les ST :

*(1) « Alors on va faire une tentative de définition du security token, puisque c'est encore un objet difficile à appréhender. Donc je vais commencer par un peu une évidence. **Security token c'est un token qui est une security, à l'opposé de l'utility token qui est plutôt une forme d'utilitaire.** Je vais passer là-dessus parce que... auguste assemblée, de ré-expliquer en détails ce qu'est un token. **Tout le monde sait à peu près ce qu'est un actif digitalisé sur blockchain.** Donc l'aspect token je vais laisser de côté, pour m'intéresser donc plutôt à l'aspect security, qui est ce qui distingue les autres types d'actifs numériques.*

*(2) Et là, ça devient tout de suite plus compliqué parce que **security c'est un terme qui a des définitions différentes selon le pays** dans lequel on se trouve, et qui,*

¹¹⁴ La U.S. Securities and Exchange Commission, communément appelée la Securities and Exchange Commission ou « SEC », est l'organisme fédéral américain de réglementation et de contrôle des marchés financiers. Il s'agit du « gendarme de la Bourse » américain. Ses fonctions sont généralement similaires à celles de l'Autorité des marchés financiers (AMF) en France.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

*comme son nom l'indique « security », dans la blockchain a un peu une origine anglo-saxonne et plus précisément aux États-Unis. C'est là que les premières réflexions sur le terme security token ont commencé à émerger et où on a eu pendant un moment **les deux dernières années beaucoup de réflexions dans la communauté blockchain en général sur « est-ce que mon token est une security ? », avec une obsession qui était de ne pas être une security. Alors pourquoi on cherche à ne pas être une security ?... Parce qu'une security en droit américain c'est, en grossissant un peu le trait, un investissement, un investissement financier, et les investissements financiers sont régulés par une autorité particulière qui est la SEC et qui a mis en place un certain nombre de règles précises sur la vente au public de securities, d'actifs financiers, et ces règles sont relativement lourdes et difficiles à remplir. Et, la crainte des acteurs blockchain qui mettaient en vente des actifs c'était d'être qualifiés de security pour se retrouver dans le cadre défini de la vente de securities aux États-Unis.***

(3) Donc security en fait ça veut simplement dire investissement. Et donc, le security token, c'est finalement un token qui représente pour l'acheteur, sur le marché primaire ou le marché secondaire, une forme d'investissement, d'une façon ou d'une autre, et donc avec un espoir de gain qui est intrinsèque au token. Donc techniquement le token comme security est identique aux autres tokens. C'est-à-dire il n'y a pas de différence formelle quand vous possédez un token qui soit security ou autre chose, c'est la même forme d'inscription sur la blockchain, technique. Mais ses caractéristiques, vont le rapprocher d'un actif d'investissement, donc d'un titre financier. (Sylvain, meetup #5, décembre 2018)

Sylvain expliquait en (1) que les ST « s'opposaient » aux jetons utilitaires, et que les définitions du monde commun (« utilitaire » ou objet qui donne accès à un service, « security » ou titre financier) définissaient naturellement les jetons en fonction de la catégorie que leur donnaient les concepteurs (jeton utilitaire, ST). Puis, Sylvain indiquait en (2) que le développement des jetons utilitaires et des ICO était incertain en raison de la réglementation étatsunienne ; à cette époque, les ST n'existaient pas. En (3), Sylvain expliquait que le ST était un jeton qui signifiait « investissement » ou « security » dans le droit américain. Ces jetons étaient « identiques » aux autres, ils avaient « la même forme technique », seule leur signification changeait aux travers de « caractéristiques » qui les distinguaient.

Regarder les relations comme un concepteur de jetons

Le raisonnement de Sylvain suppose de donner aux jetons les significations qu'ont

Chapitre 2. Les modes des jetons : instituer par les smart contracts

imaginées leurs concepteurs. Ce regard sur les jetons était partagé par les représentants des administrations publiques. La tirade de Sylvain a fait réagir Aline, représentante de l'ESMA rencontrée au meetup #1 (sous-section 2.2). Elle abondait en son sens. Pour elle, il était « artificiel » de chercher à superposer des « définitions fonctionnelles » (jeton utilitaire, ST) à des définitions réglementaires, car les jetons pouvaient tomber dans « plusieurs cases » réglementaires et les fonctionnalités pouvaient « évoluer dans le temps ». Elle prônait une réglementation fondée sur une analyse « au cas par cas des *business models* » des startups émettrices. C'était également par cette métaphore des « cases » que Germain, « chef du bureau épargne et marchés financiers à la direction générale du Trésor¹¹⁵ », justifiait l'esprit qui animait les régulateurs français et l'approche retenue pour la législation sur les jetons qui allait arriver quelques mois plus tard en France avec la loi PACTE.

Les efforts des orateurs n'ont pas convaincu différents auditeurs autour de moi. À leurs échanges de regards et sourires en coin, je comprenais qu'ils partageaient mon étonnement : comment pouvait-on sérieusement considérer que les jetons utilisés pour les ICO n'étaient pas des investissements ? Les cas de Bluzelle et de Digix montraient que les jetons utilitaires, qu'ils soient conçus au futur comme usage (Bluzelle) ou gouvernance dans une DAO (Digix), signifiaient bien financement pour les entrepreneurs et investissements pour les acheteurs des jetons, au présent. Un spectateur qui s'est présenté comme « un entrepreneur » a pris la parole à la fin de la table-ronde avec Sylvain, Aline et Germain pour poser une question qui brûlait de nombreuses lèvres :

*Alors j'ai une question volontairement anachronique et un peu opposée. **Comment pouvons-nous encore croire aujourd'hui qu'un utility token n'est pas un security token ?** Je précise ma question, enfin je peux démontrer tout à fait mon propos [d'autres spectateurs s'esclaffent] ce n'est pas une question totalement naïve. Très rapidement, **la technologie est identique**, dans les deux cas. **L'espérance de gain, aussi bien pour l'émetteur que pour l'investisseur, est identique.** Et enfin, le token, utility, même si on va dire qu'il est corrélé à un*

115 La direction générale du Trésor (DG Trésor) est une direction de l'administration publique française, rattachée au ministère de l'Économie et des Finances et au ministère des Affaires étrangères. La DG Trésor est chargée de l'analyse économique et du conseil du Gouvernement dans l'élaboration et la conduite de la politique économique, commerciale et financière et réalise des prévisions et des évaluations économiques des politiques publiques.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

*service, il est quand même corrélé à un actif [...] donc **pour moi je ne vois pas trop comment on peut encore maintenir la typologie de utility token.*** (spectateur anonyme du meetup #5, décembre 2018)

Cette question a entraîné un moment de cafouillage parmi les orateurs. Aucun d'entre eux ne semblait à l'aise pour répondre. J'ai compris la rumeur qui montait alors dans la salle comme un mélange de malaise et d'approbation d'autres spectateurs du meetup. Jean, « *Tech Lead* » chez ConsenSys et président de la première association d'utilisateurs d'Ethereum en France appelée alors Asseth¹¹⁶, tentait en premier de répondre à la question. Il expliquait que la valeur des jetons utilitaires était « personnelle », qu'elle n'était « pas financière ». Peu convaincu, le directeur de ConsenSys France, Kean, passa la parole à Doriane, représentante de l'AMF (équivalente de la SEC en France) et selon lui « la plus compétente » :

*Alors oui nous [à l'AMF] on est assez fermement convaincus, même carrément convaincus, qu'il y a une frontière qui existe entre les deux [jetons utilitaires et ST]. Pour illustrer le propos, on a rencontré au cours de l'année passée près de 80 projets d'ICO. Et nous on considère que sur les 80 projets qu'on a rencontrés il y en a moins de 5 % qui rentrent aujourd'hui dans la catégorie juridique de l'instrument financier. Donc je ne vais pas revenir dessus, mais instrument financier c'est soit un titre financier, une action, une obligation, ou une part de fonds. Soit un contrat financier, et si on ne tombe pas dans cette catégorie-là, on n'est pas considéré en droit français comme étant un instrument financier. Donc en ce qui nous concerne, on considère que la plupart des projets aujourd'hui ne sont pas dans cette catégorie. Par exemple, je ne sais pas, un projet qu'on a rencontré... connecter par exemple, à des objets connectés, permet dans le jeton, donnera accès au service que va développer la société, et dans ce jeton vous pourrez logger les données personnelles qui sont liées à vos objets connectés. Ces données personnelles ensuite vous pourrez les échanger sur un marché secondaire qui sera organisé par la plateforme. **Je ne vois pas bien en fait, où est-ce qu'est la relation avec un instrument financier.** Je trouve qu'on est sur autre chose, ce n'est pas de l'instrument financier. Alors **il y a peut-être une notion de valorisation, de valeur derrière, mais elle n'est pas liée à une société.** C'est ça un instrument financier quand même, c'est qu'on ait soit une créance, soit on représente une part sociale d'une société, mais là, je trouve que ce sont des concepts nouveaux. Donc **il ne faut pas à mon sens essayer de déformer les catégories existantes pour essayer de faire rentrer quelque chose qui justement ne ressemble pas.** (Doriane, meetup #5, décembre 2018)*

¹¹⁶ Depuis, l'association Asseth est devenue « Ethereum France ». Je reviendrai sur cette association au Chapitre 3.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Pour l'AMF représentée par Doriane, la signification des jetons devait être appréciée en fonction de la qualité juridique de son émetteur. Ainsi, si le jeton ne représentait pas explicitement une créance ou une part sociale d'une société, il ne s'agissait pas d'un investissement. Les « rencontres » de 80 projets d'ICO en question étaient les réponses du secteur des cryptoactifs à la consultation publique lancée par l'AMF entre fin 2017 et début 2018 qui a servi à l'élaboration du versant « crypto » de la loi PACTE. Cette consultation concluait qu'il n'était pas possible d'apporter une « réponse unique au sujet de la qualification des jetons émis (tokens) à l'occasion des ICO compte tenu de leur diversité » (AMF 2018). Cette conclusion, comme la position de Doriane qui jugeait important de ne pas « faire rentrer quelque chose qui justement ne ressemble pas » dans les catégories existantes du droit, donnait toute latitude à l'imagination des entrepreneurs qui ne risquaient pas d'être contraints à des « cases », selon l'expression d'Aline et de Germain.

Ces éléments témoignent de la proximité de positions entre les représentants de ConsenSys et d'administrations publiques, proximité qui était affichée. Doriane avait commencé son intervention en soulignant l'« alignement » de points de vue entre les participants, soulignant un « petit *challenge* qui est en effet de faire un peu de créativité, de ne pas répéter tout ce qui a été dit dans la table-ronde précédente, ce qui va être un peu compliqué, parce qu'heureusement nous sommes tous alignés et tous d'accord », avant de se réjouir que la France soit « pionnière » en matière de blockchain et de cryptoactifs. Symétriquement, Sylvain, qui dirigeait le principal lobby des cryptoactifs en France, évoquait des discussions régulières avec les régulateurs français pour « traiter » les questions qui freinent le développement des ST. Germain profitait de son intervention pour faire « une page de publicité » pour l'ordonnance blockchain prise en décembre 2017 qui autorisait à émettre des titres financiers par une blockchain. Il se montra rassurant quant à l'imminence de la parution de décrets très attendus qui traduiraient bientôt cette ordonnance en droit, et indiqua que pourront suivre des « effets puissants qui ont été décrits de potentiels gains de temps, de potentiels économies de certains intermédiaires, cela veut dire aussi des économies financières ». Il vantait « les possibilités ouvertes par l'univers crypto » comme opportunités d'apprentissage pour « le monde financier ».

Chapitre 2. Les modes des jetons : instituer par les smart contracts

Par ailleurs, ce meetup illustre la densité des réseaux interpersonnels constituant « l'écosystème », au-delà des appartenances institutionnelles ou organisationnelles. Sylvain était à la fois porte-parole des entreprises blockchain et de cryptoactifs et employé de ConsenSys. Florie, rencontrée au meetup de juin 2018 comme porte-parole de l'AMAFI (représentant les acteurs des marchés financiers) s'exprimait en décembre 2018 comme chargée d' « affaires réglementaires et projets dans les institutions financières avec des clients bancaires » chez ConsenSys, le deuxième pôle ou activités de conseil et lobbying selon la distinction vue plus haut, chez ConsenSys. Avant l'AMAFI, Florie travaillait pour l'AMF. Puis, après avoir quitté ConsenSys, Florie a rejoint l'ADAN en 2020, successeur de la ChainTech et association que dirigeait Sylvain comme responsable des relations institutionnelles. Ensuite, Florie a été élue présidente de l'ADAN tout en étant *Chief Operating Officer*. Jean était à la fois président de l'Asseth, principale association d'utilisateurs d'Ethereum en France et employé chez ConsenSys. Aline, présente au meetup de juin 2018, était de nouveau conviée au tour de table de décembre 2018. Maxence aura lui été orateur à trois événements sur la période d'observation.

La complexité des relations « intégrée » dans les jetons

Ces prises de positions convergeaient pour reconnaître aux relations les significations de leurs concepteurs. Elles déléguaient à ces derniers le soin de les définir, dans la conception technologique et entrepreneuriale. Ce faisant, elles faisaient de la programmation un langage naturel de formulation des relations par une infrastructure. Cette dernière n'était jamais problématisée, et très rarement évoquée. Durant les deux heures de conférence, le mot « Ethereum » est apparu six fois, soit aux côtés de « Bitcoin » pour opposer « cryptomonnaies » (« passé sulfureux ») aux ST (« sujet respectable »), sinon pour décrire les activités de l'association Asseth représentée par Jean. Cette évidence de relations formulées avec les *smart contracts* apparaissait par exemple dans l'expression de Sylvain ci-dessus : « il n'y a pas de différence formelle quand vous possédez un *token* qui soit *security* ou autre chose, c'est la même forme d'inscription sur la blockchain, technique ».

Jean associait évidence des significations de relations par la programmation avec les

Chapitre 2. Les modes des jetons : instituer par les smart contracts

standards ERC (présentés à la sous-section 2.1). Jean liait le succès des ICO à la facilité d'utilisation du standard ERC-20 comme Joseph Lubin, et indiquait que la standardisation permettait plus généralement d'inscrire des relations d'un type spécifique. En l'occurrence, en matière de titres financiers, la standardisation permettait un « contrôle de l'émetteur » sur les jetons. Ce type de relations spécifiques à la finance institutionnelle était déjà formalisé dans deux nouveaux standards, l'ERC-777 et l'ERC-1400.

Donc ce qu'on a vu par le passé, avec les ICO, donc les gens qui ont émis des jetons qui sont parfois vus comme des utility, parfois comme des security, bon, tout ça parce qu'on avait un standard qui s'appelait le standard ERC-20, et qui était très facile à utiliser. Maintenant, ce standard il est très frustré, il fait des choses très très bien, mais il les fait de façon complètement déréglementée. [...] Maintenant si on veut faire des security tokens, il est nécessaire d'avoir un contrôle de l'émetteur, [...] s'assurer que le mode qu'on utilise pour faire tout ça est bien audité. Donc un des avantages de la communauté Ethereum c'est que c'est une bonne machine à émettre des standards. Donc on a deux standards qui sont actuellement les principaux à être travaillés en open source, qui sont l'ERC-1400 et l'ERC-777. Des termes techniques, si vous cherchez ces termes sur Google, vous tombez sur des discussions avec des gens qui disent « il faut faire ça il faut faire ça il faut faire ça, ah oui, mais il faut qu'on ait des trucs par tranches, comment on le représentera ?... » et ça déjà, pour rebondir sur ce que disait mon collègue à droite, Jean-Marie, l'ingénierie financière, la créativité financière, j'attends avec impatience de voir comment elle va se saisir de ce sujet et comment elle va s'impliquer là-dedans en disant : « on a du code, on sait faire des choses très intéressantes pour les structurations, traduisons les dans le code pour faire des trucs sympas avec ça ». Maintenant avoir son standard qui fait les choses bien, c'est un travail de fond, c'est là que des experts en sécurité, des experts en blockchain, travaillent pour faire des choses intéressantes, qui ensuite sont regardées par d'autres personnes à côté qui ont plutôt des backgrounds juridiques. (Jean, meetup #5, décembre 2018)

Cette programmabilité était garantie par Ethereum et sa communauté, une « bonne machine à émettre des standards ». Cette machine était à la disposition de l'imagination, notamment financière. Dans cet extrait, Jean invitait Jean-Marie, qui travaillait à la « cellule blockchain » de la Société Générale, à exercer « l'ingénierie » et la « créativité financière » que le même Jean-Marie voyait dans les banques françaises quelques instants plus tôt.

La programmabilité de relations standards par les ERC permettait, selon les orateurs, de traduire les catégories du monde directement dans un type particulier de jeton, que ces

Chapitre 2. Les modes des jetons : instituer par les smart contracts

catégories soient réglementaires ou issues de pratiques de l'industrie financière. Ces différentes « complexités » pouvaient être « intégrées » directement dans les jetons pour fluidifier les transactions financières :

*Et enfin dernier avantage qui me semble important, c'est aussi la capacité par la blockchain de coder et d'**intégrer dans la technologie et dans le titre lui-même, certaines contraintes qui vont des contraintes pratiques aux contraintes réglementaires**, on peut citer par exemple des contraintes de diversification, des contraintes liées aux ratios d'emprise, et ça, ça peut être intégré dans la blockchain, automatiser le respect de cette contrainte, et du coup diminuer les coûts du respect de ces contraintes.* (Maxence, meetup #5, décembre 2018)

Ainsi abondait la représentante d'une association professionnelle d'institutions financières, les jetons pouvaient garantir à eux seuls la conformité des relations comprises au sens de transactions financières, sous réserve que les données « en dehors de la [block]chaîne » nécessaires au calcul soient correctement connectées.

*Effectivement là on a des **standards** qui se développent avec des jetons, qui permettent en fait de **prendre en compte l'ensemble des restrictions pour la bonne conformité du projet de STO**¹¹⁷. Qui permettent outre ça **la possibilité d'aller chercher de l'information en dehors de la chaîne**, qui est nécessaire, pour l'exécution des transactions des security tokens. Ou également la possibilité de faire du **tranching**, afin d'affecter, pour un émetteur qui émet des titres, des droits différents associés à différents types d'actionnaires.* (Florie, meetup #5, décembre 2018)

Ces différents orateurs partageaient une perspective commune : les institutions financières pouvaient devenir conceptrices sur Ethereum en tant que formulatrices de leurs relations qui pourraient y être inscrites de manière sécurisée, au sens décrit au chapitre précédent. Cette activité de formulation leur conférait le monopole sur la formulation de leurs relations, sous le regard des autorités publiques. Symétriquement, les jetons utilitaires et les ICO étaient émancipés de la qualification d'instruments financiers, dangereuse pour leurs concepteurs.

117 « Security Token Offering », ou émission de *security token*, notion bâtie en analogie avec ICO.

Parcours de conception : les security tokens et les émetteurs de titres faits concepteurs de jetons

Les institutions financières étaient elles-mêmes faites « conceptrices » de jetons avec le développement des *security tokens*. Comme pour les concepteurs de jetons utilitaires et d'ICO auxquels étaient délégué le monopole de la définition des significations des jetons qu'ils créaient, les institutions financières étaient invitées à exercer leur imagination financière et à gouverner les relations comme titres financiers. Les paragraphes qui suivent montrent que ConsenSys enrôlait des entreprises émettrices de titres financiers avec un logiciel de sa conception qui les plaçait en situation de contrôle de leurs titres, seules ou en collaboration avec d'autres entreprises de la finance de marché.

Après avoir organisé une conférence en décembre présentant la régulation et les avantages de la numérisation des actifs financiers, l'idée est cette fois-ci de réunir plusieurs entrepreneurs et investisseurs afin de présenter un deep-dive technologique et opérationnel. C'est également l'occasion pour nous de partager une démo de notre solution pour les security tokens: The Dauriel Network. (ConsenSys 2019a)

Ces lignes étaient publiées sur meetup.com en janvier 2019. Elles annonçaient le meetup #6 organisé par ConsenSys en ses murs du 1^{er} arrondissement de Paris, intitulé « *The Dauriel Network: Nouvelle solution Ethereum pour les Security Token* ». Après avoir présenté « la régulation et les avantages de la numérisation des actifs financiers » durant le meetup #5, ConsenSys accueillait des cadres d'entreprises et d'institutions financières, et plus généralement les habitués de ses meetups. Kean présentait les *security tokens* ou « tokenization des actifs financiers » comme une « nouvelle tendance ». Les orateurs étaient exclusivement des représentants de ConsenSys, désormais en explicite démonstration commerciale.

L'ambition de ConsenSys était de construire une infrastructure de marché mondial alternative dans laquelle les entreprises manipulant des titres financiers (entreprises émettrices et institutions financières) seraient en « contrôle » de la circulation de leurs actifs. Le meetup visait à expliquer le fonctionnement imaginé de cette infrastructure

Chapitre 2. Les modes des jetons : instituer par les smart contracts

imaginée par le prototype d'un ensemble de logiciel, une « plateforme d'outils » baptisée *The Dauriel Network* (TDN).

ConsenSys s'adressaient aux entreprises émettrices de titres (comme des actions ou des parts de fonds)¹¹⁸. TDN était conçu comme dispositif de rencontre entre les émetteurs de titres et leurs investisseurs. Norman, responsable du produit TDN chez ConsenSys, jonglait entre deux interfaces de TDN durant la démonstration, situant les auditeurs dans la peau de l'émetteur et de l'investisseur successivement. L'émetteur devait commencer par définir le nom du titre, le symbole choisi (typiquement un trigramme, comme pour les jetons utilitaires), et les « *campaign requirements* ». Ces derniers spécifiaient quelles étaient les informations qui seraient demandées aux investisseurs dans le cadre de la procédure « *Know Your Customer* » (KYC), permettant ainsi d'effectuer des « contrôles beaucoup plus poussés » qu'avec d'autres types de jetons. Cette procédure incluse notamment les informations imposées par la réglementation en matière de lutte contre le blanchiment d'argent et de financement du terrorisme (dite « LCB-FT »). Ensuite, l'émetteur pouvait créer le titre. L'investisseur devait passer par des étapes. D'abord, il s'enregistrait, en renseignant la procédure KYC paramétrée par l'émetteur, et déposait les fonds correspondant aux titres qu'il souhaitait acquérir. Une fois la procédure KYC validée par l'émetteur, il recevait un courriel de la plateforme, indiquant qu'il pouvait acquérir les titres financiers, ce qui générerait une proposition de signature du titre financier.

Le contrôle des émettrices de titres financiers était inscrit dans le standard ERC-1400, qui ajoutait une propriété à d'autres héritées¹¹⁹ de standards plus anciens. L'ERC-20, utilisé pour les ICO et les jetons utilitaires, permettait seulement de spécifier le montant et le destinataire ; il ne permettait pas de contrôler à qui et à quelles conditions le jeton pouvait être transféré. L'ERC-777 était construit à partir de l'ERC-20, et lui ajoutait un troisième paramètre, un « champ *data* ». L'ERC-1400 était construit comme une « surcouche » de l'ERC-777 : il lui ajoutait la possibilité de « partitionner » les jetons, donnant à des sous-

118 Kean indiquait que faire de TDN un outil d'institution de marchés secondaires, c'est-à-dire l'achat et la vente de titres financiers déjà émis, demandait encore du travail.

119 J'emploie « héritage » en référence à la notion en informatique : en programmation (orientée objet), l'héritage consiste à inclure, dans une nouvelle classe d'objets (ici l'ERC-1400), les caractéristiques de classes d'objets préalablement déclarées (ici l'ERC-20 et l'ERC-777).

Chapitre 2. Les modes des jetons : instituer par les smart contracts

ensembles d'un même jeton (représentant le titre de la même entreprise) des caractéristiques spécifiques. Les jetons de chaque partition devenaient non fongibles entre eux. Cette fonctionnalité devait répondre à la possibilité, pour les entreprises émettrices, de réaliser différentes « opérations sur titres » (comme le paiement des dividendes, fusions et acquisitions, *call*). Le « champ *data* » était utilisé pour « injecter » un « certificat » de l'émetteur de titres au moment de la signature de la transaction. Ce certificat, nécessaire à l'inscription de la transaction sur Ethereum, était communiqué à l'investisseur une fois que la procédure KYC avait été validée par l'émetteur et que les fonds avaient bien été reçus sur son compte bancaire. Le certificat était l'élément central du contrôle de l'émetteur ; il était signé avec sa clé privée, et expirait dans le temps. Une fois la transaction ajoutée par l'investisseur (en pratique, par l'interface de TDN côté investisseur), le statut des jetons réservés par l'investisseur passaient de « réservés » à « émis » sur l'interface, signifiant que la transaction avait été inscrite sur Ethereum.

L'objectif premier de ConsenSys était de faire de TDN « une plateforme » d'émission d'actifs constituant des réseaux d'entreprises et d'institutions financières, plutôt qu'un outil destiné à des « *Security Tokens Offerings* » (STO) ponctuelles. Cet objectif avait une dimension commerciale, sur laquelle je reviendrai longuement au prochain chapitre. Avec TDN, il était plus intéressant pour ConsenSys de développer un système étendu qui, par son utilisation, était susceptible de devenir un nouveau standard du marché des solutions logicielles d'infrastructures de marchés financiers. Lors de sa présentation et de la séance de questions-réponses, Kean a indiqué à plusieurs reprises que « de grands noms » s'intéressaient à TDN, qui était opérationnel et « en recherche de sa première implémentation chez un client ». Le modèle d'affaire idéal, expliquait Kean, aurait été de construire une « *joint venture* » avec un consortium d'institutions bancaires, ou plus généralement d'institutions financières (comme des banques d'investissement, dépositaires de titres, bourses), et de créer avec elles une plateforme d'émission et de gestion d'actifs financiers.

Cette notion de « plateforme » introduisait un niveau de contrôle complémentaire à celui décrit précédemment, centré sur chaque entreprise émettrice de ses titres *via* le paramétrage

Chapitre 2. Les modes des jetons : instituer par les smart contracts

permis par l'ERC-1400. Ce contrôle supplémentaire était conféré des groupes d'entreprises émettrices réunies en « consortia ». Ce dernier niveau de contrôle passait par l'architecture informatique. L'idée de ConsenSys était de développer des réseaux Ethereum privés, « à côté » du réseau Ethereum public (on parlait de « *sidechains* »), dans lesquels les entreprises émettrices seraient elles-mêmes les « nœuds » (par analogie, en lieu et place des *miners* du réseau public). Dans ces réseaux, les entreprises ne seraient pas en compétition (comme l'étaient les *miners*, voir Chapitre 1) mais inscriraient les transactions à tour de rôle selon des règles définies collectivement, chacune ayant la possibilité de vérifier les transactions inscrites par les autres. Ces réseaux auraient accueilli toutes les opérations intermédiaires précédant l'inscription définitive de la transaction sur le réseau public. Parmi ces opérations étaient évoqués l'émission d'un jeton *ad hoc* dont chaque unité représenterait un euro ou un dollar (les investisseurs paient en euros ou en dollars, pas en ethers), le déploiement d'un module permettant aux cadres de ces entreprises de se connecter au système sans avoir à disposer d'une clé USB avec leur clé privée, et plus généralement les interfaces décrites plus haut permettant de paramétrer les émissions et les souscriptions de titres. En bref, le réseau public servirait pour la « conservation des actifs à long terme », et les réseaux privés serviraient aux échanges et vérifications préalables entre entreprises ou institutions financières associées.

La « combinaison » d'Ethereum en version « réseau public » et « réseaux privés » supposaient que des groupes d'entreprises du secteur s'allient. Ces alliances permettaient de faire face à des problèmes d' « efficacité » du réseau public. Le réseau public posait des problèmes de confidentialité, il limitait par construction le nombre de transactions qui pouvaient être inscrites dans un temps donné et impliquait des délais (nécessitant d'obtenir, bloc après bloc, un « consensus » des *miners*) ce qui posait des problèmes de « finalité » des transactions nécessaires aux marchés régulés comme le sont ceux des titres financiers. Les réseaux privés permettaient au contraire de vérifier le contenu des transactions entre membres associés avant de les chiffrer et de les inscrire sur le réseau public, de valider les transactions quasi instantanément. Cette architecture visait à conserver la caractéristique essentielle du réseau public, être le « seul réseau de confiance » (Kean) car autonome et

Chapitre 2. Les modes des jetons : instituer par les smart contracts

indépendant.

Mais ces alliances étaient également imaginées comme des alliances de gouvernance des titres financiers, entre entreprises et institutions financières, par des règles collectives de distribution et de contrôle de leur circulation. ConsenSys mettait en avant la force d'Ethereum pour bâtir une infrastructure planétaire, indépendante d'acteurs de la finance comme de fournisseurs de technologies, opposant notamment Ethereum à à-vis d'autres solutions permettant de construire des réseaux privés de consortium, comme Corda ou Hyperledger. Ethereum était développé par la « plus grande communauté de développeurs au monde » qu'ils estimaient à 300 000 personnes, au contraire des 35 000 d'Hyperledger ou des 20 000 à 30 000 de Corda, garantissant la richesse des librairies logicielle et la facilité à développer. Ethereum permettait également de garantir l'interopérabilité entre un réseau public dont étaient dépourvus Hyperledger et Corda et des réseaux privés. Cette interopérabilité technique était également « réglementaire » : le standard ERC-1400 permettait de bâtir des « solutions interopérables avec les institutions réglementées ».

Six mois plus tard, c'est lors du meetup #12 que se poursuivait le parcours de la conception des *security tokens*. Ce meetup était destiné à des développeurs ; il était intitulé « *{Tech Workshop} How to implement an ERC 1400* ». Ce meetup détaillait le code du standard, présentait les outils proposés par ConsenSys pour écrire des *smart contracts*. Il avait un objectif de formation, et de diffusion des pratiques de conception sur Ethereum et des briques d'infrastructures construites par ConsenSys, objets clés de sa stratégie qui sera abordée en détails dans la première section du Chapitre 3.

Conclusion du chapitre

Les cryptoactifs ont proliféré comme marchandises. Dans le même temps, ces cryptoactifs prenaient de multiples significations pour leurs concepteurs. Ces significations étaient associées à leurs formes techniques, *coins* ou jetons. Ces jetons prenaient eux-mêmes différentes significations selon leurs usages imaginés ; sur la période d'enquête, comme jetons utilitaires et *security tokens*. Un même type de jetons recouvrait lui-même différentes significations ; les jetons utilitaires étaient imaginés comme relations élémentaires d'un nouveau Web ainsi que comme liens économiques et financiers par lesquels ce nouveau Web pourrait advenir.

Différentes articulations permettent de nuancer la séparation entre espaces des concepteurs qui imaginaient des mondes alternatifs par les cryptoactifs d'une part, et un grand public qui les voyait comme des objets financiers en marge de la finance traditionnelle d'autre part. Parmi ces articulations, ce chapitre a souligné les opérations de conversion de formes d'argents propres à différents espaces (bitcoin et ether d'une part, euro et dollar de l'autre), la promotion des cryptoactifs comme investissements rentables car porteurs d'innovations technologiques, les soutiens matériels et financiers d'administrations publiques qui donnaient aux concepteurs les moyens de créer et de diffuser les cryptoactifs. Les *security tokens* montrent que ces articulations ne diffusent pas uniquement les cryptoactifs d'un intérieur constitué par l'espace des concepteurs vers le monde entier. Au contraire, *via* ConsenSys, Ethereum deviendrait un espace d'accueil pour des acteurs qui sont *a priori* étrangers à cet espace, les institutions financières et entreprises émettrices de titres financiers.

Sur un plan analytique, ce chapitre a situé les jetons comme éléments de relations étendues pour comprendre leur institutionnalisation. Cette approche visait à prendre le travail d'ingénierie relationnelle des concepteurs comme objet d'analyse, sans réduire la signification des jetons aux significations que leur attribuaient leurs concepteurs. Leur point de vue a ceci de particulier : les relations ne doivent être formées que par des jetons. En ce

Chapitre 2. Les modes des jetons : instituer par les smart contracts

sens, les *smart contracts* sont imaginés comme une technique institutionnelle, au travers de laquelle peuvent être codées des jetons auxquels sont réduits les significations des relations. Cette intuition a été développée par des économistes néo-institutionnalistes, qui qualifiaient la blockchain et les *smart contracts* de technologies qui sont, en elles-mêmes, des institutions (au même titre que la firme ou les marchés). J'ai proposé de situer ce type d'analyse comme prolongement de l'imaginaire des concepteurs lui-même. Le cas de Backfeed illustre la rencontre entre analyses économiques de ces objets et l'imaginaire des concepteurs.

Ainsi, l'institutionnalisation des cryptoactifs se comprend, en observant le développement des jetons, comme enrôlement d'acteurs amenés à adopter le point de vue de leurs concepteurs, de manière à limiter ou à éliminer les incertitudes pesant sur leur prolifération. L'incertitude sur les jetons utilitaires était d'abord formulée en termes d' « arnaques » pesant sur le financement et l'utilisation du Web alternatif, formulation qui supposait que les régulateurs partagent ce regard. Puis, l'incertitude réglementaire sur les jetons utilitaires (étaient-ils des investissements ?) était résolue en créant un type de jeton, les *security tokens*, éliminant l'ambiguïté pesant sur leur qualification avec le concours des institutions financières.

Les jetons sont des objets financiers imaginés en dehors des institutions financières *stricto sensu*, mais de nombreux concepteurs avaient travaillé dans ces institutions ou avaient été formés à la finance de marché. En ce sens, ces objets participaient à l'expansion des pratiques et de l'influence des professionnels de la finance, un phénomène qui a été analysé par différents champs des sciences économiques et sociale en termes de « financiarisation »¹²⁰. Toutefois, plutôt qu'une analyse en termes d'expansion du domaine de la finance, ce chapitre a montré que les significations (financières ou pas) des jetons

120 Ces études du phénomène de « financiarisation » caractérisent un capitalisme devenu « financier » en analysant les processus de transformation des économies et des démocraties du Nord par les institutions et les pratiques financières (mais aussi de l'État, rejoignant des analyses politiques en termes de « néolibéralisme »). Cette littérature identifie trois ensembles de transformations : un capitalisme privilégiant l'accumulation financière plutôt qu'industrielle, un changement des idéologies et des pratiques des dirigeants et cadres d'entreprises orientés vers la maximisation de la valeur produite pour les actionnaires, ou encore comme extension des objets de la finance à des domaines toujours plus vastes de la vie quotidienne (van der Zwan 2014).

Chapitre 2. Les modes des jetons : instituer par les smart contracts

n'étaient pas acquises *a priori*. Ces significations étaient l'enjeu central de leur institutionnalisation, mettant à l'épreuve les catégories institutionnelles habituelles (comme la firme) à partir desquelles était définie la nature « financière » (comme un « titre financier »).

Le volet « crypto » de la loi PACTE¹²¹ traduisait alors juridiquement la délégation des significations des cryptoactifs à leurs concepteurs, en cadrant en droit les cryptoactifs comme objets échangés sur des marchés financiers. Elle devait combler le « vide juridique » dans lequel se trouvaient les cryptoactifs. Cette loi, élaborée à partir du travail de différents acteurs qui participaient régulièrement aux meetups de ConsenSys, était unanimement louée par le secteur des cryptoactifs. Elle avait notamment pour objectifs de lutter contre les arnaques aux ICO, d'encadrer les acteurs de marché (typiquement : les *exchanges*) et d'autoriser des fonds (finance traditionnelle, régulée) à investir dans les cryptoactifs sous certaines conditions. Concernant les ICO, la loi permettait aux émetteurs d'ICO de demander à l'AMF un « visa optionnel » qui devait garantir une « meilleure information et protection des investisseurs »¹²² (AMF 2019). Ce visa conditionnait le « démarchage » auprès du public, par exemple la publicité et l'utilisation d'un nom de domaine en « .fr ». L'AMF imaginait ce visa comme un certificat de qualité des ICO. Fin 2021, seules quatre demandes avaient été formulées, et trois visas accordés. Concernant les acteurs de marché, l'AMF proposait un « agrément », lui aussi « optionnel », à la plupart des acteurs de marché (*exchanges*, dépositaires, mandataires) dits « Prestataires de Services en Actifs Numériques » (PSAN). Il visait à « assurer l'intégrité du marché et un mécanisme efficace et transparent de formation des prix, ainsi que de fournir une information fiable et des garanties aux investisseurs ». Les mêmes PSAN étaient en théorie soumis à un « enregistrement » lorsqu'ils conservaient des cryptoactifs pour compte de tiers et des

121 La loi dite « PACTE » (Plan d'action pour la croissance et la transformation des entreprises) du 22 mai 2019 a été présentée par le gouvernement d'Édouard Philippe. Les articles 85 à 88 concernaient le secteur des cryptoactifs.

122 L'AMF listait les « exigences » suivantes : l'obligation pour l'émetteur de jetons d'être constitué sous la forme d'une personne morale établie ou immatriculée en France ; la fourniture d'un document d'information destiné à donner toutes les informations pertinentes sur l'offre de jetons, le projet financé et l'entreprise ; la mise en place d'un dispositif permettant le suivi et la sauvegarde des actifs recueillis à l'occasion de l'offre ; le respect des règles en vigueur en matière de lutte contre le blanchiment et le financement du terrorisme.

Chapitre 2. Les modes des jetons : instituer par les smart contracts

conversions avec une monnaie ayant cours légal, comme les *exchanges*. Mais cet enregistrement « obligatoire » n'était imposé qu'aux entreprises qui visaient « explicitement le public français », ce qui expliquait que la plupart des *exchanges* n'étaient soumis à aucune forme de contrainte tout en exerçant en France.

Ainsi, *via* l'AMF et la loi PACTE, l'État endossait un rôle d'auditeur de projets et d'incitateur à la diffusion de « bonnes pratiques » de « protection des investisseurs » et d'un marché « efficace » et « transparent », sans réelle contrainte sur les acteurs de la diffusion des cryptoactifs. La loi PACTE visait explicitement à faciliter le développement du secteur. Le statut de PSAN accordait notamment un « droit au compte », droit renforcé par un décret ultérieur permettant aux PSAN de recourir auprès de l'ACPR (Autorité de Contrôle Prudentiel et de Régulation, institution de surveillance des banques) en cas de refus d'ouverture de compte par une banque. Ce droit au compte était une revendication historique du secteur des cryptoactifs.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Introduction. D'organisations économiques à la gouvernance par les transactions

Ethereum était utilisé pour deux types d'organisations économiques, selon leurs concepteurs. D'une part, les utilisations « B2C » (*Business to Customer*) faisaient d'Ethereum une « plateforme de développement d'applications décentralisées », selon la formule de son inventeur Vitalik Buterin (Buterin 2014a). Elles prenaient massivement la forme de « jetons » conçus par des startups (« *Businesses* »), lesquelles imaginaient des utilisateurs individuels (« *Customers* ») d'un nouveau Web (« Web 3.0 ») et de DApps ou, plus spécifiquement, d'une nouvelle finance (« décentralisée », « DeFi » pour « *DEcentralized FInance* » pour les acteurs et dans ce qui suit). D'autre part, les utilisations « B2B » (*Business to Business*) étaient celles de ces « intermédiaires » de l'économie numérique, entreprises ou institutions, typiquement regroupées dans des « consortia » d'acteurs en compétition mais coopérant dans l'utilisation d'infrastructures comptables distribuées rendant leurs relations commerciales plus efficaces, sûres ou transparentes. Les utilisations B2C problématisaient des réseaux de l'économie numérique contemporaine par les acteurs qui les administrent, alors que les utilisations B2B coalisaient ces mêmes acteurs par la formulation collective des relations numériques.

Comment comprendre qu'Ethereum soit simultanément utilisé pour bâtir des organisations économiques aux gouvernances apparemment si éloignées ? Cette introduction commence par distinguer deux opérations de production des transactions avec Ethereum, la formation et la formulation, communes à toutes les utilisations d'Ethereum. Cette distinction permet d'analyser Ethereum comme une technologie de gouvernance modalisable par ces deux opérations. Cette modalisation se lit dans la notion de « plateforme », attribuée par les concepteurs aux applications développées avec Ethereum, quel que soit le type d'utilisation

B2B ou B2C. Cette modalisation implique de faire se rencontrer deux utilisateurs inscrits dans la conception de ces plateformes ; l'un est générique à la technologie de plateformes Ethereum, l'autre est spécifique à chacune.

Modalisations de la gouvernance par l'infrastructure : formation et formulation des transactions

Les notions de B2B et B2C orientent le regard vers les entités mises en relations dans l'utilisation d'Ethereum. Je m'intéresse ici à la relation entre ces entités, prenant la forme « transaction » quel que soit le type de réseau économique imaginé. Ce rapport entre blockchain et transaction ressemble à celui entre Web et conversation. L'histoire des services Web peut se lire comme succession de dispositifs participant à une entreprise de mise en conversation des contenus numériques (Cardon & Prieur 2016). De manière analogue, je propose de voir les deux types de réseaux économiques B2B et B2C dans une histoire, nettement plus courte, de mise en transactions d'objets numériques comptabilisés sur un registre.

Deux opérations sont en jeu dans la mise en existence de relations numériques comme transactions. La formation est l'opération d'inscription de la transaction, la rendant effective, totalisant la relation à l'échelle d'un espace transactionnel. La formulation est l'opération d'énonciation d'une transaction dans le langage des *smart contracts* (*back-end*) et dans des interfaces qui rendent intelligibles ces algorithmes aux utilisateurs de services numériques (*front-end*). Formation et formulation étaient opérées par des acteurs différents, comme le prescrit la mystique du protocole (Chapitre 1). Ces notions visent à proposer une analyse sociale d'opérations infrastructurelles désignées par les concepteurs en termes de « couches » ; la formation correspond à la « *layer 1* » (couche basse), la formulation à la « *layer 2* » (couche haute).

Dans le cas des utilisations B2C, la formation était assurée par les *miners* anonymes, non sélectionnés à l'entrée d'un espace transactionnel qui était « ouvert » à des utilisateurs de

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

services et à des concepteurs de services. Dans le cas des utilisations B2B de consortium, ce travail de formation était assuré par les entreprises elles-mêmes en lieu et place des *miners*, cooptées à l'entrée selon leur identité légale dans un espace « fermé » qui était réservé à leur propre utilisation. Les DApps étaient des dispositifs de formulation de relations numériques de type B2C. Les *smart contracts* étaient également utilisés pour formuler des relations de type B2B entre acteurs réunis en consortium, comme des échanges interbancaires, par exemple dans le cadre du projet Ubin présenté en Introduction générale.

Ces deux opérations modalisaient la gouvernance des relations par l'infrastructure : par la mise en inscription pour la formation des transactions, par les fonctions ou significations de ces inscriptions pour la formulation des transactions. J'utilise infrastructure à la suite de travaux labellisés *Science & Technology Studies* (STS) qui analysent les innovations des infrastructures numériques et d'Internet en même temps que les formes contemporaines de gouvernance par l'information, en termes de transformations des organisations et de production de connaissance (Bowker et al. 2009) ou comme un mode de gouvernance d'Internet (Musiani 2018). Ces travaux invitent à dépasser la compréhension des infrastructures dans leurs dimensions uniquement matérielles (typiquement les briques, les tuyaux, les câbles) pour inclure dans l'analyse des objets qui paraissent plus abstraits (comme les protocoles, les standards ou la mémoire), eux-mêmes enjeux de connaissance et de contrôle par différents acteurs qui les modèlent et les contestent durant leur utilisation comme leur développement.

Technologie de plateformes

Les utilisations d'Ethereum étaient dites « plateformes », aussi bien les DApp¹²³ que les plateformes de consortia. Ainsi, dans ce qui suit, je prends la notion de plateforme comme une notion à analyser plutôt qu'un élément du corpus analytique. Infrastructures et plateformes ont été décrits comme deux angles analytiques ancrés respectivement dans les STS et dans les études des médias (Plantin et al. 2016 ; Plantin et al. 2018), chacun

123 Par exemple, Digix et Bluzelle au Chapitre 2 étaient désignées comme des « plateformes » par leurs concepteurs.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

présentant des intérêts heuristiques particuliers (par ex Plantin et al. 2016 : 6-9). Ce chapitre analyse les plateformes comme résultats de travaux d'« *infrastructuring* ». Un trait est généralement attribué aux plateformes : le caractère ouvert à une construction de l'extérieur. Je propose de le comprendre comme le résultat d'un travail d'*infrastructuring*.

« Plateforme » désigne communément un vaste ensemble de systèmes techniques et d'acteurs économiques (comme les medias sociaux, les magasins d'applications, ou les systèmes d'exploitation), ainsi qu'une notion qui a pris la suite de la métaphore « place de marché » pour l'étude des infrastructures numériques dès les débuts du web participatif (Beuscart & Flichy 2018 : 11 ; 13). La notion de « plateformisation » décrit de manière processuelle la transformation de l'« environnement » des plateformes par leurs acteurs. Les plateformes sont des espaces de mise en visibilité d'offres, aussi bien marchandes (travail, service) que non-marchandes (partage, entraide). Elles déplacent des pratiques restreintes à des espaces limités en mettant en relation des entités éloignées, par exemple en termes de travail (Flichy 2017 ; Beauvisage et al. 2018) ou de partage (Peugeot et al. 2015). Dans le même temps, les plateformes sont critiquées au prisme d'un mouvement historique de « plateformisation du monde » qui pointe la captation de la valeur produite par des activités individuelles *via* le Web, comme le pointent des auteurs sur les cas devenus emblématiques des travailleurs du clic (Casilli 2019) ou des chauffeurs (Rosenblat et Stark 2016).

Une originalité d'Ethereum était d'être utilisée comme une technologie de plateformes, au sens de technique ajustable dans des processus de conception. La formation des transactions peut être définie sur mesure dans le cas des utilisations B2B, alors qu'en général, plateforme désigne un dispositif à la main d'une organisation, voire directement l'entreprise qui la contrôle. Dans le même temps, les plateformes construites avec Ethereum avaient un caractère « programmable » par leurs utilisateurs, typique des plateformes (par ex. Helmond 2015, Plantin et al. 2016) notamment *via* les API, un dispositif d'enrichissement de services proposés par la plateforme qui reste en contrôle des relations qu'elle forme avec les utilisateurs.

La séparation entre formation et formulation des transactions est une critique du contrôle unilatéral des plateformes du Web, qu'elle soit prononcée en termes de contrôle total des opérations de formation, ou termes d'asymétries de capacité de formulation entre plateforme et utilisateurs. Par exemple, avec le cas Airbnb : que ce soit par l'interface comme par ses discours, la plateforme impose par « injonctions » aux « hôtes » (les utilisateurs qui mettent leurs appartements en location) de jouer un rôle de convivialité plutôt que celui de l'hôtelier (Jacquet 2015). Ce type d'études observe la plateforme comme un tout constitué, face auxquelles les utilisateurs doivent s'ajuster comme ils peuvent. Les hôtes doivent par exemple jouer en même temps sur différents registres de l'hospitalité, rendre compatibles les injonctions avec leur idée de la location.

Prescriptions : un utilisateur générique d'Ethereum, des utilisateurs spécifiques de plateformes

Formation et formulation des transactions passaient par des objets techniques. Ces objets cadreraient la manière de représenter une relation ainsi que les individus mis en relation. Reconnaître ces cadrages permet de pointer le caractère prescriptif des dispositifs et du monde qu'il est possible d'inscrire avec Ethereum. Madeleine Akrich a appelé « scripts » les opérations de cadrage des utilisateurs d'objets techniques selon des règles fixées à l'avance. « Script » prend le sens de prescription : ce que l'utilisateur peut faire ou doit faire en tant qu'utilisateur attendu, et qui est défini dans la conception de l'objet technique lui-même (Akrich 1987, 1992). Ces prescriptions indiquent des visions du monde qui guident le travail des concepteurs.

Les logiciels de formation des transactions, typiquement les logiciels dits « clients », intégraient le script d'un utilisateur générique d'Ethereum. Dans le cas des utilisations B2C, ces utilisateurs génériques étaient des portefeuilles ou « *wallets* » ; la généralité de cet utilisateur permettait aux *miners*, que j'ai décrits comme « aveugles » dans l'Introduction générale, d'inscrire les transactions sans se préoccuper de (ou « voir ») la signification des transactions. Dans le cas des utilisations B2B de consortia, ces utilisateurs étaient les entreprises qui contrôlaient la plateforme. En général, cet utilisateur générique signait les

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

transactions, de manière cryptée, quel que fut le sens de cette transaction (par exemple un virement bancaire, un vote) ou son identité en dehors de la plateforme (par exemple détenteur d'un compte en banque, citoyen d'un pays) jusqu'à l'inscription avec le protocole de consensus.

Pour une plateforme donnée, le processus de conception des opérations de formation et de formulation des transactions articulaient cet utilisateur générique à des utilisateurs spécifiques à l'usage de la plateforme. Pour chaque application ou service de la plateforme, comme les DApps pour les utilisations B2C ou la monnaie inter-bancaire avec le projet Ubin comme cas B2B, les concepteurs inscrivait cet utilisateur spécifique, typiquement dans les interfaces de ces applications ou dans le développement de *smart contracts*.

Plan du chapitre

Ce chapitre comporte deux sections, chacune répond à la question posée en début d'introduction par un angle. Je propose une conclusion intermédiaire pour chacune, ainsi qu'une conclusion du chapitre.

La première section montre qu'Ethereum est devenue une technologie de plateformes par un processus entrepreneurial et technologique au centre duquel figurait l'entreprise ConsenSys. Cette entreprise a d'abord financé et encouragé un « écosystème » de formulateurs de transactions ; typiquement, des concepteurs de DApps, comme les développeurs de jetons utilitaires rencontrés au Chapitre 2. À partir de ses premiers investissements et son activité de développement de logiciels, l'entreprise a proposé des offres de conseils et noué des partenariats enrôlant de grandes entreprises à l'utilisation d'Ethereum. Cette section documente la diversité des tactiques déployées par ConsenSys. Elles faisaient converger différentes organisations économiques par une même infrastructure, et participaient à enrichir les possibilités de gouvernance offertes par Ethereum.

La deuxième section est dédiée aux pratiques de conception de l'écosystème de

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

formulateurs. Elles circulent, notamment par les meetups, entre concepteurs d'utilisations B2B et B2C regroupés en écosystème. Le cas du service LeVote développé au sein d'Orange témoigne de l'ampleur des modalités de gouvernance d'Ethereum. Cette technologie de plateformes suppose un utilisateur générique qui participe au développement de l'offre de service, mais n'est pas toujours conciliable avec l'utilisateur du service imaginé par les concepteurs. Les débordements du cadrage d'origine les contraints à redéfinir ces utilisateurs, et dans le même temps, à revoir la gouvernance des relations, scrutins et votes, en ajustant la manière de former et de formuler les transactions.

1. Technologiser une infrastructure, transformer l'économie numérique par les transactions

Cette section montre que la vision portée par l'entreprise ConsenSys d'une économie numérique unifiée était mise en œuvre en pratique par la conception de dispositifs de formation et de formulation ajustables pour deux types d'organisations économiques. Elle se lit historiquement dans le processus de technologisation de l'infrastructure publique d'Ethereum en logiciel. Cette technologisation permettait d'inscrire un utilisateur générique d'Ethereum quelle que soit l'utilisation, tout en permettant aux grandes entreprises de reproduire des logiques organisationnelles et de contrôle pré-existantes sur leurs relations. Les paragraphes qui suivent indiquent que la notion « bâtisseurs de systèmes » proposée par Thomas Hughes est utile pour analyser l'activité de ConsenSys.

Avec Hughes : suivre l'activité d'un « system builder » pour analyser l'« infrastructuring »

Thomas Hughes a montré que l'électrification de l'Amérique est le résultat d'innovations tout autant scientifiques et technologiques que gestionnaires et financières (Hughes 1983a, 1983b). Ces travaux sont une référence pour les STS contemporaines, et plus spécifiquement pour les études sociales des techniques qui y ont vu un témoin de l'intérêt d'une analyse plurielle de l'innovation, au-delà des disciplines ou des rôles institutionnels des acteurs en présence. Pour Ethereum, cette approche est particulièrement intéressante pour ouvrir l'analyse aux différentes alliances forgées par les acteurs, sans se limiter aux catégories établies comme utilisations B2B vs B2C. Avec ce cas, l'historien montre la richesse d'une étude du développement des « systèmes techniques étendus » (« *large technical systems* ») comme des « artefacts culturels ». Il analyse des changements à la fois techniques, scientifiques, économiques, financiers, politiques et organisationnels en lien avec les nouvelles configurations de ces réseaux entre 1880 et 1930. Hughes appelle les historiens à considérer dans le même temps les configurations des objets techniques (en

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

particulier des réseaux) et les ressources et aspirations des organisations, groupes et individus en présence : les réseaux électriques sont, comme d'autres technologies, à la fois les causes et les effets du changement social (Hughes 1983a: 2).

L'unité d'analyse de Hughes est donc le système : un ensemble de composants en relations qui sont individuellement objets de contrôle. Le système a une « direction interne », tout en étant en relation avec son « environnement », défini par ce qui n'est pas contrôlable par les composants du système et propre aux « forces culturelles » des sociétés dans lesquelles les systèmes émergent (Hughes 1983a: 6 ; 462). Le système a une cohérence interne qui est le résultat du travail des « constructeurs de systèmes » (*system builders*) (Hughes 1983b), qui fixent des « objectifs », une « direction ». Qu'ils soient scientifiques (Edison), gestionnaires (Insull) ou financiers (Mitchell), ces constructeurs dépassent leurs disciplines pour étendre leurs systèmes en le transformant tout autant que l'environnement, spécifique à leur époque. La métaphore physique ponctue l'analyse de l'innovation de Hughes : le système acquiert une « masse » constituée par les différents artefacts techniques dans lesquels du capital a été investi ; cette masse génère un « mouvement », une phase que l'auteur appelle « *momentum* » ; le système a une « vitesse », son « inertie » est sa fermeté dans la poursuite des objectifs. Les constructeurs, figures individuelles ou entreprises gestionnaires, sont dans le même temps confrontés aux impératifs de « développement économique et de changement social » des institutions publiques, qui, selon des modalités variées et en fonction des lieux, imposent des contingences conduisant le système dans de « nouvelles directions » malgré son « momentum élevé » (Hughes 1983a : 15-17). Ils se déplacent parfois sur d'autres continents pour faire d'innovations développées ailleurs des composants à intégrer à leurs systèmes (comme les turbines développées en Europe).

Je m'appuie sur l'apport analytique de Hughes pour rendre compte du travail de conception d'un réseau technique étendu. En particulier, je cherche à articuler les « visions » des concepteurs aux développements technologiques et entrepreneuriaux sur l'infrastructure d'Ethereum pour analyser comment une forme générique de gouvernance des organisations économiques était élaborée. La principale nuance par rapport aux travaux de Hughes tient aux matériaux mobilisés, à partir desquels je ne prétends pas expliquer l'extension

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

d'Ethereum en général. Ils me permettent en revanche de rendre compte de l'activité d'un ensemble de concepteurs, en l'occurrence réunis dans une société appelée ConsenSys. Comme les concepteurs de systèmes de Hughes, les dirigeants de ConsenSys avaient pour « vision » d'étendre l'utilisation d'Ethereum ; comme eux, ils définissaient leurs problèmes en fonction de cet objectif ; et comme eux, ils ont joué un rôle historique dans le développement d'Ethereum et des blockchains.

La consommation d'électricité dans le cas de Hughes et l'inscription de transactions avec Ethereum sont deux types de services de systèmes techniques étendus. Le récit de Hughes insiste sur la conjonction de différentes innovations technologiques, scientifiques, gestionnaires, financières pour faire advenir ces systèmes et étendre l'accès à l'électricité. Leurs stratégies d'extensions sont construites par rapport à des filières industrielles existantes, par exemple quand ils calculent les propriétés technologiques que doivent avoir les filaments et les réseaux de distribution par rapport aux coûts d'utilisation des lampes à gaz (par ex Hughes 1983b : 25).

La stratégie de ConsenSys consistait à constituer un « écosystème » entrepreneurial par le développement d'outils infrastructurels. Cet écosystème ressemblait à ce que Hughes appelle l'« environnement ». Les acteurs de l'écosystème étaient des formulateurs : ils faisaient des *smart contracts* des DApps prêtes à être utilisées. Ces acteurs étaient eux-mêmes des concepteurs du système ; le rôle de ConsenSys était de développer des outils de conception, en l'occurrence de formation et de formulation des transactions, équipant ces acteurs.

Ainsi, ConsenSys agissait au moins autant comme « constructeur de système » que comme « constructeur d'écosystème ». ConsenSys imaginait Ethereum comme un unique réseau de validation de transactions pour une économie numérique unifiée, qu'elle soit désignée, selon les époques, de « *global settlement layer* » ou « *financial plumbing for the world* ». Dans le même temps, ConsenSys intéressait à l'utilisation d'Ethereum des acteurs identifiés à deux types d'organisations économiques : le Web3 pour les utilisations B2C, et les réseaux économiques existants pour les utilisations B2B.

1.1. Étendre un écosystème de formulateurs par le développement infrastructurel

Cette sous-section montre comment ConsenSys enrôlait de grandes entreprises comme formulatrices et formatrices de transactions. Elle s'appuie sur la mise en parallèle de deux entretiens publics du fondateur de l'entreprise ; dans l'un il s'adressait à ces entreprises, dans l'autre il s'adressait aux acteurs de l'écosystème réunis lors de la conférence annuelle EthCC. Ces entreprises étaient non seulement enrôlées comme possibles utilisatrices de la « plateforme de DApps » avec le développement de la DeFi, mais aussi dans un processus de « technologisation » d'Ethereum, qui consistait à les inscrire (Akrich 1987, 1992) dans la conception des dispositifs de formation et de formulation.

B2C et B2B : un travail infrastructurel transverse

Deux salles, deux publics. Le 2 mars 2020, Joseph Lubin s'exprimait dans une salle située dans les étages de la Maison de la Mutualité devant un parterre de clients et de prospects de la société ConsenSys qu'il dirigeait et avait fondé cinq ans plus tôt. Cette prise de parole lançait une demi-journée de rencontres organisées par le bureau parisien de ConsenSys intitulée, comme un écho à la métaphore de Hughes : « *The Ethereum Momentum : on the road to product market fit* ». L'objectif de la société était ainsi de présenter les derniers produits de la société ConsenSys comme un événement historique auquel participaient des employés ainsi que des clients venus « témoigner » d'utilisations B2B d'Ethereum et du sérieux de l'« accompagnement » de ConsenSys¹²⁴. Le lendemain, le même Joseph Lubin s'exprimait dans le grand amphithéâtre de la Maison de la Mutualité devant des participants de l'Ethereum Community Conference (dite « EthCC »). Cette conférence internationale rassemblait principalement des développeurs et des entrepreneurs construisant des utilisations B2C d'Ethereum ou DApp, aux côtés d'autres concepteurs de l'infrastructure

124 Après Joseph Lubin, deux représentants d'utilisations B2B d'Ethereum ont pris place sur scène pour « témoigner » de l'accompagnement de leur prestataire ConsenSys, sous forme d'interview croisée, conduite par un employé du bureau parisien de ConsenSys. Puis, les participants se sont répartis dans des ateliers en parallèle les uns des autres appelés « *breakout sessions* », organisés et conduits par des employés de ConsenSys, et durant lesquels un produit de ConsenSys était présenté dans ses aspects techniques ou pratiques à un sous-groupe de participants de la matinée de rencontres.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

publique, comme les membres de la Fondation Ethereum. L'événement était organisé tous les ans, depuis 2018, par l'association de promotion d'Ethereum en France appelée Ethereum France à l'époque, anciennement Asseth¹²⁵.

Deux tons, mais un même format de communication publique dit « *fireside chat* », une notion qui existe depuis une série de diffusions radiophoniques de Franklin Roosevelt entre 1933 et 1944. À la manière du 32^e Président des États-Unis qui trouvait un moyen de communication directe de sa politique à ses concitoyens, évitant la mauvaise presse des journaux conservateurs dans une période troublée par la Grande Récession et la Deuxième Guerre mondiale, Joseph Lubin intéressait (Callon 1984) deux types de publics à l'activité de ConsenSys. Ces deux prises de paroles étaient des entretiens avec Kean et Jean respectivement, chacun dans un style propre à un public. Kean, directeur du bureau de ConsenSys à Paris, s'adressait à Lubin comme dirigeant d'une société dynamique qui avait construit un ensemble de « produits » prêts à générer de la « traction » pour des entreprises. Joseph Lubin expliquait à ces clients et prospects du bureau parisien la pertinence du « *product-market fit* », c'est-à-dire l'adéquation entre des solutions logicielles (« *products* ») de ConsenSys et leurs attentes imaginées (« *market* »). Jean était un ancien employé de ce bureau et, en même temps, président de l'association Ethereum France depuis ses débuts en 2015. Il s'adressait à son ancien patron comme à un visionnaire dont il vantait le parcours, les études de la robotique dans les années 1980, les expériences dans l'informatique financière à Goldman Sachs ou comme dirigeant de *hedge fund* dans les années 1990 et 2000, les investissements dans un label de musique reggae en Jamaïque, jusqu'à son intérêt précoce pour Bitcoin et la « tech » associée au début des années 2010.

Ces communications participaient à constituer deux types de « *Businesses* » différents, grandes entreprises le lundi et startups le mardi, en utilisatrices B2B et B2C. Elles montrent

¹²⁵Ce changement de nom a été décidé lors de l'Assemblée Générale de l'Asseth en décembre 2019. L'association reprenait le nom Ethereum France, utilisé depuis plusieurs années par l'administrateur du site web ethereum-france.com, dédié à la popularisation d'Ethereum en langue française. Le site web proposait des actualités sur Ethereum, des traductions d'articles écrits en langue anglaises, ou encore des tutoriels pour faciliter une utilisation large d'Ethereum (on parlait alors d'« adoption »). Son administrateur Simon Polrot, tout comme la plupart des contributeurs, étaient également membres de l'Asseth. Le changement de l'Asseth actait la structuration de la promotion d'Ethereum en France autour d'une même association.

que la gouvernance de l'économie numérique était imaginée dans des formes infrastructurelles, modalisable en fonction de la manière d'inscrire des utilisateurs imaginés spécifiques dans les logiciels de formation et de formulation des transactions. Cette section le caractérise en mettant ces deux communications en miroir : dans les paragraphes qui suivent, des verbatims sont présentés côte-à-côte pour faire apparaître les problèmes énoncés dans chacun des cas (surlignés en gras) et la similarité des termes utilisés pour les désigner (soulignées de part et d'autre).

Le cas de la DeFi : les entreprises comme potentielles utilisatrices de services B2C

Ces deux communications avaient une unité de situation. Leur unité de lieu s'explique par la proximité entre les membres de l'association Ethereum France, organisatrice d'EthCC, et de ConsenSys : les employés de cette dernière étaient souvent membres actifs de la première. Leur unité de temps se lit par les mentions récurrentes à la DeFi. Ce thème était naturellement attendu dans la conversation avec Jean. Début 2020, la DeFi faisait en effet la une de la presse spécialisée, et de nombreuses startups développant des utilisations B2C s'en revendiquaient. La DeFi était le label de la plus importante « *track* » d'EthCC en termes de nombre de présentations. En revanche, j'ai été surpris d'entendre Joseph Lubin parler de DeFi dans son échange avec Kean, qui cherchait plutôt à orienter son interlocuteur vers l'adéquation des produits ConsenSys aux utilisations B2B pour grandes entreprises.

La DeFi était imaginée comme un « espace ouvert » dont la popularisation était fonction du développement infrastructurel de la plateforme de DApps Ethereum. L'utilisateur naturel de la DeFi était d'abord un « *financial nerd* » ou un « *techy nerd* » (Tableau 8, droite) qui participait à faire advenir Ethereum (en augmentant sa « bande passante », Tableau 7, gauche). C'est ce que désignait Joseph Lubin en qualifiant la DeFi d'une des deux « *killer app* » (« application phare ») possibles d'Ethereum. La recherche d'une « *killer app* » occupait de nombreuses discussions dans les réseaux de passionnés et de concepteurs d'Ethereum au moment de l'enquête. Communément, cette notion désigne un programme informatique qui, a lui seul, justifie l'achat d'une machine capable de l'exécuter,

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

notamment dans le cas de jeux vidéos¹²⁶. De manière similaire, la finance pouvait être l'« application phare » de l'« ordinateur mondial » Ethereum début 2020, susceptible de populariser largement Ethereum comme une plateforme pour « être humains normaux » (sic). L'éther prenait une autre fonction que celle de monnaie d'échange pour valider les transactions entre inscripteurs : un « collatéral » pour les opérations de la finance décentralisée émergente.

| A Jean (public B2C), le 3 mars 2020 | A Kean (public B2B), le 2 mars 2020 |
|---|---|
| <p><i>If you take all the different <u>money Lego protocols</u> and understand that you can <u>wire</u> them together then, that's probably going to be [finance] and/or gaming is going to be the first killer app that draws lots of <u>normal human beings</u> to the platform. And when that happens, so, David Hoffman I think was the first person that called ether a 'permissionless collateral,' that enables the bandwidth of decentralized finance, and so as more and more value comes into the <u>decentralized finance ecosystem</u>, it's gonna raise the value of that permissionless collateral token, which is going to increase the bandwidth for <u>open decentralized finance</u>. So, the more money that comes on to this platform, the more activity and attention that drives and the more bandwidth that creates, because essentially, there will be more ether collateral available to do more lending and to drive more liquidity through these protocols.</i></p> | <p><i>So, product market fit a few years ago just involved, finding anybody who would listen to you, and, maybe selling them some education, selling them a proof of concept project, not exactly product market fit, but we had to pioneer, open up an ecosystem and do a lot of handing. So currently, product market fit is different for different kinds of customers. So, <u>if you are a financial nerd, a techy nerd</u> and the financial world is interesting to you, or if you're <u>just a human being</u> that might want to achieve a little bit of yield on their savings, we have a new world opening up called the <u>open decentralized finance space</u>, where we have these different money protocols. And, people are able to mix and match the <u>protocols, wire</u> them together. Essentially these <u>magic internet money Legos</u> are about to become what we think of as the financial plumbing for the coming decentralized economy.</i></p> |

Tableau 8 : L'importance de la DeFi face aux deux publics

Joseph Lubin distinguait deux manières d'utiliser Ethereum qui se lisent dans le rôle qu'il projetait sur les entreprises à qui il s'adressait en échangeant avec Kean. Elles étaient des utilisatrices possibles de la DeFi au même titre que tout utilisateur d'Ethereum, que les « nerds ». Il décrivait ces applications comme « *money Legos* », donnant une vision dynamique, collaborative, de construction d'une finance alternative. Les différents concepteurs d'applications décentralisées (ici financières) utilisaient les « pièces » développées par d'autres pour construire de nouveaux services. La métaphore du « Lego »

¹²⁶ *Tétris, Super Mario Bros* ou la saga des *Final Fantasy* sont connus pour avoir participé, respectivement, au succès des consoles de jeux NES (Nintendo), Game Boy (Nintendo) et Playstation (Sony).

s'inscrit dans un champ lexical de la construction de l'infrastructure : l'argent circule par des « protocoles » à « assembler ». L'existence de ces circuits valorise le fluide lui-même (l'ether) qui peut devenir un « collatéral » pour des produits financiers et ces protocoles la « plomberie financière de l'économie décentralisée à venir ». Cette utilisation d'Ethereum par la DeFi contrastait avec les utilisations B2B dans lesquelles les entreprises étaient des formulatrices dans des applications livrées clé en main, au prix de « projets » visant à les « éduquer ».

D'un écosystème B2C à faire exister par la conception de briques infrastructurelles...

L'enrôlement des entreprises dans les utilisations B2C (en l'occurrence de la DeFi) en 2020 était la suite d'une stratégie d'entreprise construite de longue date par ConsenSys qui tenait dans le concept vernaculaire d' « écosystème ». L'écosystème était au centre des préoccupations de Joseph Lubin en 2020, quel que soit son public (Tableau 9, droite et gauche). Il désignait l'ensemble des acteurs qui développaient des applications décentralisées, de l'émission des ICO et des jetons utilitaires aux « *magic Internet money Legos* » dans le cas de la DeFi en passant par les STO et les *security tokens*, jusqu'aux clients qui participaient à construire des « *proof of concept* » dans le cas des applications B2B. En bref, l'écosystème désignait tout acteur qui formulait des transactions, au sens que j'ai donné plus haut. Voici comment Jean, en entretien, définissait la notion d'écosystème¹²⁷ :

*Quand j'utilise le terme **écosystème**, pour moi, quand je parle d'Ethereum et que je dis « ah l'écosystème Ethereum », je parle **strictement des boîtes qui créent une couche applicative ou qui créent du service autour d'Ethereum**. Voilà. Mais nécessairement, ces boîtes elles sont composées des gens de la communauté ; c'est-à-dire de **toute personne qui développe des services, qui développe des choses autour d'Ethereum**. (entretien avec Jean, novembre 2021)*

Cette mise en réseau, par le développement infrastructurel, était historiquement le premier

127 Jean répondait alors à une sur le sens de la notion d' « écosystème », et de sa différence éventuelle avec la notion de « communauté », elle aussi souvent mobilisée par les acteurs (de la communauté et de l'écosystème).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

objectif de ConsenSys. Selon Joseph Lubin, l’aventure avait commencé alors qu’il était membre de l’Ethereum Foundation et participait à rassembler des personnes pour fonder une entreprise de développement d’applications décentralisées amenées à constituer le « Web3 » imaginé à partir d’Ethereum. L’enjeu était de rendre ce rêve concret en « appliquant » la technologie. Cette entreprise s’était heurtée à ce qu’il appelle « l’immaturité » de la technologie. Pour lui, la réponse était dans le développement de l’écosystème¹²⁸, via le développement de logiciels. D’abord, ConsenSys a proposé d’équiper les concepteurs d’applications décentralisées avec des outils comptables de pilotage des transactions comme Balanc3, plus tard transformée en « plateforme comptable d’actifs numériques » (Balanc3 2017, 2018) à l’époque où les jetons popularisaient Ethereum (voir Chapitre 2), ou encore des listings d’applications décentralisées (« DApp store »). Ces travaux consistaient à constituer un écosystème en rendant le développement émergent et distribué de nouvelles DApps visibles largement. Ils ont conduit ConsenSys à problématiser non seulement le manque d’information des développeurs de *smart contracts*, mais aussi leur manque d’équipement, eux qui ne disposaient alors d’aucun outil de programmation dédié.

| A Jean (public B2C), le 3 mars 2020 | A Kean (public B2B), le 2 mars 2020 |
|--|---|
| <p><i>[I] started ConsenSys to try to <u>build decentralized applications</u> on this new platform that wasn't quite released yet, and turned out it was <u>really hard to build decentralized applications</u> and so we ended up building things like a DApp store, and a little <u>accounting system</u>, and from that emerged essentially <u>infrastructure and developer tools</u>, things like <u>Truffle</u> suite, and Infura, and MetaMask, and other pieces.</i></p> | <p><i>I went ahead and started gathering people to build things like <u>accounting systems</u>. And we tried to build an <u>app store</u> [...] Essentially all of us realized it was just <u>really difficult to build decentralized applications</u> with no <u>developer tools</u>, and no real ecosystem around us. So, sort of organically and by default, we ended up having to build out quite a bit the Ethereum ecosystem, and build lots of <u>developer tooling and infrastructure</u>. [...] One thing that was a, an early success was a project called <u>Truffle</u>; the person who was building that app store, surprisingly called <u>DApp store</u>.</i></p> |

Tableau 9 : Pas d’applications décentralisées sans outils d’infrastructure et de développement

128 Lubin rappelle également qu’à l’époque, différents acteurs craignaient étaient « sceptiques » vis-à-vis du développement d’applications décentralisées, craignant que le code (ouvert) des *smart contracts* des DApp naissantes soit copié. Il explique avoir opposé une autre vision de la valeur d’une entreprise, résidant avant tout dans la qualité de service et des personnes impliquées dans l’entreprise qu’il fallait équiper.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Ainsi, le développement de l'écosystème passait au départ par ce que Joseph Lubin appelle des « outils d'infrastructure et de développement », comme Infura, Metamask ou Truffle (Tableau 9). Truffle est devenue une suite de logiciels en développement permanent et la plus utilisée par les développeurs de *smart contracts*. Il s'agissait de ce qui est appelé un « *integrated development environment* » en informatique : un logiciel qui facilite l'écriture et l'édition du code, qui automatise sa compilation et son debuggage. Metamask et Infura sont rapidement devenus des portes d'entrée essentielles à Ethereum dans ses utilisations B2C. Metamask est un gestionnaire de *wallets* qui a rencontré un succès important auprès des utilisateurs d'Ethereum pour sa simplicité d'utilisation, en particulier par son intégration réussie dans les navigateurs Firefox ou Chrome (comme « *add-on* »), lesquels servaient d'interfaces des DApps. Infura permet à des développeurs de DApps de gérer dynamiquement les transactions à acheminer vers Ethereum (c'est-à-dire vers ses inscripteurs), en particulier la gestion du gas, cette unité du coût lié à l'exécution du *smart contract*¹²⁹. Infura proposait aux développeurs d'obtenir des frais d'exécution des transactions au meilleur prix, une sorte de courtage en gas, dont l'accès se fait par abonnement mensuel qui dépend notamment du nombre de projets créés sur l'interface et du nombre de requêtes quotidiennes¹³⁰.

L'écosystème était un ensemble de personnes et d'entreprises qui travaillaient en réseau, étaient équipées des mêmes outils et savaient ce que faisaient leurs pairs. Construire l'écosystème Ethereum était une condition du développement des applications décentralisées imaginées mais absentes d'Ethereum au départ. Ce déplacement de la construction d'une infrastructure à la constitution d'un écosystème était aussi l'intuition suivie par Jean quand il fondait l'association Asseth devenue Ethereum France, motivé par

129 Le gas est facturé en ethers à chaque transaction. Il dépend notamment de l'encombrement du réseau et du nombre de lignes du *smart contract*.

130 Le site web d'Infura indique que ce service vise à faciliter le développement de DApps, orienté, à l'époque de rédaction de ces lignes, vers la construction de « jetons non fongibles » (NFTs) : « *La construction de DApps sur le réseau Ethereum s'accompagne souvent de l'inconvénient de transactions bloquées, des frais de gaz élevés et des coûts de transaction cachés. Et si vous pouviez vous concentrer sur construire ce nouveau projet NFT sans avoir à gérer les complexités de manipulation de l'ETH ?* » (Infura 2023).

« la petitesse de l'écosystème » (entretien avec Jean, novembre 2021). Au dernier trimestre 2015, l'association organisait ses premiers meetups « dans les boîtes d'informatique des uns ou les boîtes de conseils des autres, ou chez les uns et chez les autres ». Ces meetups à thèmes visaient à partager des connaissances et des pratiques, d'apprendre ensemble, par exemple à compiler un *smart contract* puis fêter les rares compilations réussies, « avec des bières ». Ces événements rassemblaient des développeurs avides de rencontres avec d'autres passionnés par « la tech » mais aussi des « rencontres vie blockchain vie réelle ». Jean construisait l'écosystème lui aussi, comme un réseau de connaissances interpersonnelles et de développement de pratiques communautaires, quand ConsenSys cherchait à construire les outils qui manquaient à des passionnés comme Jean.

... à la technologisation de l'infrastructure : briques logicielles intégrées en « full stack » B2B

Début 2020, la construction d'un écosystème n'était pas le seul objectif du fondateur de ConsenSys. La rentabilité de différents logiciels construits les années précédentes devenait sa première préoccupation (son « étoile polaire », ci-dessous). ConsenSys cherchait à « intégrer » ses logiciels comme différentes briques dans une « *full stack* », prête à être déployée chez des clients. Cette suite logicielle était imaginée comme un « système d'opérations blockchain », une notion qui désigne habituellement le logiciel d'orchestration d'un ordinateur (comme Windows de Microsoft) ou d'un smartphone (comme Android par Google). Ici, l'orchestration visait un réseau d'ordinateurs de différentes entreprises :

*Our next phase is essentially, and we're thinking this is the north star for our company, is to **take all the different products**, projects that are gaining some traction, that are seeing some product market fit. So these are the things like Infura, and our Ethereum client Hyperledger Besu, which **we have a commercial version** of, and Metamask and Identity. And, essentially **we have built a full stack**, and we're moving towards essentially **creating a blockchain operating system** so that, **like a computer** the operating system enables access to the resources, but for a blockchain operating system, **for a company or for a consortium it will enable all of the resources of those organizations to essentially be under control and effectively utilized.** (Joseph Lubin à Kean, meetup #18, mars 2020)*

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Ce faisant, ConsenSys construisait une technologie à partir de ses logiciels d'« *infrastructuring* », au départ destinés à équiper le développement d'un écosystème autour d'une « plateforme de *smart contracts* » particulière, celle imaginée par les fondateurs d'Ethereum (Buterin 2013, Wood 2014) dont faisait partie Joseph Lubin. Le transfert de ces logiciels était une technologisation de l'infrastructure initiale bâtie pour des utilisations B2C. Ce processus était « complet » (« *full* »), de la formation des transactions (couches matérielles dites « basses ») à leurs formulations (couches les plus « hautes ») : il comprenait un logiciel « client » spécifique (Besu) pour administrer les nœuds du réseau (c'est-à-dire constituer les inscripteurs) jusqu'à la gestion des identités des utilisateurs en passant par une déclinaison d'Infura pour inscrire les transactions.

Les mêmes technologies étaient mentionnées auprès des deux publics, mais elles étaient ajustées à chacun. Premièrement, le Tableau 9 met en contraste deux manières de former les transactions, spécifiques à chacun des deux publics. À gauche avec les utilisations B2C, la « plomberie financière du monde » maintenue par les *miners* ne peut être détenue par les « prêtres financiers, des gens dans les églises des banques centrales, ou dans les églises des banques commerciales et d'investissement les plus importantes ». Elle inscrit un utilisateur générique en rupture avec le système financier traditionnel. À droite, les utilisations B2B d'Ethereum permettent aux entreprises elles-mêmes de former leurs transactions ; la mise à jour du « système d'opérations » permet d'améliorer l'efficacité, de l'utilisation des ressources aux relations avec les régulateurs. Elles inscrivent des utilisateurs qui ont leurs propres pratiques commerciales et organisationnelles, répliquables dans la formation des transactions.

| A Jean (public B2C), le 3 mars 2020 | A Kean (public B2B), le 2 mars 2020 |
|--|--|
| <p>You're not a really a programmer necessarily if you're using certain tools to build websites, but the tools facilitate people moving into this information economy. And we're moving now from this information economy which is based on TCP/IP and HTTP and HTML and SMTP, to an internet of value, economy, which invents a new form of trust and that's gonna be based on different protocols. It's, it imbues strings of digits, with actual value, because we've invented</p> | <p>We now have the ability to build this full stack, blockchain operating system [...] we are fully integrated, coherent development picture, able to optimize from the protocol layer, through infrastructure, whether it's Infura on mainnet or Infura direct in some private situation. We have all of our developer tools in the mix. We have</p> |

| | |
|---|--|
| <p>something called digital scarcity, and so this becomes the new language, the new sort of base understanding of so many people in the economy. [...] So, the financial plumbing of the world, used to be owned by, and operated by, the financial priests; people in the churches of the central banks, or in the churches of the major commercial and investment banks, and now your bank is in your pocket, and you can totally program your bank. It's not quite there yet, but absolutely everybody is going to be able to operate the machine, the way they want to.</p> | <p>identity and reputation. We have wallet access, and because we've been working for quite a while with regulators around the world on token launches, we can have applications like token issuance, also documentation, or document management and legal document, all of that can be done in a fully regulatory compliant fashion.</p> |
|---|--|

Tableau 10 : À chaque public une modalité de gouvernance de l'économie

Deuxièmement, quelle que soit la manière de former les transactions, les deux publics pouvaient imaginer des utilisateurs spécifiques à leurs applications. À gauche, les *smart contracts* permettaient à « tout un chacun » de « programmer sa banque » dans un espace aussi vaste que « le monde » lui-même. Il était ouvert, peuplé d'utilisateurs qui n'avaient « pas besoin d'être programmeur » grâce à des outils et des protocoles qui leur permettaient de « bouger » : de manière similaire aux outils qui faisaient de la programmation de l'information dans le Web contemporain un « langage », les transactions étaient l'expression d'une « vraie valeur » reconnue par tous les individus peuplant cet espace. À droite, la formulation passait aussi par des outils d'*infrastructuring*, des « outils de développement » qui étaient intégrés aux outils de formation, nommés en fonction du langage des entreprises elles-mêmes, par exemple en termes d'identités, de réputation, ou encore de documentation et de réglementation nécessaire pour garantir la conformité de ce qu'il se passe dans cet espace. Pour ces acteurs, les relations devaient intégrer les exigences réglementaires auxquelles ils étaient soumis.

1.2. La preuve est dans le script : tactiques d'enrôlement des grandes entreprises

La technologisation de l'infrastructure devenait en 2020 une « *full stack* », ajustant formation et formulation pour ces entreprises. Ce processus était contemporain d'une évolution des activités financières et commerciales de ConsenSys. Il participait à

l'enrôlement de ces grandes entreprises, qui devenaient inscrites dans les dispositifs de formation et de formulation des transactions. Cette inscription visait à en faire soit des utilisatrices de consortia qu'elles gèreraient indépendamment de l'infrastructure publique (B2B), sinon à les inciter à devenir conceptrices de DApps elles-mêmes (B2C). Cette sous-section s'appuie sur le cas de Jean¹³¹, dont le curriculum témoigne de la porosité entre développement des utilisations B2C et B2B d'Ethereum.

Portrait : des cartes graphiques au conseil

Au début des années 1990, les doudous de Jean s'appellent NES, Super Nintendo et PlayStation : les jeux vidéos passionnent Jean durant toute son enfance. Adolescent, il affronte les meilleurs joueurs du monde en ligne dans des compétitions confidentielles (au contraire de la médiatisation que certaines connaissent au tournant des années 2020 par les réseaux sociaux). Il gagne des cartes graphiques et des cartes mères. Jean en profite pour bricoler des ordinateurs avec ses amis. Bac en poche, il s'engage dans la préparation des concours aux grandes écoles d'ingénieurs. Ne se découvrant ni intérêt ni facilité pour les sciences physiques, il intègre finalement l'ENS Cachan en section économie et management. Jean poursuit ses études avec un master recherche en économie quantitative. Alors qu'il réfléchit à préparer une thèse en sciences économiques, il multiplie les rencontres avec des économistes et des doctorants. C'est à ce moment là qu'il découvre le *whitepaper* de Bitcoin. Fasciné par l'idée d'une monnaie qui existerait sans banque centrale et grâce au calcul informatique, il se forme à l'informatique et aux techniques de cryptographie *via* des cours en ligne ouvert à tous (ou MOOC) mis en ligne par Stanford. Jean préfère un emploi de correspondant du Ministère de la Santé français au Conseil européen (pour l'élaboration de statistiques concernant la protection sociale) à la recherche en économie. Sur son temps libre, Jean achète et configure des cartes graphiques en « *miners* » de Bitcoin.

131 En 2021, Jean avait fait sa principale activité professionnelle de ses deux passions, les jeux vidéos et Ethereum. Sa startup construisait des jeux vidéo avec des *smart contracts* : *via* un site Web, les joueurs s'affrontent *via* des cartes numériques et des vaisseaux spatiaux qu'ils peuvent également revendre (comme des jetons non fongibles, ou NFT).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Jean découvrait Ethereum par son infrastructure matérielle, en amateur. Les cartes graphiques qu'il achetait pour construire ses *miners* de Bitcoin entre 2013 et 2014 devenaient en quelques mois peu rentables face à la généralisation des calculateurs appelés *Application-Specific Integrated Circuits* (ASICs), construits spécifiquement pour optimiser les calculs demandés par le protocole Bitcoin. En quête d'une plus grande profitabilité, Jean découvre le projet Ethereum, alors en gestation. Il participe à miner l'ether dès les premiers mois suivant le lancement d'Ethereum, en 2015. C'est à ce moment-là qu'il participe à fonder l'association Asseth. Il est alors fasciné par l'idée de bâtir un ordinateur mondial capable d'exécuter toutes sortes de services sans possibilité de censure, ce qu'il appelle un « système anti-fragile ».

Son engagement associatif suivait la même intuition que celle suivie par Joseph Lubin par l'entrepreneuriat : développer un écosystème de développement de DApps. Elle se traduisait également par le développement de l'infrastructure. Pour Jean et l'Asseth, développer l'écosystème c'était (se) former à la pratique des *smart contracts*, faire connaître Ethereum en traduisant en français de la documentation rédigée en langue anglaise, apprendre avec d'autres passionnés aussi bien en ligne que dans des réunions qui prendront plus tard la forme de meetups. En un mot, développer l'écosystème passait par le développement d'une « communauté » composée d'individus développeurs et utilisateurs de *smart contracts* :

*On utilise tous nos produits ensemble. Tout le monde utilise les software de tout le monde. C'est aussi une partie de la beauté de l'open source et de la facilité qu'on a à se login d'un produit à l'autre. Mon wallet je l'utilise sur plein de produits différents, de temps en temps j'utilise le smart contract de quelqu'un via son front end, je vais carrément contacter le gars [via Github] en lui disant « mais là tu fais carrément n'importe quoi, c'est pas cool, c'est nul, tu as pensé à changer ce truc-là et ce truc-là ? ». En fait, tu te rends compte que **tes utilisateurs sont des power users** qui connaissent aussi bien sinon mieux tes produits que toi, et qui te donnent de super bon conseils et t'aident à faire le truc bien, dont tu utilises aussi leurs produits par différents truchements. En fait tu te dis, c'est cool : mes clients font partie d'une communauté dont j'ai besoin de faire partie pour bien pouvoir les servir et qu'ils utilisent bien mes produits. (entretien avec Jean, novembre 2021)*

Les activités de Jean dans le développement d'utilisations B2C lui ont donné une

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

« visibilité dans l'écosystème » : fin 2016, il rejoint un des deux plus grands cabinets d'audit et de conseil mondiaux qui cherchaient à le recruter¹³². À la même période, la hausse du cours de l'ether participait lui aussi à développer l'écosystème et stimule son financement avec les ICO. Jean analysait rétrospectivement cette envolée du cours sur les places de marchés comme Binance ou Coinbase comme un événement majeur pour « fédérer, faire entrer des gens dans l'écosystème ». Nombreux étaient les curieux de Bitcoin et des cryptomonnaies qui commençaient et à « s'enrichir » et à « y croire ». À cette même époque a lieu la controversée expérience dite « The DAO », analysée au Chapitre 4, ainsi que la conférence internationale DevCon2 (la deuxième « *Developer Conference* ») à laquelle Jean se rend.

Prouver que les entreprises sont inscrites comme utilisatrices imaginées

Jean voyait son travail de conseil comme participation au développement d'Ethereum, préférant rejoindre le cabinet qui lui proposait d'encadrer et de former des ingénieurs plutôt que celui qui attendait de lui des démarchages auprès de prospects B2B. Son employeur cherchait à vendre des « missions d'acculturation » dites aussi « *proofs of concept* » à des institutions publiques ou privées friandes d'expérimentations d'une « technologie blockchain » annoncée comme une révolution des échanges ou, plus prosaïquement, des systèmes comptables entre entreprises. À cette époque (2016-7), différents logiciels (dits « solutions blockchain ») étaient à la disposition des sociétés de conseil pour construire des utilisations B2B. Quorum, logiciel construit à partir du code d'Ethereum par la banque d'investissement JP Morgan, était l'un d'eux. Les deux autres solutions concurrentes s'appelaient Corda et Hyperledger Fabric, respectivement développées par une startup appelée R3 et par Hyperledger, un projet de la Fondation Linux constitué comme consortium d'entreprises¹³³.

132 Jean était à ce moment-là employé comme statisticien par un think tank patronal pour lequel il construisait des modèles économiques nourrissant un travail d'influence des politiques publiques.

133 R3 comme Hyperledger fonctionnaient comme des consortia rassemblant des entreprises financières et technologiques. Ces dernières payaient une cotisation (souvent en fonction de leur taille) et impliquaient des employés dans la construction d'une solution logicielle blockchain open source. Leurs participations visaient à intégrer dans le logiciel leurs exigences individuelles ou, du point de vue de l'anthropologie des

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Le cabinet de Jean se disait « agnostique », c'est-à-dire qu'aucune « solution » parmi Quorum, Corda et Hyperledger Fabric n'était *a priori* exclue ou privilégiée dans les prestations de conseil¹³⁴. La notion d' « agnosticisme » est utilisée en ingénierie informatique pour désigner un logiciel compatible avec différentes plateformes ; par exemple, une application mobile est agnostique si elle est compatible avec iOS et Android. Ici, l'agnosticisme prend un sens plus proche de sa signification philosophique : les sociétés de conseils tenaient une position sceptique face à l'ensemble de ces solutions. Plutôt que trancher et risquer de ne pas avoir misé sur la bonne solution, elles cherchaient à les comparer pour traduire le concept abstrait de « blockchain » en « *proofs of concept* ». Ce travail de comparaison était lui-même objet de prestations de conseil, souvent associé à des présentations théoriques de la blockchain, en termes de bénéfices attendus ou comme une architecture informatique distribuée héritant de Bitcoin. Ces prestations étaient appelées « itérations » : elles visaient non seulement à former les clients mais aussi à préparer la prestation de conseil suivante, en identifiant des « cas d'usage » de la blockchain qui devaient correspondre (si possible) à des problèmes appelés « points de douleurs » (*pain points*) formulés dans ce processus « itératif » entre les consultants dépositaires de la connaissance sur « la technologie blockchain » et les clients indiquant où ils avaient « mal ».

Tu vois, quand tu vends ces projets tu as toujours une première phase 'ok on fait de l'itération, ça vous coûte 50 mille balles'. Ensuite 'on vous fait un premier proto[type], et ça vous coûte 200-300 mille'. Ensuite 'on essaie de passer le proto[type] en prod[uction], et ça vous coûte 3-4 millions'. Ça c'était la bonne vie du consultant en SSII¹³⁵, mais premium, version [cabinet de Jean] ou autre. (entretien avec Jean, novembre 2021)

Cet enrôlement par phases commerciales successives témoigne de la dynamique de conception à l'œuvre. Les sociétés de conseil problématisaient des relations numériques existantes (qui faisaient « mal ») et tentaient de « prouver » qu'elles pourraient

techniques, leurs visions politiques, économiques, sociales. Ces consortia sont tout à fait différents de ceux qui sont imaginés par l'utilisation d'Ethereum ou « utilisations B2B », résultats de la mise en place du logiciel développés par les premiers.

134 Mes informateurs d'autres cabinets utilisaient la même expression.

135 Acronyme de « société de services en ingénierie informatique », aussi appelées « entreprise de services du numérique ».

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

efficacement être re-formées avec Ethereum. Elles cherchaient à faire coïncider les cadres de ces grandes entreprises avec le script d'un utilisateur générique, en augmentant progressivement l'ampleur des expérimentations jusqu'à remplacer les relations telles qu'elles étaient formées et formulées dans les systèmes d'information en place. Cette dynamique était inverse à celle des startups qui, au contraire, enrôlaient leurs utilisateurs par la détention de jetons avant même que le dispositif de formulation d'utilisateurs spécifiques à ces applications existent (par un « jeton utilitaire », voir Chapitre 2). Au contraire, elle consistait à partir d'une technologie blockchain théorique, pensée comme un calque, une architecture informatique généralisable au travers duquel reproduire des relations existantes. Ces utilisateurs clients étaient « acculturés » à cette nouvelle manière de former les transactions. Le travail des sociétés de conseil était de leur « prouver » que la blockchain permettait de former différemment des relations qui étaient jusque-là « douloureuses ». Leur travail de conception de dispositifs de formulation consistait à inscrire l'utilisateur spécifique de ces clients, au plus proche de leurs relations existantes. Cette dynamique contrastait avec les DApps dont la construction supposait l'adhésion préalable des utilisateurs, c'est-à-dire préalablement intéressés¹³⁶.

Ce sont ainsi deux utilisateurs bien différents que projettent les utilisations d'Ethereum sur la plateforme publique des versions pour consortia. Ce décalage ne satisfaisait pas Jean. L'« agnosticisme » de sa société conduisait nécessairement à des missions d'acculturation d'ampleur limitée (« pas scalable ») en comparaison de l'ampleur de la « plateforme de *smart contracts* » et des utilisations B2C. L'utilisateur que cherchait à inscrire sa société était éloigné de celui qu'il imaginait lui : un portefeuille qui utilisait des *smart contracts* codés par les autres, un utilisateur autonome qui agissait dans un monde ouvert. En 2017, il rejoignait ConsenSys comme membre de la direction du tout premier bureau parisien. Jean se fait accompagner par différents collègues de l'équipe qu'il avait mise sur pied au sein du cabinet d'audit et de conseil, qu'il a convaincu que « le vrai truc » était dans Ethereum, pas dans une abstraite « technologie blockchain ». Chez ConsenSys, Jean avait quatre activités principales : il recrutait (ou négociait des plans de licenciement, selon les époques), il

¹³⁶ Le Chapitre 4 indique néanmoins que cette infrastructure supposée et ses modalités de formation des transactions sont parfois objets de controverses.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

participait à des comités de décisions internes au bureau de Paris ou en relation avec l'entreprise au niveau mondial, il formait les employés de ConsenSys en interne (par exemple comment faire tourner un nœud Ethereum, comment coder un *smart contract*), et il participait au « *business development* » autant auprès de clients B2B que de développeurs de DApps en B2C qui cherchaient à bénéficier d'un audit technique sur leur code (« diligence technique »).

Développer l'écosystème par l'infrastructure : transformer les briques en produits

La politique financière et commerciale de ConsenSys a évolué selon deux phases sur le temps de l'enquête. Cette chronologie distingue deux rapports de l'entreprise à l'enrôlement d'acteurs de l'écosystème. Une première phase tient dans l'expression « *startup venture studio* ». ConsenSys a été fondé par Joseph Lubin, un « multimillionnaire qui ne savait pas que faire de son argent » selon un informateur et ancien employé de la société. De 2015 à 2018, Joseph Lubin a injecté des millions de dollars dans cette pépinière de startups. Ces dernières avaient deux types d'objets : le développement des DApps, sinon le développement de logiciels d'infrastructure, permettant aux premières de développer des DApps¹³⁷. En entretien, Jean comparait le ConsenSys de cette époque à « un fonds ». Il estimait à plus de 100 le nombre de startups financées entre 2015 et 2019 ; un chiffre similaire à celui donné par Joseph Lubin à la Maison de la Mutualité et dans la presse. Selon Jean et *a posteriori*, seule « une poignée » de ces investissements ont acquis ce que Lubin désignait comme une « traction significative » (voir *supra*). C'était notamment le cas d'Infura qui, en 2021, gérait jusqu'à 10 milliards d'appels à la blockchain Ethereum par jour, du gestionnaire de *wallets* Metamask qui avait 1,2 millions d'utilisateurs.

Une deuxième phase commençait au moment de l'« hiver crypto » (« *crypto-winter* ») de 2018-9. Cette saison n'avait rien de météorologique ; la température avait plutôt à voir avec la valorisation marchande des cryptoactifs, qui ont connu une baisse généralisée après

¹³⁷ L'organisation de ConsenSys sera abordée à la section suivante de ce Chapitre ; les employés de ConsenSys appellent ces startups « *spokes* ».

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

l’emballée de 2017-8 liée au développement des ICO. Elle est marquée par un changement de politique d’entreprise¹³⁸. ConsenSys licenciait une partie importante de ses effectifs (Victor 2019) et cherchait à rendre rentables des logiciels qui, jusque-là, étaient développés « pour l’écosystème » sans générer de revenus directs, et publiés dans des licences autorisant la réutilisation du code source. Jusque-là, les investissements dans l’écosystème n’offraient pas de perspective précise de rentabilité : les startups développant des DApps n’avaient pas de comptes équilibrés, et les logiciels développés par ConsenSys devaient servir à ces startups. Jean m’expliquait en effet que les priorités des équipes de ConsenSys évoluaient en fonction des manques des startups incubées : lorsqu’une brique infrastructurelle manquait, les équipes commençaient par chercher un projet similaire dans l’écosystème et la communauté de développement. Si elles le trouvaient, elles y participaient, sinon, elles lançaient un projet *ad hoc*. Jean m’indiquait à ce propos que la culture de l’open source était vivante chez ConsenSys, les participations des employés à l’alimentation de dépôts (de code) publics étaient valorisées.

Les briques infrastructurelles à succès (notamment Truffle, Metamask, Infura ou Besu) étaient des logiciels développés durant la première phase pour instaurer l’espace transactionnel public (utilisations B2C) et qui ont été adaptés durant la deuxième d’enrôlement de plus grandes entreprises. Deux enrôlements ont eu lieu simultanément. D’une part, ces logiciels ont été assemblés pour bâtir des consortia. La suite de développement de *smart contracts* Truffle comme le gestionnaire de *wallets* Metamask étaient des outils de formulation des transactions. Ils étaient téléchargeables et utilisables gratuitement. La première permettait aux développeurs de coder les DApps, le second permettait aux porteurs de jetons de les utiliser. Infura et Besu étaient des outils de formation des transactions. Le premier permettait aux développeurs de gérer dynamiquement les transactions à acheminer vers la blockchain, en particulier de gérer le gas. Le second était un logiciel « client » d’administration des nœuds de réseaux privés pour utilisations B2B qui a été développé par PegaSys, une équipe de ConsenSys chargée

138 Selon différents informateurs, ce changement de politique est lié à la baisse du prix du bitcoin et de l’ether qui auraient diminué la valeur en dollars des actifs détenus par ConsenSys et par Joseph Lubin. Je n’ai pas eu accès à suffisamment d’éléments pour vérifier cette information (comme les comptes de ConsenSys).

de participer à la nouvelle version du protocole de consensus. En 2018, un New-yorkais de cette équipe animait un meetup à Paris sur les dernières évolutions du protocole d'Ethereum, la plus symbolique étant le passage du « *proof-of-work* » au « *proof-of-stake* »¹³⁹.

D'autre part, différents logiciels d'abord développés pour des utilisations gratuites dans la perspective de développement d'un « écosystème » entrepreneurial ont évolué vers des offres payantes ajustées pour enrôler de grandes entreprises dans le Web3 ou la DeFi. Les offres d'Infura et de Metamask visaient par exemple et respectivement à faire des entreprises des formatrices et des utilisatrices d'Ethereum public et de ses DApps. Infura+ était annoncée en 2019 pour compléter la version gratuite du service d' « *infrastructure-as-a-service* » (ConsenSys 2019e) avec différentes options de volume de transactions et de service client, pour accompagner les entreprises « de *proof-of-concept* jusqu'à la production globale » (ConsenSys 2019d). Metamask Institutional, annoncé fin 2020, visait à « permettre aux fonds en cryptomonnaies, aux gestionnaires de fortunes, et aux institutions financières d'accéder et d'être exposés aux différentes opportunités de la finance décentralisée qui compose le Web3 » (Adarme 2021) en câblant l'application Metamask aux circuits de dépositaires de cryptoactifs agissant soit comme intermédiaires financiers sinon comme gestionnaires pour le compte de ces « institutionnels ».

1.3. Faire converger des organisations économiques par l'infrastructure

ConsenSys promouvait une convergence entre l'infrastructure publique et les solutions de consortia construite sur la « technologie Ethereum ». Cette « convergence » était préparée par un assemblage de dispositifs de formation et de formulation susceptibles d'être utilisés indifféremment sur un réseau public ou privé. Cette vision apparaissait nettement quand ConsenSys enrôlait des entreprises comme utilisatrices (par ex. *via* Metamask Institutionnal) ou comme formatrices (par ex. *via* Infura+) du Web3 et de la DeFi. Cette sous-section montre qu'elle s'observait par le positionnement de ConsenSys dans une compétition entre sociétés financières et technologiques pour imposer un standard de

¹³⁹ Ce passage, appelé plus tard « The Merge », a eu lieu en septembre 2022.

marché de logiciel « client » de formation des transactions.

Vision : une économie unifiée par une infrastructure universelle

Jean m’expliquait que sa motivation pour participer à des projets utilisant Ethereum dans le cadre de ses missions de conseil tenaient à une vision : faire d’Ethereum une « vaste *settlement layer* », notion qu’il a entendue en 2016, lors de la conférence DevCon2. Cette couche infrastructurelle de « règlement », ou d’enregistrement des transactions, devait être une « nouvelle fondation de confiance » qui serait « automatique » plutôt que « subjective » (Tableau 11) pour Joseph Lubin, façon de dire la séparation entre formation et formulation des transactions.

| A Jean (public B2C), le 3 mars 2020 | A Kean (public B2B), le 2 mars 2020 |
|--|--|
| <p><i>We probably spend 60% or more of our attention on public main net things. And we use that exact same technology in private permission systems, and we built some some multi-million dollar production systems for projects like Kongo and another one, Covantis that's going to be just as big. But... all of that infrastructure, I guess our main focus is is public main net, and trying to bring the rest of the world in that direction [...] and so we think of that as <u>building a foundation of trust for the planet, moving the planet, from subjective trust to automated objective trust</u>. And what that enables is the building of <u>a new financial layer for the planet</u>. So, it's... open decentralized finance, it's the the money Legos, it's protocols essentially that will enable the world to rearchitect all of its systems, and draw legacy businesses and enable new businesses to essentially build at the <u>emerging decentralized economy</u>.</i></p> | <p><i>Ethereum and some other decentralized protocols are essentially enabling the world to have a new trust foundation, enabling us to <u>move systems from subjective trust to automated objective trust</u>. And so that's the base layer, that is currently Ethereum 1. And <u>on top of that, we're essentially building the financial plumbing, for the emerging decentralized economy</u>.</i></p> |

Tableau 11 : L’universalité de l’inscription comme fondement d’une nouvelle économie numérique

Face aux deux publics, Joseph Lubin esquissait l’universalité de l’enregistrement des transactions comme fondement d’une nouvelle économie numérique. Cette « couche de base » pouvait être construite autant comme plomberie financière avec la DeFi que dans des utilisations B2B ; il mentionnait le cas de Komgo, un consortium d’acteurs de la finance traditionnelle, et de Covantis, consortium du commerce international de céréales. Cette

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

convergence devait produire ce qui, selon Joseph Lubin, était nécessaire à une économie globale : une infrastructure qu'on n'imagine pas défaillir, c'est-à-dire libérée des aléas techniques ou politiques. Il désignait là un idéal universel, sous-tendant aussi bien la perspective d'un Web3 peuplé d'entités autonomes représentées par leurs *wallets* que d'entreprises qui échangeant de manière sûre et privée.

Cette convergence était possible grâce à une même manière de représenter les acteurs de l'économie numérique comme utilisateurs génériques. Le Tableau 12 met en regard deux manières de verbaliser cet universel en problématisant différemment le contrôle sur les relations : à gauche, le scepticisme quant à la capacité de l'État à assurer le nécessaire rôle d'infrastructure économique par la monnaie, et à droite, la nécessité d'une infrastructure économique qui respecte la confidentialité des transactions pour les entreprises.

| A Jean (public B2C), le 3 mars 2020 | A Kean (public B2B), le 2 mars 2020 |
|---|--|
| <p><i>I think so, if you look at nation states, and central banks and in their Treasury Departments, and how they issue bonds, because they can print as much money as they want. They can pretty much guarantee that they can pay off the bonds that they sell to financial institutions, or to people, and so, that's why it's called a risk free rate. But it's not really risk-free. Because nation states don't last forever, so I think what will be interesting is whether the risk-free rate in Japan, or the EU, or the United States, how that compares? Because a system of laws is basically a set of protocols, and if an ecosystem like Ethereum and a protocol like Ethereum gets really really big, global, incredibly well utilized, it'll be interesting to see if the risk-free rate of that protocol, of that set of rules is more risk-free than the risk-free rate of nation states, going forward.</i></p> | <p><i>Our client is actually gonna be able to enable a confidentiality overlay on Ethereum 1 public transactions, so that, uh, businesses will be able to transact in full confidentiality [...] we're actually gonna announce with two major companies, a new protocol, uh, to enable private information to be shared amongst counterparties, and private information and processes can be anchored into public main net Ethereum, so that they can track their work together in a fully confidential way. So with no leakage of information.</i></p> |

Tableau 12 : À chaque public sa problématisation du contrôle sur les relations

Différentes stratégies commerciales et financières traduisaient cette tentative de faire d'Ethereum une technologie universelle de formation et de formulation des transactions. Les paragraphes suivants montrent qu'elles s'insèrent dans des dynamiques de compétition

et d'alliance entre concurrents des secteurs technologique et financier, qu'elles se traduisent par la transformation de briques infrastructurelles en « produits » comme « plateformes » pour utilisations B2B, ou dans le cadre de mise en œuvre de « projets » qui s'appuient sur ces produits.

Compétition des « solutions blockchain »

L'histoire du logiciel « client » Besu informe sur les dynamiques de compétition et d'alliance dans lesquelles ConsenSys était engagée. Ce logiciel permettait d'administrer les nœuds physiques du réseau, c'est-à-dire de participer à la formation des transactions. À la manière du modèle d'affaire de RedHat, PegaSys vendait des prestations de mise en œuvre et d'assistance à la mise en place de réseaux B2B en s'appuyant sur ce logiciel. Besu était le nom qu'a pris le logiciel Pantheon en août 2019, un client écrit en Java et publié dans sa première version en février de la même année par PegaSys, après que ConsenSys contribue le code (ouvert) de Pantheon au consortium Hyperledger.

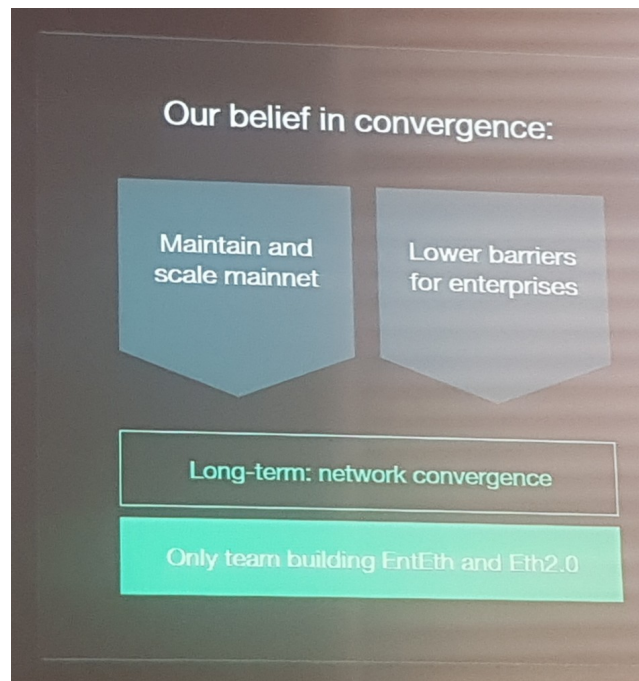


Figure 16 : Photographie de la représentation de la « convergence » entre B2B et B2C (meetup #18, mars 2020)

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

L'objectif affiché de ConsenSys était alors de faire converger le développement de réseaux B2B avec le réseau public Ethereum. Les responsables de PegaSys annonçaient eux-mêmes *via* le consortium Hyperledger que Besu devenait le premier logiciel d'Hyperledger compatible avec la blockchain publique Ethereum et conçu de manière modulaire, afin de pouvoir être réutilisé par d'autres logiciels clients développés par d'autres membres du consortium Hyperledger (Dawson & Baxter 2019), comme Fabric ou Sawtooth. C'était encore ce qu'affirmait ConsenSys et PegaSys à la Maison de la Mutualité, lors d'une présentation qui suit celle de Joseph Lubin dont est issue la Figure 16 qui présente la « convergence » entre réseaux B2C (à droite) et réseaux B2B (à gauche).

La contribution du code n'était pas anecdotique. Elle témoigne d'une stratégie d'extension d'Ethereum au-delà des utilisations B2C desquelles étaient largement absentes les grandes entreprises. En effet, ConsenSys ne proposait pas uniquement une nouvelle solution de formation des transactions aux membres du consortium Hyperledger qui regroupait nombre de grands représentants de la mise en place d'utilisations B2B de la « technologie blockchain ». En diffusant son logiciel, ConsenSys tentait d'imposer un langage de formation et de formulation des relations différent de ceux des autres fournisseurs de solutions blockchains, les *smart contracts*.

En effet et d'une part, ConsenSys intégrait la suite de développement Truffle au client Besu. À la différence de produits comme Metamask ou Infura qui visaient à faire des entreprises des utilisatrices et formulatrices du réseau public en facturant leur accès à ce réseau (voir *supra*), Truffle et Besu devenaient une suite logicielle pour que les développeurs forment les transactions (Besu) et les formulent (Truffle). D'autre part, et comme l'indique le Tableau 12 à droite, ConsenSys intégrait dans Besu (« *our client* ») une couche logicielle de confidentialité (appelée Orion) qui s'ajoutait au logiciel « client » d'Ethereum public pour crypter les transactions avant qu'elles soient inscrites. ConsenSys ajustait le script dans ces logiciels, faisant des grandes entreprises des utilisateurs imaginés, notamment en garantissant la confidentialité de leurs transactions. Ainsi, les transactions pourraient être formées et formulées par des objets techniques, dans un même langage, quels que soient les utilisateurs (B2B et B2C).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Le projet Ubin de la banque centrale de Singapour (MAS) est un cas élatant de mise en scène de cette compétition technologique entre « solutions blockchain ». Il montre qu'elle n'est pas uniquement produite dans les *power points* des consultants qui les comparaient pour des missions d'acculturation. L'institution a structuré son expérimentation en deux phases, chacune pilotée par un cabinet de conseil, Deloitte puis Accenture. Elles devaient évaluer les forces et les faiblesses de trois solutions, à partir d'expérimentations conduites par des binômes constitués d'une banque de la place financière de Singapour et d'une société de développement de logiciel, chacune garante de l'évaluation d'une solution parmi trois possibles : Hyperledger Fabric, Quorum et Corda. Ces trois solutions répondaient à une même problématisation des réseaux informationnels (ou un même « point de douleur ») : le réseau inter-bancaire d'argent de banque centrale devait être rendu plus efficace et plus sûr. Les référents technologiques de ces expérimentations étaient respectivement IBM, ConsenSys et R3.

Du projet Ubin jusqu'aux prises de parole de Joseph Lubin à la Maison de la Mutualité, le développement de logiciels « clients » révélait des convergences industrielles, de coopérations de circonstances jusqu'aux structures comptables des sociétés impliquées. Depuis le projet Ubin au moins, ConsenSys travaillait avec l'Étatsunienne JP Morgan Chase. Dès 2015, la plus grande banque privée au monde en termes de taille de bilan a mis sur pied l'équipe de développement de Quorum, une des trois solutions évaluées par la banque centrale de Singapour qui avait la particularité d'être construite à partir du code d'Ethereum, dans le langage Go. Avec ConsenSys et des dizaines d'autres sociétés, JP Morgan a fondé un consortium appelé *Ethereum Enterprise Alliance* en 2016, qui se donnait pour mission de construire les logiciels nécessaires à une adoption large d'Ethereum par les entreprises. Début 2020, Joseph Lubin analysait le rôle de JP Morgan comme un frein vis-à-vis des autres acteurs susceptibles de construire des réseaux B2B avec Ethereum :

*Joseph Lubin: [JP Morgan] want people to use the Quorum technology, they want people to use their systems, but I think **there's been been some resistance amongst other financial institutions** and just other kinds of institutions, to make use of this technology that's effectively owned by a big bank, and so, **they decided that they***

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

*wanted to externalize that project, and they've been looking at different groups, they've been talking to different groups about who would take on that project, and... we are now in deep discussions with them*¹⁴⁰.

Jean: Yes so it seems like ConsenSys is poised to be the one that will bring the balance to the finance world?

*Joseph Lubin: "So, bring balance I would say bring... integration. **The vision has always been to move the world from top-down command and control**, centralized systems, subjective trust systems, to automated objective trust, on massively decentralized protocols. **It started out, with enterprise needing to do its own thing, in more circumscribed private systems**, that's the way enterprise adopted the web technologies too.*

(discussion entre Joseph Lubin et Jean à EthCC, Maison de la Mutualité, mars 2020)

Six mois après cette déclaration, JP Morgan investissait dans ConsenSys tout en lui cédant Quorum. La banque cherchait à s'assurer que la technologisation d'Ethereum continuerait et devienne un standard¹⁴¹. La banque s'appuyait en effet sur Quorum pour son JPM Coin, un projet de monnaie bancaire privée appelé Onyx en 2021. Dans le même temps, la banque était chargée par ConsenSys d'organiser une levée de fonds auprès d'investisseurs venant à la fois des secteurs technologiques et financiers traditionnels (JP Morgan elle-même, mais aussi et par exemple Mastercard et UBS) que du Web3 et de la finance décentralisée (ConsenSys 2021a). À cette occasion, ConsenSys leva 65 millions de dollars en actions convertibles, signe que la société cherchait à augmenter sa capitalisation financière et à obtenir une valorisation de marché¹⁴². Cette ouverture coïncidait avec le début de la deuxième phase indiquée à la section 1.2, ou un passage du « financement d'un écosystème » à la recherche d'un modèle économique pour ConsenSys. Dès 2019, ConsenSys cherchait des capitaux et licenciat 13 % de son personnel (Victor 2019), puis

140 Ces négociations entre ConsenSys et JP Morgan ont été annoncées dans la presse spécialisée quelques semaines auparavant (Irrera 2020).

141 Ce que dit Joseph Lubin ci-dessus, mais aussi la presse spécialisée (Maffock 2020).

142 Les actions convertibles sont des contrats qui associent à un titre financier une option de transformation de ce titre sous certaines circonstances. Dans le financement de startups, les convertibles sont utilisés lorsque la startup n'a pas de valorisation estimée comme fiable ou stable. Les convertibles sont au départ des obligations, permettant aux investisseurs, à court terme, de garantir des intérêts (comme des prêts), puis susceptibles d'être transformées en actions une fois que la startup aura été valorisée (typiquement, après plusieurs levées de fonds).

14 % en février 2020 et de nouveau en avril (Quittner 2020) réduisant de 900 à tout juste 600 le nombre de ses employés en un an. Quelques mois plus tard suivaient de nouvelles levées de fonds, et ConsenSys affichait sa valorisation (3,2 milliards de dollars fin 2021) au gré des nouveaux cycles de financements (voir par exemple ConsenSys 2021b).

Construire une « full stack » en intégrant les briques en produits

ConsenSys jouait un rôle « d'intégrateur » selon Lubin qui se voyait en diffuseur d'Ethereum auprès d'entreprises dans des réseaux privés, première étape d'une convergence annoncée. C'était aussi comme « intégration » que Hughes décrit les innovations successives des concepteurs des réseaux électriques ; elles passent par exemple par des dispositifs techniques aux usines de production, comme le convertisseur rotatif, « élément de couplage des sous-systèmes dans l'édification des systèmes » (Hughes 1983b : 30). Mais ici, le « tout cohérent » que cherche à créer Joseph Lubin n'était pas le réseau lui-même, mais un ensemble de produits technologiques qu'il pourrait vendre à de grandes entreprises pour transformer leurs systèmes d'information. En 2021, la page d'accueil de ConsenSys avait pour titre « *The Most Trusted Ethereum Blockchain Solutions* ». Comme le montre la Figure 17, les indicateurs mis en avant par ConsenSys amalgament les produits *a priori* destinés à des utilisations B2C (comme le nombre d'utilisateurs actifs de Metamask) et d'autres destinés à des utilisations B2B (nombre de clients et partenaires, ou le nombre de téléchargements du client Besu). »

Les « produits » issus des « briques » (voir *supra*, 1.2) étaient intégrés dans une « pile » logicielle (« *a full stack* » ; voir *supra*, 1.1), allant de ce que les informaticiens appellent les couches les plus « basses » (infrastructure matérielle, administrée par le logiciel « client » comme Besu ou Pantheon) aux couches les plus « hautes » (en contact direct avec l'utilisateur « final »). Cette pile, en développement continu au moment de l'enquête, est représentée sur la Figure 17. Les produits de ConsenSys étaient assemblés par usages pour les développeurs, de la formation des transactions et la mise en place des réseaux (en bas) aussi bien pour des usages B2C (à gauche, avec Infura) que pour des usages B2B (à droite),

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

à la formulation des relations commerciales et financières en haut (la suite Codefi) par les clients de ConsenSys, en passant par les outils de développement de *smart contracts* (comme Truffle).

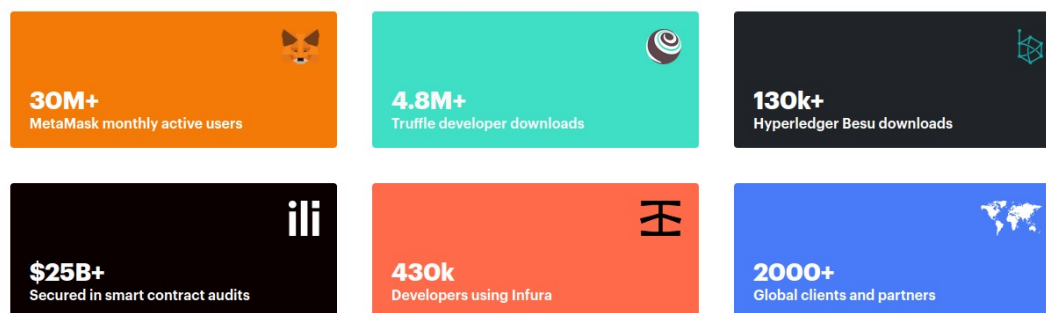


Figure 17 : Indicateurs marketing qui assimilent utilisations B2C et B2C

Avec cette pile, ConsenSys équipait ses prestations de conseil d'un ensemble d'outils reconnaissables par ses clients et prospects tout en formant des développeurs à leur utilisation, objet du meetup durant lequel la photo reproduite en Figure 3 a été prise. La politique d'entreprise de ConsenSys était intimement associée au développement d'Ethereum comme une technologie. Cette stratégie tranchait avec celle des sociétés de conseils « agnostiques », bien que le modèle de revenu de ConsenSys vis-à-vis de ses clients « entreprises » ressemble aux leurs : comme elles, ConsenSys parlait de *proofs-of-concept* avant d'envisager une mise en production¹⁴³. Mais avec ConsenSys, la « technologie blockchain » était Ethereum. Le concept de blockchain n'était pas abstrait : la « preuve du concept » était équipée par des produits, qu'elle se vantait de maîtriser car les ayant elle-même développés, et intégrés à ses prestations. Fin 2018 déjà, c'est-à-dire à la fin de ce que j'ai qualifié de « première phase » de ConsenSys, Adèle et Cécile (deux employées de ConsenSys, voir Chapitre 2, section 2) m'indiquaient que le bureau parisien privilégiait largement des solutions technologiques basées sur Ethereum (Quorum, puis Besu), bien qu'il ne fût pas tout à fait exclu d'accompagner des clients réclamant une autre solution.

¹⁴³ Voir par exemple le vocabulaire des responsables de PegaSys (2019).

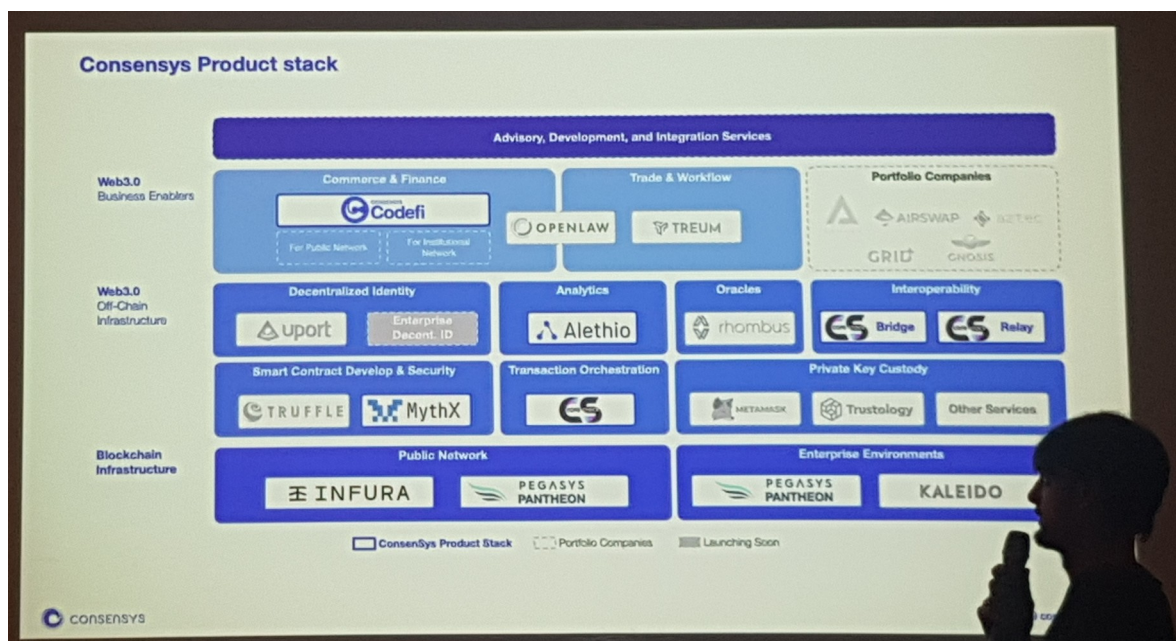


Figure 18 : Représentation de la « full stack » durant le meetup #16 (septembre 2019)

Ce gnosticisme se traduisait en pratique par des équipes spécialisées dans le développement d'un (ensemble de) produits mobilisables pour la construction d'infrastructures destinées à des usages B2B comme B2C. C'est le cas de PegaSys pour le développement d'un logiciel « client », cela a été mentionné. C'est aussi le cas pour des utilisations financières avec Codefi, équipe qui développe une suite d'offres de services dite « *The Blockchain Application Suite for Commerce and Finance* ». La page Web de Codefi faisait apparaître de nombreuses références d'entreprises dans une section « *Powering Leading Organisations* », aussi bien associées à des utilisations B2C que B2B¹⁴⁴. La suite de services annoncés de Codefi était très large, et visait à garantir à ses futurs clients que l'ensemble de la « solution » blockchain pourrait être « intégrée » par ConsenSys. Parmi ses neuf modules¹⁴⁵, Assets et Activate symbolisaient la convergence des utilisations B2B et

144 Pêle-mêle : AAVE, Mata Capital, Covantis, Société Générale, Maker, Metamask, SKALE, Ethereum Foundation, Protocol Labs, CPA Global.

145 Ces neuf modules étaient nommés (et désignait, dans le vocabulaire de ConsenSys) : Orchestrate (éléments « techniques » décrits comme universaux pour toute « solution blockchain d'entreprise »), Worflow (gestion des « process métiers » avec la blockchain), Assets (tokenization, émission et cycle de vie des actifs numériques), Markets (swaps de monnaies numériques de pair-à-pair), Payments (règlement de monnaies numériques pour banques centrales et stablecoins), Activate (outils de lancement et de participation de réseaux et protocoles décentralisés), Staking (proof-of-stake pour clients institutionnels),

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

B2C. Assets était un module de gestion, d'achat, de comptabilité, de jetons, notamment des jetons utilitaires rencontrés au Chapitre 2 et étendards des utilisations B2C d'Ethereum. Activate était présenté comme une plateforme de conception de jetons, d' « activation » des « réseaux décentralisés ». Des employés détaillaient l'offre de service aux clients et prospects de ConsenSys à la Maison de la Mutualité, lors d'un des ateliers organisés immédiatement après la conférence de Joseph Lubin. Un an plus tard, les services de Codefi devenaient englobés dans un ensemble appelé « *DeFi for Institutions* », incluant également des pages web dédiées, des canaux de communications spécifiques (notamment, la constitution de mailing-list à partir des inscriptions spontanées ou des listings obtenus à partir des inscriptions à différents événements), l'organisation de conférences ou de formations sur les thèmes d'actualité croisant DeFi et préoccupations des entreprises.

Enfin, l'intégration des briques à disposition d'un écosystème en « produits » de la « pile » de ConsenSys passait par des changements de statuts juridiques visant à renforcer le contrôle de la société sur ces éléments d'infrastructure. Ces changements transformaient la signification des investissements initiaux de ConsenSys. Au départ, ConsenSys agissait comme un « fonds » pour le développement de l'écosystème. Dans un second temps, les produits valorisés pour leur large utilisation B2C étaient transformés en actifs, selon différentes modalités, mais participant à une même idée du futur : une économie unifiée par une même infrastructure, étendue en intéressant des entreprises qui en étaient *a priori* éloignées par la mise à disposition de la technologie comme un produit accessible *via* des prestations de conseil.

Deux cas de changements de statuts juridiques peuvent être distingués. D'une part, le changement de licences logicielles. La licence de type MIT de Metamask est devenue propriétaire pour conditionner toute réutilisation commerciale du code dépassant les 10 000 utilisateurs à un contrat de développement. Ce changement visait selon son dirigeant à assurer des revenus à l'équipe de développement pour poursuivre le développement du gestionnaire de *wallet* le plus utilisé dans l'écosystème Ethereum (Finlay 2020). Il a généré

Compliance (conformité anti-blanchiment et contre le financement du terrorisme pour les actifs créés sur Ethereum), Data (données de risque et d'analyse pour les actifs et protocoles de la DeFi).

des débats classiques des communautés *open source*, autour de l'articulation entre développement communautaire et rémunération d'un travail, remarqués par la presse spécialisée (De La Roche 2020)¹⁴⁶. D'autre part, ConsenSys prenait des parts dans les sociétés qu'elle avait participé à fonder. Truffle et Infura étaient deux startups qui avaient été incubées par ConsenSys. En 2019, Infura annonçait et décrivait son acquisition par ConsenSys comme un geste continu, d'une propriété « partagée » devenant « pleine » (Infura 2019). En 2020, ConsenSys annonçait l'acquisition de Truffle pour poursuivre le développement d'utilisations B2B. La suite logicielle avait déjà intégré le client Quorum, son nouveau patron cherchait alors à faire communiquer l'équipe de développement avec d'autres produits ConsenSys (dont Infura) de manière à faire de Truffle une suite de développement complète pour les développeurs des entreprises clientes de ConsenSys.

Conclusion de la section : conception d'une convergence infrastructurelle de l'économie numérique

La vision d'une « *global settlement layer* » et d'une organisation économique mondiale par le « *system builder* » ConsenSys passait par la construction d'un écosystème constitué d'acteurs hétérogènes : tous étaient imaginés comme formulateurs malgré des appartenances à des organisations économiques différentes. Cette convergence stratégique passait par deux tactiques. Toutes deux faisaient de ces différents acteurs économiques, dans la conception des dispositifs de formation et de formulation des transactions, des utilisateurs génériques d'une même technologie tout en laissant la possibilité de spécifier ces utilisations en fonction des usages (formulation) comme des vellétés de contrôle sur les inscriptions (formation).

D'une part, les entreprises *a priori* étrangères au Web3 étaient inscrites dans les dispositifs de formulation des transactions sur la « plateforme de DApp », à la fois comme utilisatrices et comme formulatrices, notamment de la DeFi. Elles devenaient ainsi de possibles actrices

146 Un an plus tard, au moment de l'investissement (minoritaire) de JP Morgan dans ConsenSys, les dirigeants de Metamask affirmaient que le changement de licence garantissait l'indépendance de Metamask, toujours au service de l'écosystème (Metamask 2021).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

du Web3 par des briques infrastructurelles ajustées, au départ développés pour l'écosystème de startups. D'autre part, ces entreprises étaient inscrites simultanément dans les dispositifs de formation et de formulation des transactions pour constituer des consortia. Ces derniers reproduisaient les organisations de ces acteurs à partir d'usages déjà existants (points de douleur), ce que j'ai appelé « technologisation ». Sans perspective historique, cet enrôlement paraît se détourner de la vision de long terme ; les entreprises pouvaient en effet gérer leurs relations entre elles, sans rejoindre une seule et même infrastructure « mondiale ».

Pourtant, la stratégie de ConsenSys participait à instaurer les *smart contracts* comme un langage universel de formulation des relations numériques : ils devenaient utilisés aussi bien pour les DApps que par les entreprises réunies en consortia. La gouvernance par l'infrastructure était ainsi rendue modulable pour des acteurs qui codaient les relations dans un même langage. ConsenSys poursuivait ce que Hughes désigne comme une exigence de « systématisme » (Hughes 1983b : 22, 23, 24, 25, 29, 36, 41) des « *system builders* ». Hughes explique leur succès par les ajustements de composants d'un système comme résultat de leur intelligence, leur inventivité, leur habileté qui leur fait voir dans le système un « tout cohérent » (Hughes 1983b : 22, 33, 41). Ici, le « transfert » qu'opère ConsenSys est de l'ordre de la continuité plutôt que de la rupture : continuité langagière entre différents formulateurs et continuité dans le contrôle que les acteurs en présence exercent sur les relations.

Ainsi, ConsenSys peut être vu comme « constructeur d'écosystème », par analogie avec « constructeur de systèmes » de Hughes. Cette expression a été employée par Plantin et ses coauteurs (2016) :

In all cases, scholars of infrastructure could attend to the technological influences and policy alternatives that tip the delicate balance between the public interest and corporate power. It would recover the goal of comparative analysis that is often missing from some accounts of single platforms. It would recognize that the “system builders” that dominated infrastructures of the past may be replaced by “ecosystem-builders” that leverage programmability and interconnection to achieve control, rather than relying on direct provision and expansion. (Plantin et

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

al. 2016 : 15)

Mais ici, ConsenSys ne cherchait pas à « obtenir le contrôle » (sur l'infrastructure, ou l'écosystème), plutôt à développer en même temps l'infrastructure et l'écosystème. Cette vision n'était pas seulement discursive : elle était ancrée dans une politique d'entreprise et des stratégies commerciales élaborées dans le processus de conception lui-même, depuis la fondation de l'entreprise en 2015. Un informateur m'indiquait que Joseph Lubin aurait au départ imaginé Ethereum comme une société développant des DApps, alors qu'il participait à son lancement aux côtés de Vitalik Buterin. Pour des raisons qui seront abordées dans le Chapitre 4, le modèle d'une plateforme de *smart contracts* complètement open source a été privilégiée, laissant à Lubin la possibilité d'investir dans des startups regroupées en « *startups venture studio* » autour d'un protocole *open source*, le conduisant à orienter son travail entrepreneurial de développement de l'écosystème.

Quelles que soient les motivations de ces constructeurs de systèmes et d'écosystème, et sans présager de l'avenir d'Ethereum dont le succès est quotidiennement mis à l'épreuve de son développement au moment de l'écriture de ces lignes, la vision « cohérente » de ConsenSys rendait au moins théoriquement inter-opérables des infrastructures aux modalités de gouvernance économiques différentes. Autrement dit, l'usage généralisé des *smart contracts* pour la formulation des transactions et les passerelles permises par les logiciels de formation des transactions du réseau public et des réseaux privés rendaient possible le développement d'un « réseau des réseaux » transactionnels unifiant espaces transactionnels privés et espace transactionnel public.

2. L'écosystème en action : les transactions, opérations duales des plateformes

L'écosystème était l'ensemble des acteurs participant à la conception de plateformes utilisant Ethereum. Cette section donne deux points de vue sur l'écosystème : depuis des meetups organisés par ConsenSys, et depuis le processus de conception d'une plateforme par un intrapreneur au sein d'Orange. La première sous-section indique l'intrication entre l'écosystème et la notion de plateforme, qui était également un horizon organisationnel partagé par les acteurs le constituant. La seconde sous-section analyse le cadrage de la conception du service LeVote d'Orange comme prescription d'un utilisateur mêlant utilisateur générique d'Ethereum et citoyen imaginé par les concepteurs. La troisième sous-section analyse l'échec de la mise en œuvre commerciale du service comme une incompatibilité entre deux formes scripturales ayant chacune leur politique : d'une part, la plateforme imaginée par les concepteurs, et de l'autre, les scrutins en France.

2.1. L'écosystème, réseau de concepteurs de plateformes

Cette sous-section commence par préciser le rapport particulier entre les membres de l'écosystème et la notion de plateforme : une manière de penser l'organisation des sociétés et condition de sa propre existence. Puis, deux ensembles de réflexions des concepteurs sont abordées. Premièrement pour les relations de travail, la métaphore de l'écosystème agissait comme un modèle (incarnée dans l'organisation « opale ») qui supposait l'autonomie du travailleur, qu'il soit salarié ou indépendant. Cette vision libérale du rapport au travail était incarnée par des plateformes présentées comme traductions pratiques de ce modèle. Les nuances de gouvernance des relations par la formation (architecture client-serveur traditionnelle contre DApp) étaient finalement secondaires par rapport au modèle général de la plateforme qui faisait l'unanimité. Deuxièmement, les acteurs de l'écosystème voyaient leurs compétences de conception de plateforme en termes générique : former ou formuler les relations pouvait indistinctement être mis au service de DApps et du Web3 que

pour des consortia. Dans ces deux cas, la formulation des relations par la plateforme était une manière générale d'envisager la formation du lien social.

Polysémie de « plateforme » : support d'un écosystème et objets de conception

Généralement, l'écosystème était un ensemble de concepteurs de services qui avaient en commun de formuler les relations numériques par des plateformes. Je n'ai jamais observé de définition plus nette de cet ensemble. « L'écosystème » sans épithète désignait les concepteurs de services sur le *mainnet* (infrastructure publique). À d'autres occasions, il désignait les entreprises et institutions qui construisaient des « projets » ou consortia ; il était alors plutôt question de « l'écosystème blockchain ». Dans tous les cas, l'écosystème était un objet de développement, pensé au futur : il devait advenir. La technologisation de l'infrastructure décrite à la section précédente rend compte d'une extension des pratiques de développement d'une plateforme unique (le *mainnet* ou simplement « Ethereum ») à différentes plateformes (consortia). La constitution d'un écosystème de formulateurs des relations numériques allait de pair avec ce processus : ConsenSys équipait des développeurs et des entreprises chargés de formuler les relations numériques en diffusant des pratiques de développement communes, notamment par la circulation de briques et de produits technologiques ; les sociétés de conseil formaient et « prouvaient » la technologie avec des entreprises.

Sous cet angle, l'écosystème désignait des acteurs divers qui, ensemble, construisaient des services avec Ethereum. Le terme résonne avec « écosystème d'affaires », notion d'abord apparue sous la plume du consultant James Moore dans la *Harvard Business Review* pour désigner des ensembles d'entreprises à la fois en situation de coopération et de compétition dans la production de nouveaux produits ou en réponse à la satisfaction de besoins de clients (Moore 1993). Des travaux en sciences de gestion ont discuté la portée analytique de ce concept qui déplace l'attention de la forme entreprise inscrite dans un secteur à une entité appartenant à un ensemble en réseau (Daidj 2011 ; Fréry et al. 2012). Transposition du concept d'écosystème biologique inventé par Arthur Tansley en 1935, ce concept est

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

bâti, dans son sens minimal, sur une analogie qui suggère une situation dans laquelle des entreprises sont en situation d'interdépendance (Fréry et al. 2012 : 72). Ces travaux ont comparé le concept « écosystème d'affaires » à d'autres formes d'organisations entrepreneuriales en réseau, comme l'industrie, le cluster ou le réseau de valeur.

Ces auteurs voient dans les plateformes numériques l'aspect le plus novateur de l'organisation en écosystème. Pour ces chercheurs, les plateformes technologiques permettent « d'analyser la transformation progressive des formes d'organisation en réseau jusqu'à l'émergence des écosystèmes » (Daidj 2011 : 123-4). Elles sont mises en place par des entreprises dites « pivots », qui n'ont pas pour objectif de contrôler l'ensemble de l'écosystème, mais plutôt « par leur vision et leurs capacités relationnelles, de mettre sur pied un nouveau réseau de valeur [et elles] captent une part importante de cette même valeur » (Ronteau 2009, cité par : Daidj 2011). Ces entreprises utilisent les plateformes comme des « stratégies » pour bénéficier des apports d'autres acteurs de l'écosystème.

ConsenSys endossait un rôle d'entreprise pivot. À Singapour, ConsenSys fédérait différents entrepreneurs qui concevaient des DApps et jetons (Chapitre 2) ; plus tard et comme indiqué à la section précédente, ConsenSys créait de nouveaux réseaux en technologisant l'infrastructure d'Ethereum. Les meetups matérialisaient cette mise en réseau : ils réunissaient des entrepreneurs et des développeurs qui travaillaient en commun à faire advenir un Web3 ou une finance décentralisée. Ils étaient organisés par ConsenSys aux côtés d'autres organisations qui fédéraient l'écosystème, comme Ethereum France, présidée par Jean, ou la ChainTech, une association professionnelle agissant comme chambre de commerce française des startups et des entreprises des cryptoactifs et de la blockchain.

Mais avec Ethereum, le rapport entre « plateformes numériques » et « écosystème » prenait deux sens qui apparaissent nettement avec les utilisations B2C. D'une part, Ethereum était effectivement « une » plateforme d'applications décentralisées et de ses jetons, support de l'écosystème. Sans elle, ce dernier n'aurait aucune raison d'être. D'autre part, la plateforme était l'horizon organisationnel de cet écosystème. Les applications décentralisées étaient conçues par les acteurs de l'écosystème comme des plateformes, ou espaces de mise en

relation d'offreurs et de demandeurs de services au moyen de jetons ; pensons par exemple aux cas de Digix ou Bluzelle (voir Chapitre 2, section 1). Ils imaginaient une économie numérique constituée d'autant de plateformes que de relations incarnées dans les jetons. Autrement dit, les concepteurs n'étaient pas seulement des acteurs économiques organisés en écosystème autour d'une plateforme de DApp ; ils étaient également des concepteurs de dispositifs marchands qu'ils concevaient comme des plateformes.

Figure du concepteur de DApps : travailleur autonome en « organisation décentralisée »

Les meetups étaient des occasions pour les concepteurs de plateformes de formuler publiquement les bonnes manières de s'organiser et de travailler. Cette question était abordée de front durant le meetup #4 (novembre 2018) intitulé « *Future of Work : What about yours ?* »¹⁴⁷. Agueda, employée chez ConsenSys, avait la parole pour le premier temps de ce meetup. Elle présentait le modèle d'organisation promu dans un de « ses livres préférés », l'ouvrage « *Reinventing Organizations. A Guide to Creating Organizations Inspired by the Next Stage of Human Consciousness* » de Frédéric Laloux¹⁴⁸ (2014). Ce modèle, appelé « teal » pour « bleu canard » en anglais, traduit en « opale » dans la version française (Laloux 2016), était présenté comme le dernier « paradigme » d'une lignée de formes d'organisation des sociétés humaines qui aurait commencé avec le modèle « rouge ». Selon ce dernier, le travail était divisé et dirigé par un dirigeant puissant faisant régner la peur. Agueda expliquait que chaque modèle, désigné par une couleur (et reproduits sur une diapositive, Figure 19), avait un « problème » intrinsèque conduisant à l'« émergence » d'un nouveau modèle. Le changement était ici naturalisé plutôt que théorisé ; pas d'organisation particulière provoquant ces bouleversements à la manière de la

147 La notion de « *Future of Work* » est reprise d'une série de travaux de McKinsey qui explorent « le futur du travail ». Les organisateurs de ConsenSys listaient quatre grands enjeux sur la page du site meetup.com annonçant l'événement : « un nouvel âge d'automatisation avec la progression de l'intelligence artificielle et de la robotique, l'exploration de nouveaux modèles organisationnels, la gestion du revenu de base, et l'évolution des sites de travail ». L'objectif du meetup était : « discuter les modèles en train de changer et comment ils impactent les gens et la productivité ».

148 Frédéric Laloux est belge, ingénieur de formation, coach en stratégie d'entreprise à l'écriture de ces lignes. Le titre de l'ouvrage, traduit en français, est « *Reinventing Organizations : Vers des communautés de travail inspirées* ».

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

« science extraordinaire » pour les révolutions scientifiques (Kuhn 1983). Les organisations rouges étaient intrinsèquement instables par manque d'objectifs de long terme, faisant émerger les organisations jaunes stables en raison du contrôle exercé par une hiérarchie. Incapables de s'adapter précisément en raison de cette stabilité, les organisations oranges auraient émergé en déclinant la notion de compétition au sein même de l'organisation, stimulant la recherche du profit financier, et par conséquent promouvant l'innovation par la méritocratie. Toujours selon Agueda, les organisations vertes ont émergé en instaurant des valeurs partagées auxquelles étaient soumis les objectifs communs et dont étaient dépourvues les organisations oranges seulement orientées par le profit financier, de manière à l'équilibrer avec la satisfaction des consommateurs et des employés (on parle alors d' « engagement »).



Figure 19 : Diapositive d'Agueda présentant les différents modèles organisationnels dans Laloux (2016)

Les organisations opales étaient appelées « organisations décentralisées ». Les orateurs de ce meetup filaient la métaphore de l'écosystème pour les désigner, par contraste avec les

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

métaphores de la tribu, de la hiérarchie, de la machinerie et de la famille pour les organisations rouges, jaunes, oranges et vertes respectivement. Elles suivaient un « processus évolutionnaire », elles étaient « anti-fragiles » (même qualificatif que celui employé par Jean pour dire son intérêt pour Ethereum, voir *supra*). Le second temps du meetup donnait la parole à des entrepreneurs qui partageaient leurs visions sur l'organisation du travail. La distribution du pouvoir de décision à tous les individus était particulièrement promue par les intervenants : comme les cellules ou les êtres d'un écosystème, l'individualité propre s'exprimait naturellement dans les relations avec les autres, selon un mécanisme de consensus.

Un porte-parole de la startup Talent.io¹⁴⁹, qui décrivait l'ouvrage de Laloux comme sa « bible », défendait l'idée de « propriété de la décision » (*ownership*) aux membres d'une entreprise : chacun devrait être en capacité de créer une offre, un produit, un événement, d'acheter des fournitures. Chacun devrait alors confronter son initiative à « chaque personne qui pourrait être impactée » pour totaliser, individuellement, « toute l'information nécessaire ». Une porte-parole de la startup Briq¹⁵⁰ abondait : c'est en montrant de la « gratitude » à ses collègues en toute circonstance (y compris « quand on est débordé »), en rendant l'atmosphère « fun », qu'il serait possible de créer un « équilibre » entre deux objectifs : investir l'individu d'un « objectif global » et étendre à chacun les missions d'organisation d'événements comme de lancement d'un nouveau projet. Les liens de reconnaissance mutuelle et de prise de décision pourraient selon elle être matérialisés par des jetons, susceptibles d'objectiver un « alignement » interne à l'entreprise.

*You have to accept that **you will not control** everything. This is **something between you and you**.* (représentant de Talent.io, meetup #4, novembre 2018)

*The breakthrough idea [...] is the wholeness : this idea you can bring to your job, wherever you are, **all the facets of you**. You can be safe, nobody is gonna judge. So if you're a spiritual, if you're a real yogi, or a super mathematician... All the types, all the different personalities you have. Like you can come one day and*

149 Talent.io était une startup proposant une plateforme numérique de mise en relation de travailleurs et de recruteurs.

150 Briq était une startup proposant une plateforme numérique offrant aux entreprises de construction un ensemble d'outils pour gérer leurs flux financiers et matériels.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

being away, your all self is gonna be welcome and nobody is gonna judge you.
(Agueda, meetup #4, novembre 2018)

La métaphore des organisations comme écosystèmes projetait un individu autonome dans une « totalité » qu'il était inutile de chercher à « contrôler » et qui ne « jugeait » pas. Cette idée du rapport individuel au groupe (de travail) organisé apparaissait aussi nettement dans le troisième temps du même meetup, dédié à la promotion du travail indépendant (« *freelancing* », ou travail « autonome » au Québec). Christophe, était le représentant de la startup Comet, une plateforme de mise en relation et de contractualisation entre employeurs et travailleurs indépendants dans le domaine des technologies numériques et des données. Alors que le premier participait à développer le travail indépendant au sein de grandes entreprises¹⁵¹, Sofia représentait une autre forme de travail indépendant : le travail à la tâche. The Bounties Network (TBN) permettait à quiconque de faire se rencontrer des demandeurs et offreurs de réalisation d'une tâche (comme traduire un texte, rechercher une information, écrire du code, ou réaliser un visuel) sur un prix et un cahier des charges déclenchant le paiement. Un « *bounty* » désigne une rémunération offerte à un individu ou à une organisation pour accomplir une tâche spécifique.

Ces deux plateformes envisageaient le travail dans les termes de contrats fixés dans le cadre d'une rencontre marchande entre des offreurs et des demandeurs. La relation devait être à la fois « flexible » et « inclusive ». Différents orateurs du meetup aimaient raconter combien il était libérateur de travailler pour ce qu'on veut, quand on veut, et d'où on veut. Sofia expliquait par exemple qu'elle voyait là un moyen de concilier un boulot quotidien avec des envies temporaires, comme travailler pour une cause qui a un « objectif plus élevé », social ou écologique. Pour Christophe, le travail indépendant succédait au travail dans les usines : avec les startups, les gens ne cherchaient plus à travailler pour une entreprise, mais étaient à la recherche d'« expériences ». Ce rapport individuel au travail était également promu comme inclusif : le travail autonome était imaginé comme un « accès à la table économique mondiale pour tous », notamment pour les travailleurs habitant hors d'Europe ou

151 En 2022, Comet donnait comme exemple de clients la filiale « Digital » du constructeur automobile Renault, la plateforme de streaming de musique Deezer, ou le groupe de grande distribution Les Mousquetaires (Intermarché).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

d'Amérique du Nord : une « collaboration 2.0 ».

Ces deux cas illustrent que la forme « plateforme » recoupe différentes manières de gouverner les relations numériques, pourtant distinctes en termes de ce que j'ai appelé formation en introduction. Dans les deux cas, ces plateformes permettaient de formuler des relations de travail. De manière en apparence assez similaire à une plateforme comme Airbnb, offreurs et demandeurs de travail se rencontraient et formaient une relation monétisée nouée par la plateforme. Pourtant, les significations données à la « transparence » clamée par ces deux plateformes montrent différentes manières d'envisager l'organisation économique. Pour Christophe, la plateforme Comet se substituait à toute forme d'intermédiaire en annonçant à l'avance le montant de la commission (un pourcentage prélevé sur les revenus du travailleur et sur les paiements de l'employeur) : la transparence était parfaite information des parties, et la plateforme agissait comme un arbitre neutre, dont la rémunération était connue à l'avance. Pour Sofia et TBN, la transparence se comprenait comme indépendance des gestionnaires de la plateforme elle-même qui n'agissaient pas comme arbitre, mais comme interface de formulation. La transparence était pensée comme inscription dans le format des contrats eux-mêmes. Les *bounties* étaient codés dans des *smart contracts* qui formulaient les rôles des parties prenantes de la relation de travail, identifiées par leurs *wallets* : les *issuers* spécifiaient les tâches, les *contributors* participaient à réaliser la tâche, les *fulfillers* étaient les contributeurs qui réalisaient effectivement la tâche, les *submitters* étaient des *fulfillers* ou leurs délégués, et les *approvers* acceptaient les actions des *submitters* (The Bounties Network 2019). Pour Sofia, cette répartition des rôles dans un format « simple » et « flexible » permettait de formuler des relations sans intervention de tiers autres que ceux directement impliqués dans la tâche en question et spécifiés à l'avance. En particulier, les gestionnaires de la plateforme elle-même n'apparaissaient pas. Les fonds étaient bloqués dans un dépôt (*escrow*) dès la soumission du *bounty*, et transférés automatiquement quand la tâche était approuvée par les personnes dont c'était le rôle¹⁵².

152 Au moment du *meetup*, un mécanisme d' « arbitrage » était envisagé pour résoudre les éventuels conflits sur la réalisation effective de la tâche. Ce problème du recours était pris en charge directement par une autre startup appelée Kleros avait développé un type de *smart contract* destiné justement à « arbitrer » les situations de désaccords entre acteurs de l'écosystème portant sur le résultat de l'exécution d'un *smart*

L'écosystème : espace de convergences entre utilisations B2C et B2B

Ethereum était construit comme une pratique professionnelle générique qui dépassait les types d'organisations économiques imaginées avec Ethereum (utilisations B2B, B2C) ou les types d'acteurs en présence (entreprises, institutions publiques, startups). Les paragraphes suivants montrent que le développement de ces compétences génériques était organisé par les acteurs de l'écosystème (en l'occurrence, au sein même de ConsenSys) et qu'elles étaient diffusées par ses porte-paroles (notamment *via* les meetups). L'écosystème se comprenait alors comme un espace d'élaboration et de diffusion de pratiques partagées entre acteurs d'une économie numérique à faire advenir. L'ouverture des meetups comme sites de diffusion de compétences et d'enrôlement de curieux (en futurs utilisateurs, entrepreneurs, ou développeurs) ont rendu mon accès aisé pour en faire un terrain d'enquête.

L'organisation du travail au sein de ConsenSys était donnée par Agueda comme exemple du modèle opale. Selon elle, l'autonomie d'action prônée par le modèle était réalisée par une organisation décrite dans un vocabulaire issu de l'artisanat : des rayons (*spokes*), des cercles (*circles*), une maille (*mesh*). Les rayons étaient les différentes startups incubées par ConsenSys (à l'origine « *startups venture studio* », voir *supra*). TBN de Sofia était un de ces rayons. Les cercles travaillaient avec les entrepreneurs des rayons sur des questions précises, afin de laisser à ces derniers le temps de concevoir leur modèle d'affaire (*business model*) et leur analyse de rentabilisation (*business case*) : il existait par exemple un cercle « ressources humaines », un cercle « marketing », un cercle « création de contenu », un cercle « marketing ». L'animatrice de la plupart des meetups de ConsenSys, Daria, était par exemple dans le cercle « Entreprise » (*Company*) chargée des relations publiques de la société et de l'organisation des événements. Daria elle-même désignait ConsenSys comme un « écosystème décentralisé » en introduction de ce meetup. La « maille » était une autre manière ramassée de désigner comment ConsenSys s'imaginait depuis 2015 : tisserand de liens faibles entre organisations et individus travaillant à faire advenir un Web3 ou « futur

contract, c'est-à-dire une mise en discussion du rapport entre l'exécution d'un *smart contract* et la réalité des données qu'il représente dans le monde. Je n'ai toutefois pas lu ou entendu de lien direct entre ces deux startups.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

décentralisé ancré sur la blockchain Ethereum » (ConsenSys 2019b). Le sens de « maille » a plus récemment été utilisé pour désigner l'activité d'incubation de ConsenSys, prenant une forme organisationnelle plus indépendante du reste de la société que par le passé (Mesh 2023)¹⁵³.

Le processus de technologisation, décrit à la section précédente, mobilisait des compétences qui circulaient au sein de ConsenSys grâce à cette organisation. L'activité de conseil aux entreprises avait un cercle dédié appelé « Solutions » auquel appartenait Agueda, ainsi que Jean. Elle expliquait que son travail était « de faire du conseil à certains moments », ce qui ne l'empêchait pas de se charger d'autres tâches de manière autonome. Les employés de ce cercle valorisaient les « rayons » (ou startups) auprès de clients « entreprises » dans des missions de conseil, tout en intégrant certaines à la « *full stack* ». C'est le chemin qu'ont suivi PegaSys, société de conception de logiciels « clients » (servant à faire fonctionner les nœuds du réseau), Metamask, le gestionnaire de *wallets*, Infura, permettant d'acheminer les transactions vers l'infrastructure matérielle, ou encore Truffle, la suite de développement de *smart contracts*. Toutes ces startups étaient initialement incubées comme « rayons » parmi une quarantaine d'autres en 2019 (ConsenSys 2019c). Les différentes activités de Jean indiquées plus haut participent à faire de ce « maillage » une réalité.

Cette circulation de compétences entre utilisations B2C et B2B était au centre du meetup #10 (mai 2019) sur le thème « Entreprendre dans la Blockchain: Quelles clés pour réussir », organisé un soir de la grande exposition française du développement technologique, VivaTech. Cet événement faisait partie de l' « *Ecosystem Night* », ensemble d'événements promu sur le programme officiel de VivaTech. Daria disait « esp[érer] amorcer l'opération séduction blockchain ce soir » et écrivait¹⁵⁴ sur la page meetup.com de ConsenSys :

ConsenSys France s'associe à Viva Technology pour l'Ecosystem Night: l'idée

153 Ces développements récents confirment la tendance historique de l'objet de la société ConsenSys décrite à la section : d'abord un « fonds » pour startups tout orienté vers le « développement de l'écosystème », ensuite une société de service mêlant incubation et développement de logiciels pour entreprises.

154 Je suppose que Daria sinon une personne de son « cercle » écrivait ces descriptions, étant systématiquement identifiée comme « hôte » des meetups de ConsenSys.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

est de réunir les acteurs clés de la tech en France pour faire raisonner [sic] l'événement auprès des communautés d'entrepreneurs.

*Cette initiative nous donne l'occasion de **féderer l'écosystème Blockchain** pour organiser le rendez-vous Blockchain de Viva Tech autour d'un sujet-clé: un point d'étape de **l'adoption de la technologie et des takeaways activables** pour les entrepreneurs désireux de se lancer dans un projet Blockchain.*

Deux associations d'acteurs de l'écosystème français étaient représentées parmi les orateurs de ce meetup : la ChainTech et l'Asseth. Antoine était président de la ChainTech, une association de « défense des intérêts » des professionnels (principalement des entrepreneurs et juristes) du secteur de la blockchain et des cryptoactifs notamment auprès des institutions publiques¹⁵⁵. Antoine était également dirigeant de Blockchain Partners, une société proposant des prestations de conseil aux grandes entreprises et aux startups développant des « cryptoactifs » (souvent, des jetons). Témoignages de la convergence entre les compétences blockchain pour entreprises et startups, sa société était rachetée deux ans plus tard par KPMG, un des plus grands cabinets d'audit et de conseil mondiaux (KPMG 2021). Antoine a également été très visible médiatiquement dans ses oppositions contre les critiques de Bitcoin et les cryptomonnaies dans l'arène publique, notamment vis-à-vis de Nicolas Dufrêne, président de l'Institut Rousseau. Comme Jean, Antoine travaillait en même temps à développer Ethereum et les cryptoactifs tout en participant à la diffusion de la blockchain comme une technologie destinée aux entreprises.

Blockchain et crypto étaient des choix entrepreneuriaux dirigeant vers des « carrières différentes » pour Antoine. Il s'adressait à un auditoire d'entrepreneurs en quête de conseils (« *takeaways* ») pour entrer dans l'écosystème. Pour lui, il était important que quiconque veuille construire à long terme (plutôt que surfer sur une vague et spéculer sur le prix d'un jeton) aie la bonne « posture » : humilité face aux extraordinaires possibilités offertes par cette technologie, et esprit critique quant à la manière de s'entourer pour construire son projet. La blockchain consistait à réaliser des intranets entre sociétés, à « blockchainiser l'existant » pour le rendre rentable à « court terme ». Les cryptos consistaient plutôt à

¹⁵⁵ Association que représentait Sylvain, au Chapitre 2. La ChainTech avait des activités de lobbying auprès des institutions en charge de la réglementation des cryptoactifs. Elle a notamment participé à la préparation du versant blockchain et crypto du texte législatif qui deviendra la loi PACTE.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

construire « l'Amazon ou le Google de demain ». La blockchain, son choix en tant qu'entrepreneur, était un choix de sécurité personnelle ; le second était plus risqué, mais était susceptible de déboucher sur des réussites extraordinaires, à l'image de la place qu'occupent les grands acteurs du Web dans l'économie numérique contemporaine.

Le développement informatique était l'autre activité professionnelle phare des acteurs de l'écosystème, avec l'entrepreneuriat. Durant le même meetup, Noé, employé de ConsenSys et représentant de l'Asseth, décrivait un « marché des développeurs blockchain » en plein essor en comparant deux ensembles de sources. Il s'appuyait, d'une part, sur les statistiques de LinkedIn et d'Indeed, respectivement réseau social professionnel et plateforme de recrutement en ligne, faisaient apparaître un déséquilibre entre offre et demande : le marché de l'emploi manquait cruellement de candidats. « Développeur blockchain » était l'emploi le plus recherché aux États-Unis en 2018¹⁵⁶, il était très bien rémunéré, mais la croissance du nombre de candidats était linéaire alors que l'augmentation des offres était exponentielle. D'autre part, Noé s'appuyait sur les statistiques produites par des acteurs de l'écosystème pour montrer la professionnalisation de l'activité de développeur blockchain et l'ampleur du vivier déjà disponible. Un rapport du fonds d'investissement spécialisé dans les projets crypto Electric Capital indiquait par exemple que le nombre de développeurs blockchain avait doublé entre 2017 et 2019 (Electric Capital 2018). La sous-évaluation du nombre de développeurs blockchain tenait selon à lui à un problème de recensement, notamment à un oubli de certains mots-clés par les algorithmes des plateformes comme « Bitcoin », un oubli des développeurs de l'infrastructure matérielle d'Ethereum ou « *core developers* » et des indépendants, la désaffection des développeurs blockchain pour LinkedIn, ou encore une attention particulière aux startups dans les cartographies d'institutions comme BPI France.

Articulant le thème du meetup (la promotion des compétences et des acteurs de l'écosystème français de la blockchain et des crypto) à sa présentation (professionnalisation de l'activité de développeur), Noé arguait que les développeurs français étaient nombreux

156 Les entreprises les plus demandeuses étaient IBM, ConsenSys et Chainyard outre-Atlantique, et Accenture, CGI, Talan et Octo Technology (quatre sociétés de prestations de conseil) en France.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

et actifs. Où les trouver ? *Via* les meetups ou plus généralement en s'adressant à différentes associations qui les regroupent en communauté, notamment : CryptoFR, association érigée en porte-parole des utilisateurs de cryptomonnaies, l'Asseth et la ChainTech¹⁵⁷. Noé inventoriait les outils, les formations et la recherche propres à cette activité. Parmi les outils, Noé listait différents MOOC sur la blockchain en général et sur Ethereum en particulier, les « valeurs crypto-anarchiques [sic], libertaires (*decentralization, censorship-resistance*) », la programmation orientée-objet et la « compréhension des bases de données », les compétences en cryptographie, cybersécurité, crypto-économie et réseaux décentralisé, mais aussi d'être « autodidacte ». Les formations avaient lieu dans des Écoles d'ingénieur et de commerce, dans les meetups, *via* des formations professionnelles ou encore en libre accès sur des « sites communautaires et éducatifs » comme Bitcoin.fr, Ethereum-France.fr (futur nom de l'Asseth), ou des médias en ligne comme le Journal du Coin¹⁵⁸. Enfin, Noé listait quelques institutions conduisant des projets de recherche en sciences informatiques, et rappelait que l'Asseth co-parrainait¹⁵⁹ (*sponsoring*) l'attribution d'un prix de recherche d'une valeur de 1 500 €¹⁶⁰.

2.2. Cadrage par une technologie de plateformes : l'utilisateur-citoyen, cas LeVote

Cette sous-section et la suivante sont consacrées à un cas de conception de plateforme dans lequel Ethereum était mobilisée comme une compétence et comme une technologie. Cette sous-section (2.2) montre que l'utilisateur imaginé de la plateforme, que j'appelle dans ce

157 Il s'agissait des trois principales associations qui structuraient l'écosystème compris au sens large, entre 2018 et 2020, à Paris. Le Cercle du Coin était une association intéressée exclusivement par Bitcoin. À la fin de l'enquête, DeFi France devenait un acteur important de l'écosystème en spécialisant ses événements sur la diffusion de pratiques entrepreneuriales pour l'émergente finance décentralisée.

158 Les formations participaient directement à la stratégie de ConsenSys indiquée à la section précédente. « ConsenSys Academy » était un ensemble de formations par lequel ConsenSys popularisait ses produits, aussi bien pour les entrepreneurs que pour les développeurs. L'initiative a été accompagnée d'annonces participant à la construction de ConsenSys comme suite logicielle de référence pour Ethereum, se fixant par exemple l'objectif d'atteindre « 1 million de développeurs » (cf. site OneMillionDevs.com, qui n'est plus actif à l'écriture de ces lignes) en 2019 (ConsenSys 2019f).

159 L'Asseth co-parrainait avec Kaiko, une société de production de données sur et pour l'écosystème.

160 En 2019, le prix a été accordé à deux développeurs de Kleros, société proposant un « oracle décentralisé » ou plateforme d'arbitrage des conflits portant sur l'exécution d'un *smart contract*.

qui suit « utilisateur-citoyen » tentait d'intégrer deux scripts (Akrich 1987, 1992). D'une part, l'utilisateur devait correspondre à l'utilisateur générique que j'appelle « utilisateur-autonome » en raison des qualités prêtées à Ethereum, alors vue comme une infrastructure déjà-là, à disposition des concepteurs pour développer le service. La formation des transactions devait être confiée à l'infrastructure. D'autre part, l'utilisateur était imaginé de manière spécifique à l'application qui était développée : un « citoyen-imaginé », inspiré de mouvements contemporains associés à la démocratie participative. Ainsi, la formulation était l'objet de conception ; les relations signifiaient votes lors de scrutins. L'intéressement d'Élus, clients du service, les faisaient entrer dans la formulation des relations.

Deux utilisateurs imaginés : un utilisateur-autonome et un citoyen-imaginé

Au printemps 2016, Geoffrey suivait les événements place de la République via l'application Periscope¹⁶¹. Apparu en opposition à la « loi Travail »¹⁶², le mouvement Nuit Debout prenait de l'ampleur. Différentes luttes convergeaient : pour l'amélioration des conditions socio-économiques d'existence, contre l'économie capitaliste, pour la reconnaissance des minorités ou encore pour l'accueil des réfugiés. Geoffrey voyait dans Nuit Debout un mouvement d'expression politique très stimulant. Il retrouvait une ferveur démocratique qu'il avait connue lors du mouvement Occupy Wall Street : les citoyens pouvaient prendre la parole, ils semblaient pouvoir s'organiser de manière autonome pour exercer un pouvoir direct, émancipés de leurs représentants élus.

L'idée lui est alors apparue : il imaginait un outil « transparent, sécurisé et autonome » (entretien avec Geoffrey, novembre 2018)¹⁶³ qui permettrait de déployer à grande échelle les innovations démocratiques qu'il voyait dans les rassemblements de Nuit Debout.

161 Periscope était une application pour mobiles fonctionnant sous iOS et Android qui permettait à l'utilisateur de retransmettre en direct ce qu'il était en train de filmer. Le projet a été racheté par Twitter puis arrêté.

162 Loi numéro 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels, dite « loi Travail » ou « loi El Khomri ».

163 Sauf précision, les citations qui suivent sont des verbatims de Geoffrey et des membres de son équipe rencontrés individuellement en entretiens entre novembre 2018 et janvier 2019.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Geoffrey cherchait lui-même à mettre en place ces principes d'organisation au sein des équipes qu'il dirigeait chez Orange : vote à main levée, réactions d'approbation par des mouvements de mains silencieux. Cet outil démocratique autonome serait numérique, disposant ainsi de qualités dont était dépourvu le « parcours du vote papier », certes « robuste » mais peu « transparent ». Cet outil d'expression individuelle serait indépendant d'un acteur comme Facebook, « centralisé » et qui ne garantissait pas l'unicité du vote.

Geoffrey avait une seconde source d'inspiration : Bitcoin, qui lui avait fait percevoir « un nouveau paradigme, une nouvelle manière de penser » un an plus tôt. Geoffrey s'était créé un *wallet* et avait senti quelque chose de « mystérieux, sibyllin, presque un peu complexe » mais qui avait l'air « assez énorme ». Il « sentai[t] une force, mais pas dicible » qui permettait de faire des choses de manière absolument évidente et immédiate, comme un transfert d'argent, mais sans acteur central ou intermédiaire. Ainsi, il voyait dans la blockchain un possible prolongement des « valeurs de transparence et de sécurité [de Bitcoin] au domaine démocratique et du vote ».

Ce qui deviendrait deux ans plus tard le service LeVote d'Orange avait été imaginé à partir de la rencontre de deux utilisateurs : à partir de Bitcoin, l'utilisateur-autonome exprimant des préférences directement ou « sans intermédiaire », et à partir de Nuit Debout, un citoyen-imaginé frustré de ne pas participer suffisamment au processus démocratique. Les paragraphes qui suivent détaillent le cadrage qui suit l'idée de Geoffrey au sein d'Orange en s'appuyant sur les récits qu'en font ce dernier, « intrapreneur » et dirigeant ou *Chief Executive Officer* (CEO) de LeVote, et trois autres membres de son équipe : Denis, responsable du *business development* ; Fabrice, en charge de l'expérience utilisateur et de la conception des interfaces ; Salah, responsable technique ou *Chief Technology Officer* (CTO).

2.2.1. La plateforme comme cadrage des relations numériques : le cas du vote

Le service LeVote était imaginé comme une plateforme. Geoffrey m'expliquait avoir deux

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

sources d'inspiration : Doodle et Change.org, respectivement site web de création de sondages partagés *via* une URL et plateforme de pétitions en ligne. La première établissait une relation de disponibilités partagées entre participants qui exprimaient leurs préférences individuelles, la seconde permettait d'organiser la signature à grande échelle d'un texte érigé en pétition. Dans ces deux cas, les plateformes étaient des supports génériques : des disponibilités partagées quelle que soit la réunion concernée, un soutien partagé quelle que soit la cause défendue. De manière comparable, la plateforme LeVote visait à permettre l'organisation de scrutins quels qu'ils soient. Geoffrey envisageait de proposer son service pour des scrutins destinés à des corps électoraux variés, des élus des territoires et de la Nation (en commençant par les maires, représentants de communautés d'agglomérations, de métropoles, de départements ou de régions) aux élections internes aux associations (du bureau) ou aux entreprises (comme les élections des délégués du personnel).

La blockchain permettait de concilier deux ensembles d'exigences : d'une part, la généralité d'un vote platformisé (dont l'objet pourrait être fixé indépendamment du dispositif technique), et d'autre part, les qualités d' « unicité » et de « transparence » du vote vues comme plus petits dénominateurs communs de l'expression individuelle en démocratie. Geoffrey m'expliquait que la blockchain donnait à chacun la possibilité de vérifier que son vote serait bien comptabilisé, ce qui n'était pas garanti par les solutions traditionnelles de vote électronique. Aucune d'entre elle n'apportait une « preuve scientifique » du vote. Au contraire, la technologie permettrait de faire vivre la démocratie participative sans suspicion de triche. Il citait l'exemple de la ville de Bordeaux qui avait demandé à ses administrés de se prononcer pour ou contre la transformation d'un pont sur la Garonne en piste cyclable. Le « pour » l'avait largement emporté, mais Geoffrey suspectait des associations de cyclistes d'avoir organisé un bourrage d'urnes en faisant massivement voter leurs adhérents pour la construction de pistes cyclables. Denis justifiait l'intérêt de la blockchain dans les mêmes termes : se protéger contre des actions qu'il voyait comme anti-démocratiques. Selon lui, l'Affaire du Siècle, campagne conduite par quatre associations militant pour la condamnation de l'État pour inaction climatique, n'aurait jamais acheté la solution LeVote, car elle les aurait privés de manipulations du scrutin en mobilisant leurs fichiers

d'adhérents.

L'utilisateur-citoyen imaginé par les concepteurs problématisait le rapport entre citoyen et décision politique. Cette problématisation était formulée dans les termes des plateformes. Chacun des interviewés exprimait son admiration pour la démocratie directe et sa méfiance pour la démocratie représentative dans des termes plus ou moins virulents. En revanche, tous voyaient dans la plateforme une nouvelle forme de démocratie directe permettant de totaliser des préférences individuelles. Pour Denis, c'était bien la « responsabilité » individuelle plutôt que la confiance dans les « décisions » de représentants qui feraient advenir les mouvements collectifs dont le monde a besoin. La limitation du réchauffement climatique à 1,5 degrés serait par exemple une affaire individuelle et pas une question de politiques publiques ou de lois encadrant l'activité des entreprises. Au contraire, LeVote inciterait chacun à s'exprimer sur tous les sujets, grâce à la forme plateforme. Pour Denis, il était tout aussi aberrant d'avoir différents systèmes de parcmètres entre Paris et Houilles que d'avoir différents dispositifs de vote en fonction des scrutins. Geoffrey exprimait ce rapport entre utilisateur-citoyen imaginé et décision collective en faisant du vote un droit individuel, fétichisé par la carte d'électeur qui pouvait être détenue dans un *wallet*, comme des cryptoactifs :

*Je crois en ce concept, je crois au fait que ça devienne [...] une commodité, que LeVote soit un réflexe aujourd'hui, **que LeVote ça soit le portefeuille de tes cartes d'électeurs**. Aujourd'hui, tu as le wallet de l'iPhone, quand tu as un billet SNCF ou Air France, tu as un wallet, et bien là, c'est pareil, tu auras ta carte d'électeur. C'est un peu ça la stratégie. Et que **ce soit une commodité**, c'est-à-dire que quand tu veux envoyer, je ne sais pas, un mail, tu utilises Outlook, tu ne t'emmerdes pas, c'est comme ça dans les entreprises, **quand tu voudras voter, tu utilises LeVote, c'est comme ça, tu ne te prends pas la tête**. (entretien avec Geoffrey, novembre 2018)*

Cet utilisateur-citoyen propriétaire identifié par son *wallet* de cartes électorales apparaît dans le choix technique de plateforme pour le service LeVote. La première version du service, appelée MVP pour « *minimum viable product* », était construite comme une DApp sur Ethereum. L'organisateur du scrutin, typiquement un Élu, obtenait un nombre de jetons égal au nombre d'administrés puis les distribuait à chacun. Le jeton, sorte de bon-pour-un-

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

vote-au-porteur, n'était utilisable qu'une fois. Pour Fabrice, qui qualifiait explicitement le *design* de l'application de « plateforme », deux facteurs différençaient LeVote des autres services de votes électronique : l'interface, pensée pour être à la fois simple et générique pour tous types de votes, et la possibilité donnée à chaque utilisateur de vérifier son vote.

Le vote était cadré comme une transaction *via* un *smart contract*, codé de manière unique pour tous types de scrutins dont on peut ajuster des paramètres comme le nombre de participants, la question posée ou la date limite de participation. Fabrice disait clairement ce que j'appelle formulation. Il m'expliquait qu'il voyait l'interface comme une manière de donner une signification, un « contexte », à une transaction inscrite sur la blockchain. Sans ce contexte, la transaction serait certes inscrite de manière indélébile, mais perdait tout sens :

Ethereum qui est mondial et qui a une blockchain qui n'appartient, a priori, à personne, puisque tout le monde y met ses billes, et les données qui y sont toutes entrelacées, n'ont aucun rapport avec du vote. Nous on est au milieu de tout ça, simplement, la transaction qui dit « un vote », c'est nous qui lui donnons le sens de « c'est un vote », mais en fait, c'est une simple donnée blockchain, pour écrire cette information qui permet de dire « en fait toi, en consultatif, sur la proposition qu'on ta faite, tu as répondu oui, voilà ton certificat, il y a marqué oui, il n'y a pas ton nom, mais il y a marqué oui, et des sortes d'informations techniques, des clés, donc il y a des chiffres ». Ce « oui » s'il est perdu dans la rue ne permet pas de remonter jusqu'à toi parce qu'il n'y a pas ton nom, mais si toi, tu l'archives, en fait, tu en es possesseur, si tu vas sur la blockchain Ethereum et que tu rentres en saisie manuelle, même c'est [...] très fastidieux pour l'instant. (entretien avec Fabrice, décembre 2018)

Ethereum apportait l' « unicité » et la « transparence », le deuxième pilier de l'expression en démocratie aux yeux des concepteurs de LeVote. Autrement dit avec cette double qualité, Ethereum était un dispositif de formation des transactions : la forme transaction, ou l'inscription sur la blockchain, garantissait la « propriété » du vote aussi bien avant qu'après son expression.

Le choix de la blockchain était fixé avant que Salah ne rejoigne l'aventure LeVote. Il m'expliquait que le choix d'Ethereum s'était rapidement imposé pour deux raisons. D'une part, le choix d'une blockchain « privée » de type Hyperledger était exclue, car elle ne

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

garantissait pas la « transparence » attendue pour le service ; autrement dit, ce type de solution ne totalisait pas les transactions au-delà des acteurs qui participaient à administrer le réseau. D'autre part et alors que je l'interrogeais sur la raison de ce choix par rapport à d'autres blockchains publiques permettant comme Ethereum de formuler des relations (comme NXT ou NEO), Salah m'expliquait qu'Ethereum était la blockchain publique la plus connue pour automatiser des inscriptions, et par là la solution la plus évidente. Salah était par ailleurs très satisfait de la simplicité à « configurer » un nœud du réseau Ethereum. Il avait choisi un nœud en version « légère », c'est-à-dire qui ne mine pas d'ether. Ces nœuds étaient moins contraignants que les nœuds complets (*full nodes*) ; ils ne constituaient en temps réels que certains en-têtes, permettant d'explorer directement l'historique des transactions sans dépendre d'un serveur distant qui donne accès aux informations¹⁶⁴.

Salah associait la notion de « transparence » à Ethereum par hypothèse, et en opposition aux solutions de blockchain privées ou de consortium comme Hyperledger. Il faisait ainsi un choix de gouvernance, la formation des transactions devant être extérieure à Orange pour que le citoyen-imaginé puisse individuellement et en autonomie « vérifier » son vote. Ce faisant, Salah faisait ce que théorisaient différents intervenants des meetups organisés par ConsenSys. Parmi les compétences entrepreneuriales et de développement qui faisaient converger les utilisations B2B et B2C d'Ethereum figurait la manière de former les transactions. Nathan, employé de ConsenSys depuis l'ouverture du bureau parisien en 2017, répondait par exemple à la question « Comment choisir son réseau blockchain » lors du meetup #16 (septembre 2019) où Ethereum était présentée comme une « boîte à outils » dont la mobilisation dépendait de l'usage imaginé et de la gouvernance associée aux relations. Il indiquait que l'infrastructure publique devait être privilégiée pour des usages comme les ICO et les STO qui demandent un « maximum de décentralisation », ce que Salah et les concepteurs de LeVote exprimaient en termes de « transparence ».

J'ouvre une parenthèse avant de revenir au cas LeVote, pour mettre en évidence que la gouvernance par la formation des transactions relevait d'un choix sur un marché

¹⁶⁴Ce type d'information est distribué à tout un chacun par des sites web comme Etherscan (<https://etherscan.io>).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

technologique en plein développement. L'infrastructure publique s'opposait aux usages privés d'Ethereum, préféré par les entreprises françaises selon Jordan, employé de ConsenSys dans le cercle « Solutions », quand il prenait la parole durant le meetup #10 (mai 2019) à la suite d'Antoine et de Noé. Son intervention était intitulée « État de l'adoption de la technologie Blockchain par les entreprises françaises » ; il se présentait comme un « passionné de crypto » qui « bosse aujourd'hui en blockchain pour entreprises » : comme pour Jean et Antoine, le profil de Jordan témoigne de la circulation des savoir-faire entre cryptomonnaies et projets d'entreprises. Il n'était pas directement question d'Ethereum en particulier dans cette présentation, mais plutôt de la technologie blockchain en général dans les projets des « entreprises », au sens de grands représentants du capitalisme français. Pour Jordan, ces dernières sortaient du stade expérimental¹⁶⁵. Jordan résumait l'intention des acteurs réunis en consortium : on se fait confiance entre acteurs qui n'ont pas les mêmes intérêts, de manière à partager les coûts de développements de systèmes et de créer des standards industriels communs. C'était le cas d'une réalisation de ConsenSys citée par Jordan : la plateforme d'échange de produits financiers sur les matières premières (*commodity trade finance*) appelée Komgo à laquelle participait la banque de financement et d'investissement du groupe Crédit agricole (Crédit agricole Corporate and Investment Bank) aux côtés d'autres acteurs bancaires comme l'Étatsunienne Citibank et d'énergéticiens. Komgo était également l'exemple cité par Joseph Lubin (voir *supra*) pour illustrer l'adoption d'Ethereum par les entreprises. Le fondateur de ConsenSys voyait dans Komgo la preuve de gains opérationnels pour les entreprises : il estimait à 3 ans le temps de mise en œuvre d'un système développé en 6 mois grâce à la nature de la blockchain¹⁶⁶ :

165 Il s'appuyait sur une enquête du cabinet d'audit et de conseil Deloitte, toutes les entreprises françaises avaient un budget alloué aux projets blockchain en 2019, 69 % de ceux-ci dépassait 1 million d'euros, et 86 % d'entre elles prévoyant un passage en production d'ici la fin de l'année ; plus de la majorité d'entre elles voyaient dans la blockchain une « base de données financière », bien que des cas d'application concerne les chaînes logistiques et la « certification et identité souveraine ». Jordan identifiait différentes raisons pour comprendre les réticences des entreprises pour la blockchain : incertitudes juridiques et réglementaires, interrogations quant à l'interopérabilité avec les systèmes existants de ces entreprises, les problèmes de passage à l'échelle, le refus de perdre le contrôle sur les processus blockchainisés, des problèmes de confidentialité, ou encore la mauvaise compréhension de la valeur ajoutée de la technologie.

166 Pour Lubin, ce temps pouvait encore être réduit quand la « pile » de produits ConsenSys, construite notamment à partir de ces premières expériences de mise en œuvre de projets blockchain, serait complète.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

*because of the nature of blockchain where you get so much secure transactional infrastructure for free, you get the replication of all these databases or all these states machines, you set up nodes, you point them at each other, they pretty much find each other and stay up and in sync. And so **what you're left to do is figure out the business logic that you write into smart contracts and user interface, that you use to access the different actions.** And so, it took six months from initiation of the project to integration with 15 banks and energy companies. (Joseph Lubin, meetup #18, mars 2020)*

La gouvernance par la formation des transactions était ainsi théorisée dans les meetups et pratiquée dans des projets comme LeVote ou Komgo comme un choix de formation des transactions préalable qui ouvrait dans tous les cas à ce que Lubin appelait « définition de la logique d'affaires ». Avec le choix de l'infrastructure publique, comme LeVote, l'inscription était externalisée à un réseau considéré comme un tiers neutre. Au contraire, dans le choix des consortia, la formation était maîtrisée par les partenaires. Cette différence devenait nettement visible lors d'une séance de retour d'expérience organisée suite à l'intervention de Joseph Lubin la veille d'EthCC (cf. section 1). Un représentant d'un consortium monté par ConsenSys, une « plateforme » appelée AURA, était interpellé par un intervenant dans la salle. Ce dernier demandait, au nom de son propre employeur, s'il était possible de rejoindre le consortium. AURA était une association de grands acteurs du luxe, dont LVMH, qui visait à développer un certificat des produits de luxe. Le représentant était visiblement embarrassé. Pourtant, l'extension la plus large possible du consortium était un objectif annoncé et affiché durant sa présentation. Mais le représentant répétait que le consortium n'était « pas dans un mode communication pour l'instant », et cherchait à passer à une autre question. Cette situation témoigne d'une recherche de contrôle par les membres des consortia dans la formation des transactions, opérations limitées à des accords commerciaux formalisés en dehors du dispositif technique. Au contraire, sur l'infrastructure publique, la formation des transactions était ouverte à tous sans condition d'accès. Je referme la parenthèse et reviens au cas LeVote.

2.2.2. Le cadrage par la plateforme à l'épreuve du monde : l'intéressement des Élus

Le processus d'intéressement des Élus, prospects d'Orange et par là premiers interlocuteurs des concepteurs, mettait à l'épreuve la problématisation de départ par l'utilisateur-citoyen. Les paragraphes qui suivent esquissent ce processus multi-acteurs à partir des verbatims des concepteurs recueillis en entretiens. Ces derniers avaient lieu alors qu'une première version du service LeVote avait été achetée par plusieurs collectivités locales. Cette version du service « consultatif » réduisait l'ambition de généralité de la plateforme de vote : les scrutins ne pouvaient pas être utilisés pour des élections, mais seulement pour des consultations. Ce choix simplifiait le cahier des charges du service : le vote « électif » était soumis à une réglementation spécifique et à des audits réguliers¹⁶⁷, il comportait des dizaines d'exigences spécifiques contraignantes pour la conception. Au moment de l'enquête, une solution de vote « électif » était en train d'être préparée par les équipes de LeVote et imposait une conception nouvelle. Denis m'expliquait que les deux versions du service impliquaient de résoudre un paradoxe intrinsèque au vote : l'articulation entre anonymat (ou « fermeture ») et transparence pour éviter la fraude (ou « ouverture »).

Le rôle d'Orange et de LeVote : assistance technique à la formulation de scrutins par les Élus

Les concepteurs cherchaient à transcrire le processus de vote dans le dispositif technique. Geoffrey m'expliquait par exemple que la formulation des scrutins imposait aux organisateurs de scrutins (les Élus) de désigner « au minimum trois assesseurs » composant un « bureau virtuel » en charge de dépouiller une « urne virtuelle » qui collectait l'ensemble des votes. La fermeture de l'« enveloppe », dans laquelle chaque votant glissait son bulletin, se faisait avec une « clé privée » individuelle. Le certificat de vote envoyé par l'application devait servir de preuve au votant. Orange était imaginé comme fournisseur du matériel électoral, de l'urne à l'isoloir en passant par les enveloppes et le bureau de vote lui-même.

¹⁶⁷ Le label « e-vote » a été initialement proposé par l'association professionnelle « Fédération Nationale des Tiers de Confiance ». Il a été approuvé par la CNIL en 2016.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

*[Si les Élus] ont besoin de support, s'ils m'appellent tous les quatre matins, là, c'est compliqué. Sinon là, **ils ont un outil autonome**, ils ont le back office, c'est comme si tu écris un article dans un blog, date de début, date de fin, questions à poser, le contexte, tu balances, et automatiquement les mecs qui ont l'application, ils vont avoir le truc, ils n'ont pas besoin de nous, et ça, forcément, **on travaille à cette automatisation parce qu'il n'y a pas de miracle pour le coup**. (entretien avec Geoffrey, novembre 2018)*

Cette vision procédurale du vote correspond au rôle que se donnaient les concepteurs : celui d'assistant des Élus à l'organisation de scrutins en autonomie. Le vote « consultatif » avait des ambitions relativement modestes. Geoffrey citait le cas type d'un Maire qui pourrait demander à ses concitoyens si tel terrain vague devait être aménagé en stade ou en médiathèque, ou de se prononcer sur la manière d'aménager les rythmes scolaires ou encore sur le passage de la commune à la 4G. Fabrice expliquait que le travail d'Orange ne consistait pas à construire des scrutins du début à la fin : le stockage des votes, l'archivage, ou même la possibilité d'accéder à des informations sur le vote ne dépendaient pas d'Orange mais d'Ethereum et de ses propres interfaces¹⁶⁸. LeVote cherchait plutôt à « faire la courte échelle » aux Élus, c'est-à-dire les aider à faire du vote une « hygiène de vie », un réflexe qui peut être mobilisé régulièrement pour impliquer les citoyens à la vie de la Cité sur des questions pratiques et quotidiennes, « ré-intéresser les gens au fait de prendre en main un peu plus leur destin quand ils ont des votes d'ordre légal à suivre ». Ce travail d'intéressement des citoyens, consistant à « faire comprendre aux gens qu'il y a un intérêt pour eux », était entièrement celui de l'Élu, pour les concepteurs. Pour Fabrice, « Orange n'[était] qu'un intermédiaire » qui permettait d'accéder à Ethereum et aux propriétés associées de « transparence » et d'« unicité » du vote. Comme pour la fourniture d'accès à Internet auquel Orange donnait accès sans l'avoir « réinventé », historiquement avec Wanadoo, ici, LeVote donnait accès à Ethereum et à la totalisation des transactions.

Du point de vue d'Orange, le critère de succès de l'application était avant tout commercial, c'est-à-dire a minima que le service ne coûte pas plus à l'entreprise qu'il ne lui rapporte. Le rôle de Denis était précisément de veiller à cet impératif ; il m'expliquait qu'il avait été recruté à ce titre courant 2018, en tant que contractuel, par un dirigeant de l'entreprise qui le

168 Comme le site Etherscan indiqué plus haut.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

connaissait *via* des réseaux d'anciens diplômés de grandes écoles. Il veillait à ce que « le *business* soit autoportant avec le minimum de capital ». Son travail était de rationaliser l'ambition du projet : il opposait une attitude « amoureuse », consistant à voir dans l'innovation en général et dans la blockchain en particulier des caractéristiques prometteuse, à une attitude pragmatique garantie par le succès industriel du projet.



Figure 20 : Présentation de l'application LeVote par Geoffrey à VivaTech 2019

Le principal dispositif d'intéressement des Élus était le réseau des employés d'Orange dans les territoires : Denis et Geoffrey parlaient de « grosse » ou « incroyable » « force de frappe » sans laquelle LeVote « ne ferait pas grand-chose ». Ils se nomment DR, DRCI, DPI ou encore AE. Un premier ensemble de ces employés était en contact permanent avec les élus locaux. Ce sont les Directeurs Régionaux (DR), les « patrons » d'une région donnée, qui encadrent des « Délégués Régionaux aux Collectivités Locales » (DRCI) et des

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

« Directeurs de Projets Innovants » (DPI). Geoffrey m'expliquait que le rôle principal des DR et des DRCL était de garantir les services d'Orange localement, typiquement à veiller à ce que la fibre fonctionne bien ou à planifier des travaux de maintenance. Du fait de leur proximité avec les élus des 36 000 communes françaises, il leur était possible de parler de LeVote, tout comme les DPI donc le rôle est statutairement de parler de produits innovants comme LeVote. Les Agences Entreprises ou AE formaient un réseau de commerces locaux pour les entreprises et les collectivités locales complémentaire.

L'équipe de LeVote menait dans le même temps ses propres actions commerciales directement auprès d'Élus, que ce soit dans des rencontres bilatérales ou dans le cadre d'événements comme VivaTech durant lequel les concepteurs avaient obtenu une place sur le grand stand d'Orange, en 2019 (Figure 20 avec Geoffrey masqué par le smiley).

Prototype et inclusion des Maires dans le processus de formulation des votes

Les concepteurs de LeVote avaient une idée assez nette des motivations des Élus susceptibles d'utiliser leur service. D'une part, ils voyaient une tendance électoraliste à laquelle LeVote pourrait répondre : en consultant leurs électeurs, les Élus pourraient renforcer la légitimité de leurs décisions, aussi bien lors de futures campagnes que sur les réseaux sociaux. Pour Denis par exemple, la consultation permettrait à l'Élu de se dédouaner par avance d'éventuels mauvais choix de gestion, et symétriquement, d'éviter au citoyen-imaginé de subir des décisions politiques dommageables sans qu'il ai eu l'occasion de se prononcer. D'autre part, les concepteurs voyaient une adhésion aux principes de la démocratie participative. Fabrice m'expliquait que le déclenchement d'un vote semblait particulièrement utile pour l'Élu quand celui-ci n'avait « aucun avis » sur une question donnée, c'est-à-dire pour les questions qui ne lui semblaient pas relever directement de son mandat lui conférant l'incarnation de l' « intérêt général ». L'outil permettrait ainsi de déléguer un pouvoir de décision sur une question précise et d'une importance jugée *a priori* limitée pour la collectivité. Ainsi, les Élus auraient un outil pour impliquer les citoyens sans affaiblir leur autorité ni remettre en cause leur pouvoir de décision légitimement garanti par

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

leur propre élection. Deux cas de clients de LeVote illustrent ces tendances (Tableau 13).

| Cas du Maire de la Commune A | Cas du Maire de la Commune B |
|---|---|
| <p><i>C'est un vrai personnage, il signe, photographes, photos dans le journal, serrer la main d'Orange, ils n'ont jamais utilisé le service. Je te jure que c'est vrai. [...] Rien à foutre. Par contre, le jour J, il y avait les petits fours, le champagne, les photographes, les journalistes. Donc là, c'est vraiment un enjeu de communication, parce qu[e Commune A], c'est vrai, alors ils nous font confiance, c'est pour ça qu'on bosse avec eux, parce qu'ils veulent être toujours en amont de ce qui se fait dans les smart cities, dans les nouvelles technologies.</i></p> | <p><i>Lui le Maire, 15 000 habitants, 2 semaines après on signe, alors quelques centaines d'euros ou milliers d'euros, on signe avec lui... 15 jours après il fait son scrutin qui dure 15 jours, en 4 semaines, hyper content, il dit : « Maintenant, j'aimerais bien que l'on fasse ça et ça pour le bureau municipal », il se projetait, dans l'usage et pour ses citoyens. Et la plupart, il y en a beaucoup en France qui sont plutôt apolitiques, ils ne sont ni de gauche, ni de droite, ou alors oui, mais ils s'en foutent, ils sont là parce que ce sont les docteurs du village, tu en as quand même beaucoup. Et lui, il était content parce que ça évitait de faire des papiers, des flyers, une économie certaine, et puis il se projetait sur des nouveaux usages et en 15 jours, alors c'est 13 000 et quelques habitants, il y a 800 personnes qui se sont inscrites, donc ça faisait, on avait fait le ratio, mais c'était peut-être 4 ou 5 %, alors que normalement sur une consultation papier, papier physique, à 3 %, les maires commencent à être contents.</i></p> |

Tableau 13 : Verbatims issus d'un entretien avec Geoffrey (novembre 2018) : contractualisation avec deux Communes clientes

Le cas du Maire A parle autant d'une tendance de nombreux acteurs à s'émerveiller face à la nouveauté technologique que d'une stratégie commerciale d'Orange. Denis m'expliquait que LeVote était pensé comme un produit d'appel pour une suite de services destinée aux collectivités locales sur le thème des *smart city*. En faisant bénéficier de ce service à bas coût à de nombreuses collectivités, quitte à ne pas faire d'argent, Orange se faisait connaître comme un acteur des *smart city*. Denis estimait que l'outil de consultation était incontournable pour une suite *smart city*. Réciproquement, les Élus pouvaient s'équiper et se prévaloir de faire bénéficier les territoires qu'ils représentaient des dernières nouveautés technologiques. Denis voyait là une manière de contrer la « résistance à l'innovation » qu'il identifiait dans les administrations publiques, tout en répondant aux manifestations des Gilets Jaunes. Il imaginait intégrer LeVote à un portefeuille de produits *smart city* qui pourrait se présenter comme un « *Appstore Smart City* » de produits Orange susceptibles de rivaliser avec les offres d'acteurs comme Google, qu'il avait observé au dernier Salon des

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Maires¹⁶⁹. L'expérience tirée avec LeVote et les éventuels bénéfices du service pourraient, toujours selon Denis, participer à financer un incubateur de *civic tech* au nom d'Orange.

Le Maire B confortait Geoffrey dans son ambition de changer la démocratie par de nouveaux outils numériques. Ce Maire avait rapidement pris goût au service « se projetait » en imaginant de nouveaux usages, comme utiliser le service au sein même de son conseil municipal. Fabrice m'a confirmé que cette fonctionnalité était à l'étude, parmi d'autres que des Élus auraient suggéré en débordant l'usage initialement imaginé ; par exemple : cibler les votants en fonction de leur âge ou de leur adresse de résidence. Ces enthousiastes espéraient dans le même temps un outil d'organisation de consultations qui soit efficace, c'est-à-dire qui permette d'économiser de l'argent et des complexités logistiques, en comparaison d'une consultation papier, aussi bien dans la mise à disposition d'espace que dans le processus de dépouillement qui devenait instantané avec une solution numérique. Dans le même temps, Fabrice m'indiquait qu'un des principaux obstacles du point de vue des Élus à l'utilisation du service était la « fracture numérique » : nombreux étaient les citoyens qui n'avaient pas d'adresse de courriels ou jugeaient trop compliqué d'accéder au service depuis leur ordinateur ou leur tablette personnelle. Les Élus choisissaient ainsi souvent de mettre une borne à disposition de toutes et tous, au sein de bâtiments publics, de manière similaire à celle qui apparaît en guise de démonstration lors du salon VivaTech, en Figure 20.

Les Élus recevaient la notion de « blockchain » de manière ambivalente : si la technologie « brillait » aux yeux des Élus pour Geoffrey, elle n'était vraiment comprise que par les « technophiles » et soulevait des interrogations, comme toute technologie numérique. Les concepteurs m'expliquaient traduire les bénéfices de la technologie en termes de « sécurité » du vote. Fabrice aimait raconter que la fiabilité d'un dispositif informatique ne pouvait jamais être tout à fait garantie, mais que les Élus étaient réceptifs au fait que la blockchain apportait une « sécurité extrême », puisque Bitcoin n'avait jamais pu être cassée, et que si elle l'était, tout le monde le saurait nécessairement. La blockchain, centrale pour garantir l'unicité du vote tel que l'imaginaient les concepteurs au départ, avait

169 Orange participe chaque année à cet événement organisé par l'Association des Maires de France.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

finalement plus séduit par son caractère d'innovation technologique que pour le bénéfice imaginé : l'unicité du vote. Fabrice était par exemple étonné de constater que différents Élus ne s'émouvaient pas beaucoup du fait qu'il était possible de voter plusieurs fois dans les consultations organisées par la Mairie de Paris pour le budget participatif. De manière similaire, revenant sur l'Affaire du Siècle, Denis se demandait s'il « exagérait la sensibilité à la fraude », constatant que légalement il était plus important de garantir l'anonymat du vote que la vérifiabilité du vote.

Les contacts des concepteurs avec les Élus ont fait apparaître deux ensembles de problèmes liés au cadrage du service comme une DApp. Premièrement, il n'était pas satisfaisant de déléguer aux Élus le travail de distribution des accès (numériques) au vote à leurs administrés. LeVote, construit comme une DApp, faisait en effet endosser à ces derniers la distribution de jetons, ce qui supposait que les Élus disposent d'une base de données avec les courriels de tous les administrés pour que ceux-ci se connectent, à partir d'une URL transmise par courriel, à l'application LeVote :

[Les Élus] ont une liste de votants, ils disent « voilà, nous, on envoie à telle personne un token anonyme », donc il est envoyé, on ne sait pas à qui, mais il est envoyé, à une personne, et ce token, il ne peut être utilisé qu'une seule fois, donc libre à eux d'envoyer les tokens quand ils créent un scrutin. Ils vont créer un scrutin pour 50 personnes, ou pour 50 000 personnes. Alors si c'est 50, je génère 50 tokens aléatoires, ou 50 000, et le Maire, dans son back office, il peut télécharger un fichier Excel avec tous les tokens avec un flag au début qui est burn à zéro parce qu'il n'a pas été utilisé. Il envoie à ceux qui ont la base de données des votants. Après le votant, qu'est-ce qu'il fait ? Il clique sur une URL. Il clique sur l'URL avec le token et là, il arrive sur une page Web pour voter. Il vote, donc il y a une transaction qui est envoyée sur la blockchain, après s'il relance cette même URL, il va tomber sur « Vous avez déjà voté » et si le scrutin est terminé, il aura les résultats, toujours sur cette même URL, d'accord ? (entretien avec Salah, décembre 2018)

Or, les Élus ne disposaient pas des informations nécessaires à la distribution de jetons. Fabrice m'expliquait que certains d'entre eux auraient techniquement pu constituer la liste d'adresses électroniques requises, par exemple en s'appuyant sur les inscriptions aux services numériques des villes (comme les bibliothèques ou autres activités culturelles et sportives), mais l'utilisation de ces données pour un usage différent du motif de collecte

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

d'origine était interdite par la CNIL. Geoffrey m'expliquait que certaines collectivités avaient entrepris de constituer à la main la liste des administrés : des employés de la collectivité étaient dans ce cas chargés de constituer la base de données, avec des risques importants d'erreur, et sans éviter des coûts d'organisation importants à chaque consultation.

Deuxièmement, le modèle économique défini avec la forme DApp ne convenait pas aux budgets des Élus qui attendaient un service bon marché, selon tous les interviewés. Geoffrey m'expliquait qu'avec l'efficacité attendue par la numérisation venait également une efficacité économique. Selon lui, l'indicateur que les Élus avaient à l'esprit était le « coût [du scrutin] par tête » (d'administré), dont ils connaissaient généralement le nombre à l'unité près. Les solutions de marché concurrentes à LeVote allaient de 3 à 5 euros par personne ; avec le processus papier traditionnel, il fallait compter autour de 5 à 15 euros par personne. Or, la solution proposée par LeVote dépendait des cours de l'ether, impliquant un coût volatil à chaque transaction, c'est-à-dire à chaque vote. Par conséquent, le coût de chaque consultation était à la fois fonction du nombre de votants et des circonstances sur le marché des cryptoactifs. Ce modèle n'était pas compatible avec les attentes des Élus qui attendaient au contraire un « coût maîtrisé ».

2.3. Débordements du cadrage, négociations de la formation et de la formulation

Cette sous-section analyse le débordement du cadrage de l'utilisateur-citoyen provoqué par l'irruption des Élus dans le processus de conception, qui a conduit les concepteurs à reprendre les opérations de formation et de formulation des transactions. Les qualités projetées sur la relation entre l'utilisateur-citoyen et le processus de décision collective, comme la « transparence », étaient remises en question. Le rôle d'assistant à la formulation des Élus que se donnaient les concepteurs était lui-même mis en question par la nature des ajustements contraints par ces débordements. Cette situation conduisait les concepteurs à repenser la constitution du corps électoral et le script de l'utilisateur-citoyen.

Un nouveau dispositif dit « V1 »¹⁷⁰ a été conçu à partir du « *minimum viable product* », insatisfaisant à la fois par la manière de constituer un corps électoral (comment garantir que tous les administrés aient accès au scrutin, puisque la distribution de jetons étaient impossible) et par les conditions d'organisation des scrutins (problème de coût). Le processus d'intéressement a ainsi « débordé » le cadrage initial des concepteurs de l'utilisateur-citoyen comme utilisateur-autonome et citoyen-imaginé. Comme le précédent, ce dispositif était construit selon le modèle de la plateforme, mais les opérations de formulation et de formation des transactions ont été ajustées. Ces ajustements scellaient une alliance entre les concepteurs et les Élus, les premiers revisitant leur problématisation initiale du processus de consultation d'une population au contact des seconds.

2.3.1. Réformer les transactions : coût et politique de la totalisation

*On s'était dit, « alors là le cours, ça fluctue », mais je crois que ça nous coûte 5 ou 6 centimes l'écriture, vote par vote. La création du smart contract, elle est plutôt de 50 ou 60, d'éditer le scrutin. Mais en one by one, les 6 centimes, au moment où c'était un peu plus haut, on avait fait **une simulation à 20 ou 30, on a dit 'ce n'est pas grave', si on facture 1 euro... Mais le marché n'est pas prêt. Enfin le marché n'est pas suffisamment riche, sur du consultatif, c'est-à-dire des sujets du quotidien. Payer 1 euro par tête, par scrutin, c'est mort, ils n'ont pas les moyens. Une commune de 10 000 habitants, ça ne va pas lui coûter... Potentiellement, tous ne voteront pas, mais 10 000 euros, pour un sujet, c'est pas possible. 10 000 euros, déjà, ça dépend de la commune, mais c'est énorme, c'est énorme. Donc on a été confronté à ça, et ça, tu ne peux pas l'anticiper tant que tu n'es pas sur le terrain et face à la réalité, et on a dit : « Il faut que l'on change le truc ».*** (entretien avec Geoffrey, novembre 2018)

Mutualiser pour diminuer les coûts de formation des transactions

La formation des transactions était trop coûteuse avec le MVP ; l'inscription des transactions était un facteur de production trop cher pour Orange, rendant le prix du service inacceptable pour les Élus. Ce problème a conduit les concepteurs à changer la manière de former les transactions de manière radicale : plutôt que d'inscrire autant de transactions que de votes, une unique transaction serait inscrite pour chaque scrutin. Cette unique transaction « mutualisait » les votes reçus pour un même scrutin. Ces différents votes étaient liés entre

170 Une courte vidéo de présentation est disponible publiquement (Le Vote Officiel 2018).

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

eux par l'application LeVote dans un « arbre de Merkle », la structure informatique des transactions d'Ethereum. En effet, Ethereum ajoute chaque transaction aux autres, de manière similaire à Bitcoin : chaque ajout de transaction est le résultat d'un consensus entre les différents inscripteurs qui se matérialise dans une « chaîne de blocs » structurée en « arbre de Merkle ». La V1 de LeVote produisait cet arbre elle-même durant toute la durée du scrutin, et envoyait les transactions déjà structurées à Ethereum pour inscription de l'ensemble. Le coût d'inscription sur Ethereum devenait alors marginal :

*Qu'est-ce que ça m'a permis de faire ça, cette mutualisation ? On a investi pour le développer, mais ça permet de dire, en gros, ton scrutin à 10 000 euros, pour 10 000 personnes, moi, ça me coûte 1 euro, moi [Geoffrey] LeVote, ça me coûte 1 euro au lieu 10 000, modulo tout ce... donc je **disrupte le marché, enfin pas le marché, mais le modèle**. Je peux dire à un client de commune qui n'a pas beaucoup les moyens, je le rappelle et moi je ne réalisais pas ça avant, pas suffisamment qu'il y avait une **pression budgétaire des collectivités**. Je peux dire à quelqu'un : « Toi, ta commune, c'est combien ? C'est 10 000 habitants, ça va te coûter 1 000 euros, c'est-à-dire 10 centimes par tête » parce que je calcule toujours, c'est le **KPI qu'ils ont en tête**, c'est le nombre d'habitants tu vois. (entretien avec Geoffrey, novembre 2018)*

Ce changement de modèle économique et technique impliquait un serveur intermédiaire, propriété d'Orange, que Salah décrivait comme une « API ». Cette API enregistrait les transactions, les liait entre elles, et envoyait un certificat de vote à chaque votant une fois le scrutin terminé. Cette nouvelle architecture permettait de rendre les coûts d'inscriptions quasiment nuls. Elle permettait aussi de pouvoir absorber un très grand nombre de votes simultanément en comparaison d'Ethereum qui, au contraire, limitait le nombre de transactions par minute en fonction de la taille des blocs (problème dit de « *scalability* » ou de passage à l'échelle, abordé au Chapitre 4). Autrement dit, la mutualisation des transactions avait lieu « *off chain* », expression utilisée pour désigner les opérations informatiques « en dehors de la chaîne » de blocs (par opposition à « *on chain* », sur la blockchain).

Salah : la V1, qu'est-ce qu'elle fait ? Elle mutualise, voilà, on mutualise.

Clément : Off chain, donc.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Salah : Voilà, off chain, c'est-à-dire que l'on va créer l'arbre de Merkle, donc quand tu votes, tu vas voter, on va générer, donc tu vas signer ton vote, tu vas te créer une entrée dans cet arbre de Merkle et à la clôture du scrutin, pas de communication avec la blockchain, par contre à la clôture du scrutin, l'arbre de Merkle ou Merkle root va être créé, d'accord ? Par rapport à tous les votes et c'est cet arbre de Merkle qui est envoyé sur la blockchain, d'accord ? Après le votant, qu'est-ce qu'il va voir ? Quand le scrutin est terminé, il peut récupérer son certificat de vote, seulement à la fin, il ne peut pas le faire avant, parce que l'arbre n'est pas encore construit. Et là, dans ce certificat de vote, il va avoir quoi ? Il va avoir sa signature de vote, son voisinage, et le Merkle root, d'accord ? Et donc il va faire une requête. Qu'est-ce qu'il va donner ? Il va donner toutes les informations, donc sa signature, les voisinages, etc., il va faire une requête sur le serveur LeVote et le serveur LeVote, à partir de ces données, il va calculer le Merkle root et il va le renvoyer. Si le Merkle root renvoyé par le serveur est égal, c'est le même, l'utilisateur peut le voir, c'est le même que le Merkle root qui est dans ce certificat PDF, ça veut dire que son vote il a été ancré, correctement ancré, et pris en compte. Pris en compte. (entretien avec Salah, décembre 2018)

Par conséquent, la gouvernance était transformée : la totalisation des transactions en faits avec la V1 était tout à fait différente de celle imaginée pour le MVP. Dans ce dernier, Orange endossait un nouveau rôle, un rôle d'intermédiaire permettant à des Élus de formuler le scrutin, et à des utilisateurs-citoyens de signer leurs votes comme on signe une transaction Ethereum. Orange et ses serveurs totalisaient le scrutin dans son ensemble. Ainsi, Orange a un rôle tout à fait différent : l'entreprise devenait formulatrice des transactions. L'infrastructure Ethereum totalisait non pas les actions d'utilisateurs-citoyens en votes, mais le scrutin formulé par Orange. Au contraire avec le MVP, les concepteurs concevaient un dispositif de formulation du scrutin de manière à rendre l'utilisateur-citoyen autonome dans le processus de vote, une fois en possession des jetons distribués par les Élus formulateurs des scrutins.

Politique du serveur mutualisateur : un intermédiaire entre Ethereum et l'utilisateur-citoyen

L'utilisation d'un serveur intermédiaire était autant un changement d'architecture informatique qu'un changement de gouvernance par les inscriptions. Salah m'expliquait qu'avec la V1, il n'était plus nécessaire d'utiliser de *smart contracts*. Avec le MVP, le *smart contract* faisait lui-même « des contrôles » et « des vérifications » sur chacune des

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

transactions, de manière « très simple » : il décomptait d'un nombre de votants formulé dans le code au départ chaque vote ou utilisation d'un jeton, jusqu'à ce que le scrutin soit clos, car tout le corps électoral avait voté ou parce que le temps du scrutin était écoulé. Or, le serveur intermédiaire se substituait à ce travail de constitution du scrutin, de la réception des votes à l'envoi de l'arbre de Merkle constitué à Ethereum pour enregistrement.

Ce changement dans la constitution du vote impliquait dans le même temps une nouvelle manière de constituer le corps électoral et d'identification des citoyens. Sans *smart contract* les jetons devenaient inutiles : leur qualité était justement de permettre une relation « sans intermédiaire » entre détenteurs et Ethereum. Le serveur d'Orange assurait lui-même le contrôle des votants et autorisait ou non le vote. Les utilisateurs-citoyens devaient scanner leurs cartes d'identité et indiquer leur lieu de résidence pour pouvoir voter. Le processus électoral n'était ainsi plus entièrement délégué aux Élus, qui avaient la charge de distribuer les jetons à leurs administrés ; Orange ne jouait plus un simple rôle d'assistant à la formulation de scrutin, mais devenait partie prenante du scrutin lui-même en vérifiant la conformité de forme des pièces d'identité.

Clients et concepteurs voyaient dans ce changement d'architecture un affaiblissement des valeurs constitutives du projet de départ, sinon un renoncement. Geoffrey et Salah m'indiquaient tous les deux que des clients continuaient à utiliser le service tel que conçu dans le MVP, quitte à payer plus cher, pour bénéficier de la « transparence » d'un vote inscrit directement sur Ethereum. Denis trouvait le MVP « décevant » : pour lui, le critère de transparence, qualité qui faisait la valeur de la blockchain pour l'inscription du vote, était remis en cause. Sans inscription directe des votes sur Ethereum, il devenait impossible à l'utilisateur-citoyen (« Madame Michu » ci-dessous) de vérifier lui-même son vote avec un outil indépendant d'Orange, ce qu'il appelle un dispositif « du domaine public », comme Etherscan¹⁷¹ :

Denis : En fait, ce qui est stocké vraiment, de manière réaliste, ce n'est pas le résultat de la blockchain mais tous les votes sont agrégés sur un arbre de Merkle, et c'est la racine de l'arbre de Merkle qui est mis sur la blockchain.

171 J'ai utilisé ce dispositif pour l'Annexe 2.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Clément : Donc ce n'est pas chaque vote individuellement.

*Denis : [Il approuve par un geste]. Avec un petit inconvénient, ça a un gros effet déceptif [sic] chez moi, j'ai fait la gueule, c'est que pour vérifier... Ce n'est pas facile de vérifier directement. **Tu ne peux pas aller avec Etherscan vérifier ton vote.** Ça, c'est juste pas possible.*

Clément : Et ça, c'était l'objectif de départ ?

*Denis : Ça m'aurait plu, si tu veux. Mais en fait c'est quand tu te racontes que tu peux vérifier, parce que pour moi **la vérification elle ne tient qu'à partir du moment où tu peux prendre un truc du domaine public** et tu vas aller voir le machin toi-même. Bon cela dit, après c'est une question de négo et de compromis. [...] Moi ce que j'imaginai... **Madame Michu veut vérifier son vote, elle en est parfaitement incapable, mais elle trouve un mode d'emploi sur le site, en disant voilà : va sur Etherscan.** (entretien avec Denis, janvier 2019)*

Par ailleurs et en pratique, le MVP lui-même ne fonctionnait pas exactement comme une DApp, c'est-à-dire sans jouer de rôle d' « intermédiaire ». Le MVP disposait lui aussi d'un serveur intermédiaire entre les utilisateurs réels et Ethereum. Il avait deux fonctions. Premièrement, ce serveur collectait les transactions signées par les utilisateurs-citoyens et les enregistrerait (avec un ID spécifique) avant de les transmettre, une par une, à Ethereum. Ce n'est qu'une fois l'inscription confirmée par Ethereum (la transaction « formée ») que ce serveur intermédiaire communiquait le *hash* au votant pour qu'il puisse vérifier la prise en compte de son vote. Ce serveur tampon, dont le code était gardé secret, fonctionnait comme une boîte noire. Denis m'expliquait que certains prospects, dont la Mairie d'une des vingt plus grandes villes de France, avait refusé d'utiliser le service, car le code de l'application n'avait pas été ouvert. Les concepteurs expliquaient que cette ouverture, bien que souhaitable à terme, n'était pas décidée pour prévenir des problèmes de sécurité.

Deuxièmement, ce serveur traduisait l'intuition de Geoffrey indiquée plus haut : le vote comme une « commodité ». Cette notion suggère un double sens : celle d'être « commode » pour organiser des scrutins, et celle de « produit de base échangeable » (francisation de l'anglais « *commodity* ») quel que soit le scrutin organisé sur la plateforme LeVote. Selon ces deux sens, la vente ou la distribution de jetons était indépendante d'un scrutin donné : le *smart contract* (dans le modèle MVP) acceptait les jetons quel que soit le scrutin organisé.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Le rôle du serveur intermédiaire était de vérifier que le scrutin n'était pas terminé afin d'éviter de perdre des jetons. Ce n'est en effet qu'en interrogeant Ethereum que le décompte du *smart contract* pouvait être connu, une information qui n'était pas fournie aux utilisateurs. Par conséquent et sans serveur de contrôle intermédiaire, certains auraient pu dépenser leur jeton pour rien, induisant des coûts d'inscription (en gas) inutiles.

L'existence plus ou moins évidente d'un serveur intermédiaire dans les différentes versions du service LeVote (le MVP, et la V1) pourtant imaginé comme une DApp témoigne de l'écart culturel entre un Web imaginé « sans les serveurs » à la suite du cofondateur d'Ethereum Stéphane Tual (Atmani 2014), peuplé d'individus utilisant des services de manière autonome par la détention de jetons sans liens directs avec les fournisseurs de services, et les processus des entreprises dont le rôle est précisément de contrôler, pour des raisons commerciales, de protection des données des utilisateurs ou pour garantir un niveau de qualité et de continuité de service. La principale inquiétude de Salah, au moment de l'entretien, était justement de garantir la continuité de service de la plateforme LeVote. Interrogé sur le sens du mot plateforme, Salah me répondait du tac au tac : « une infrastructure avec un serveur ». Il souhaitait qu'Orange se dote d'un nœud Ethereum (partie « formation » de la plateforme), avec les standards de l'entreprise, en remplacement de la solution que lui-même avait mis en place. Cette dernière ne garantissait pas la continuité de service en cas de panne. Il souhaitait également disposer d'un serveur dédié à LeVote (partie « formulation »), car au moment de l'entretien, le serveur hébergeant LeVote était mutualisé avec d'autres projets d'Orange.

2.3.2. (Re)formuler des transactions, (re)constituer un corps électoral

*Moi, mon principal objectif, c'est d'arriver à **faire comprendre pour provoquer le comportement souhaité**. Le comportement, c'est de voter, mais en **s'assurant d'abord que la personne avait bien un intérêt** pour ça et après m'assurer que rien n'y fait obstacle. (entretien avec Fabrice, décembre 2018)*

Partir de l'utilisateur (plutôt que du jeton)

Une part importante du travail de Fabrice consistait à ajuster le script de l'utilisateur-citoyen aux utilisateurs en chair et en os. Il les appréhendait par des enquêtes et des retours d'expérience. Une première étude a été conduite à l'aide de questionnaires en ligne auquel ont répondu une trentaine de personnes¹⁷². Elle visait à obtenir des avis pour concevoir la V1 de LeVote. Fabrice identifiait deux groupes. Le premier était constitué de personnes très enthousiastes. Elles voyaient un instrument de partage, bien que plusieurs d'entre elles indiquaient des problèmes dans la manière de s'identifier par le processus proposé par l'application. Les personnes du second groupe étaient au contraire « furieusement opposées » au service, notamment, car il était proposé par une « société commerciale ». Dans un second temps, Fabrice a conduit « quelques entretiens » avec des « votants », et a identifié trois « profils » : un premier « très *civic tech* » qui voulait voter plus souvent et sur une grande étendue de question, un second occupé qui n'est pas franchement opposé à la démarche mais ne prendra jamais la peine de voter s'il ne comprend pas précisément pourquoi il vote, et un troisième « dans le devoir de vote » mais intimidé par le numérique.

Ces études cherchaient à approcher l'utilisateur-citoyen par des « profils » et un rapport individuel au processus de vote. Ce cadrage individuel et comportementaliste était prolongé par une étude cognitive et ergonomique déléguée par les concepteurs à une société spécialisée appelée Netway. Cette société proposait de relever des « données biologiques » sur 16 personnes soumises à l'utilisation d'un prototype de l'application : « données oculaires » (suivi du mouvement des yeux), « activités cérébrales » (casque), « expressions faciales » (caméra vidéo). Deux scénarii étaient comparés, écran par écran de l'application : un utilisant la méthode d'identification Mobile Connect, l'autre utilisant un module produit par Orange demandant aux utilisateurs de scanner leurs cartes d'identités. Fabrice retenait de cette étude que le votant était en attente d'une « récompense » pour son action de vote, c'est-à-dire qu'il puisse en sentir l'utilité. Fabrice convenait qu'il s'agissait là d'un problème fondamental du vote : l'action est rare et l'adéquation entre les préférences motivant le vote et les conséquences sont rarement nettes.

172 Ce travail a été conduit par une collaboratrice de Fabrice, en stage. Je n'ai pas obtenu d'information concernant la méthodologie.

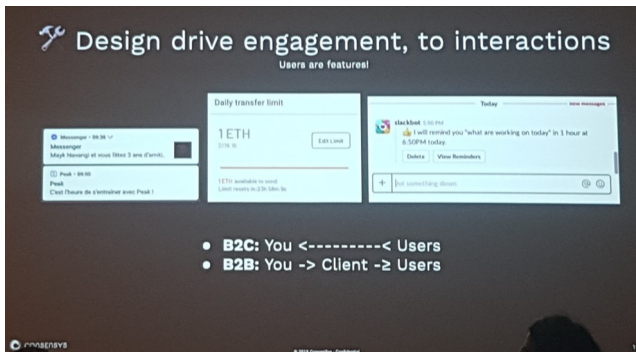


Figure 21 : « Users are features! », Bastien, sep. 2019

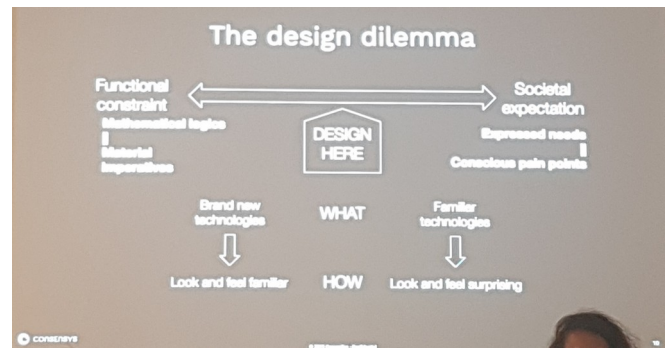


Figure 22 : « The design dilemma », Bastien, sep. 2019

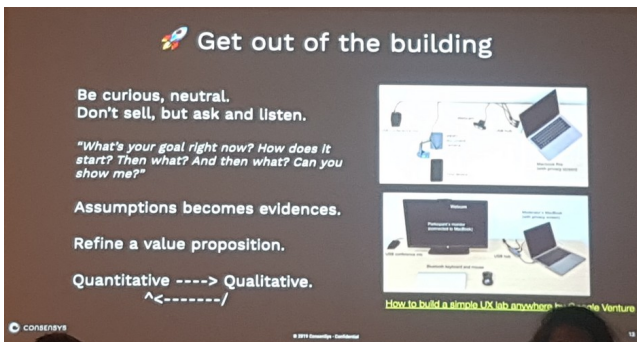


Figure 24 : Enquêter sur l'utilisateur, Bastien, sep. 2019

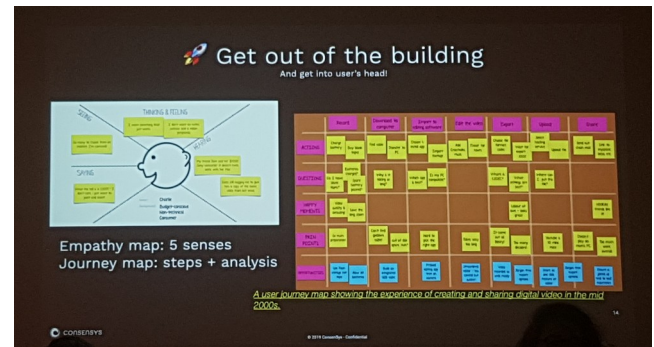


Figure 23 : « Get into user's head! », Bastien, sep. 2019

Les concepteurs cherchaient à appréhender les utilisateurs en chair et en os. Fabrice suivait une approche similaire à celle préconisée par Bastien, autre orateur du meetup de septembre 2019 présentant une « boîte à outils » pour répondre à la question « *How to build a successful Blockchain product* ». La présentation de Bastien était intitulée « *Start with the users, not the token* ». La première partie, dont sont issues les photographies des diapositives reproduites en Figures 21 à 24, décrivait « l'état d'esprit » à adopter pour concevoir un « produit » blockchain, c'est-à-dire implicitement un service bâti avec Ethereum comme en témoigne la Figure 21 : bien que la manière d'obtenir du *feedback* de l'utilisateur était plus compliquée avec les utilisations B2B qu'avec les utilisations B2C, la conception devait être orientée vers l'« engagement » pour favoriser les interactions quel que soit l'usage. Elle devait se situer comme point d'équilibre entre « contraintes fonctionnelles » et « attentes sociales » (Figure 22) qui se trouvait par des enquêtes

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

classiques pour les ergonomes, aussi bien qualitatives que quantitatives, notamment : filmer l'écran de l'ordinateur ou du téléphone de l'utilisateur tout en enregistrant ses verbalisations (« approche conversationnelle »), ou par entretiens (Figure 24).

Ce faisant, les concepteurs de LeVote cherchaient à intégrer l'utilisateur en chair et en os dans le script de l'utilisateur-citoyen. Autrement dit pour Bastien, l'objectif était d'« entrer dans [la] tête » de l'utilisateur (Figure 23) pour faire en sorte que « les hypothèses deviennent des évidences » (Akrich 1987, 1992). Pour être bien conçus, les fonctionnalités des services devaient correspondre aux utilisateurs eux-mêmes : « *users are features* » (Figure 21). Cet ajustement du script de l'utilisateur-citoyen passait, pour Bastien, par la conception de fonctionnalités dans les *smart contracts*. La méthode de conception montre la proximité des opérations de formulation prenant différentes formes techniques, alors que Fabrice ne travaille plus avec des *smart contracts* depuis le changement dans la manière de former les transactions en raison des problèmes de coûts.

Enrôler l'utilisateur en formulant le vote « simplement »

Les études de Fabrice étaient traduites pour concevoir la formulation *via* l'interface de l'application : elle devait faire que l'utilisateur se « fasse entendre » en incitant à l'utilisation du service le plus fréquemment possible. La simplicité d'utilisation devenait centrale : elle permettait aux concepteurs d'enrôler les utilisateurs en « diminuant l'écart entre attendu et réalisé » du vote. En effet, les concepteurs voyaient l'acte de vote comme un effort en soi, une peine qui devait être commensurable avec et compensée par l'espoir d'un impact sur le monde (le « réalisé » conséquent du vote). En simplifiant l'utilisation, les concepteurs réduisaient l'effort d'utilisation, donc l'écart entre attendu et réalisé (quel qu'il soit), et favorisait la réutilisation future de l'application. Denis voyait deux obstacles au recours systématique au vote en démocratie. D'une part, des causes qu'il appelait « endogènes », propres aux processus démocratiques ; en l'occurrence, avec le vote électronique, les « frictions » dans la possibilité de voter. D'autre part, les causes « exogènes », c'est-à-dire le manque de motivation et d'implication propre à ses contemporains qu'il constatait, sans trouver de solution technologique.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

La simplicité d'utilisation allait avec un changement de dispositif de formulation des votes convergent avec le changement dans la méthode de formation des votes (des jetons au serveur). Avec le MVP, l'utilisateur-citoyen se trouvait devant un ordinateur, ou devant tout dispositif permettant de cliquer sur un lien URL qu'il recevait par courriel. Avec la V1, il était utilisateur de smartphone. En confiant le rôle d'identification des votants au serveur intermédiaire entre Orange et Ethereum avec la V1, Orange avait toute la latitude pour concevoir l'ensemble du « parcours de vote » dans une application dédiée. L'utilisateur-citoyen n'était plus en attente des jetons communiqués d'un Élu nécessaires pour voter sur une plateforme ouverte à la manière d'un Doodle ou d'un Change.org, mais s'identifiait avec sa carte d'identité au service LeVote par une application dédiée disponible sur les magasins d'applications d'Android ou d'Apple.

Ainsi, la constitution du corps électoral n'était plus produite par l'Élu, contraint de distribuer des jetons, par le citoyen qui devait « s'enroller ». Cet anglicisme vient de s'inscrire (*enrol*), mais elle résonne avec la notion d' « enrôlement » de la sociologie de la traduction : l'application était construite pour que l'utilisateur-citoyen scelle l'alliance avec l'Élu et Orange par sa carte d'identité. Les Élus pouvaient librement mettre des dispositifs de vote à disposition de leurs administrés, comme des tablettes en libre service dans des bâtiments des administrations publiques. En scannant leurs cartes d'identités, les utilisateurs-citoyens recevait un identifiant unique (un « *hash* ») obtenu à partir des informations contenues sur la carte d'identité, permettant à l'utilisateur de retrouver ses informations en scannant sa carte d'identité sans qu'aucune information personnelle ne soit conservée sur le serveur d'Orange. Ainsi, le vote restait anonyme et minimisait le traitement de données personnelles.

Développer l'application comme un lien durable entre Élus et administrés

Contrairement à ce que pouvait laisser penser le modèle initial de l'application, selon lequel l'utilisateur-citoyen était en situation d'autonomie face à différents scrutins publiés sur une plateforme, la V1 était plutôt imaginée comme renforcement du lien entre administrés et Élus. L'enrôlement de ces derniers s'est imposé comme un point de passage obligé pour

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Orange, et avec eux, un cadrage du rapport entre citoyen dans son rapport aux Élus plutôt qu'une agrégation d'individualités connectées par des outils numériques. Geoffrey admettait que ce changement n'avait pas été évident à accepter, mais qu'il fallait s'y résoudre à la suite des différentes études et retours de terrain, en partie conduits par Fabrice :

*En fait on a travaillé sur les motivations psychologiques de base, et la quintessence pour un votant, citoyen, c'est 'j'existe, en gros ma voix compte, j'existe, et j'ai un impact sur mon quotidien'. Donc **tout le folklore d'une plateforme avec tous les scrutins du monde entier, ça fait plaisir à [Geoffrey], mais en fait, ça ne répond pas au problème et à l'envi du citoyen, et c'est ça le plus important. En fait, avaler, ravalier son égo et sa fierté et travailler pour les gens, faire des services pour les gens, et pas pour le kiff, je l'ai fait et je me faisais bananer soit par mes clients, donc faire un service pour les gens et c'est pour ça, comme tu le fais, c'est important d'interroger les gens. L'incarnation et trouver la bonne solution face à un vrai problème.** (entretien avec Geoffrey, novembre 2018)*

L'interface elle-même devait rapprocher Élus et administrés. Le travail de diminution de « l'écart entre attendu et réalisé » du vote n'était pas uniquement une préoccupation des concepteurs portée sur les utilisateurs-citoyens. Elle concernait également les Élus eux-mêmes, considérés comme garants du « réalisé ». L'Élu pouvait voir son autorité déstabilisée par un outil de « consultation » qui n'était pas « légal » ou « engageant ». Selon Fabrice en effet, l'Élu se mettait en difficulté dans le cas où les administrés ne voyaient pas de conséquences aux consultations. Fabrice envisageait en conséquence de développer une interface permettant aux Élus de publier les résultats des scrutins. De cette manière, il imaginait un unique canal de communication fonctionnant à double sens entre citoyens et Élus, afin que ces derniers puissent rendre des comptes aux premiers.

L'application avait également la charge de maintenir le lien entre Élus et administrés entre deux scrutins. Le passage d'un fonctionnement par mail et sur ordinateur à l'application mobile permettait de solliciter les utilisateurs-citoyens qui s'étaient « enrôlés » par des notifications. La communication des Élus organisateurs de scrutins devenait nettement plus simple et économique que la traditionnelle utilisation de tracts papiers et de mise à disposition de bureaux de votes. Pour Denis, le *push* permettait de réduire les « frictions »

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

entre Élus et citoyens. Geoffrey me donnait l'exemple de la Commune B comme illustration de l'efficacité de la communication avec l'application. Cette commune avait non seulement atteint les 3 % de participation, taux indicatif de satisfaction des Élus, mais surtout un taux de 95 % de participation au scrutin parmi les 800 électeurs qui s'étaient enrôlés par l'application.

Enfin, elle permettait de filtrer les participations aux scrutins, bien que le modèle du « secret du vote » initialement imaginé avec le cryptage des transactions sur la blockchain et le stockage vote par vote ait été abandonné avec le choix de mutualiser les transactions. Le vote était rendu anonyme plutôt que « secret » par l'application qui, lors de chaque « enrôlement », créait un *hash* ne permettant pas de retrouver l'identité de l'utilisateur. Une fois « enrôlés », les utilisateurs-votants ne pouvaient voter qu'aux scrutins correspondants à leur lieu de résidence déclaré. Le changement de lieu de résidence était possible sur simple déclaration, mais tout changement bloquait le lieu de résidence pendant trois mois pour éviter les « fraudes ». Cette solution répondait imparfaitement mais de manière satisfaisante à la préoccupation des concepteurs voyant dans l'empêchement de la fraude une condition de réussite du service, ainsi qu'une manière de répondre à la demande de certains Élus qui souhaitaient limiter la participation aux scrutins à des administrés réels, c'est-à-dire qui payaient des impôts. Fabrice admettait volontiers que la question « qui a le droit de voter ? » n'avait pas de réponse définitive en dehors de l'intuition « je ne vote qu'une seule fois », et que les réponses intermédiaires étaient les résultats d'ajustements qui avaient émergé au cours de la conception de l'application.

Conclusion de la section : la plateforme, dispositif de gouvernance modalisable

Cette section a commencé par distinguer deux significations que les concepteurs donnaient à la notion de « plateforme ». D'une part et de manière comparable au sens identifié par les gestionnaires travaillant sur les « écosystèmes d'affaires », la plateforme est un support qui assemble l'écosystème. Ce sens est incarné par Ethereum comme « plateforme de DApps »,

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

mais il se retrouve aussi dans Ethereum comme logiciel pour utilisations B2B. Ethereum était dans les deux cas le support commun qui articulait les acteurs rassemblés en écosystème. D'autre part, la « plateforme » était un horizon organisationnel qui se retrouvait aussi bien dans les utilisations B2C que B2B : un dispositif de totalisation de relations entre individus.

Ces deux significations se lisaient dans la manière dont les concepteurs pensaient leur propre organisation. D'une part, l'organisation de la diffusion des pratiques de conception sur Ethereum (entrepreneuriales et de développement) par les meetups, qui résonne avec le cas LeVote, indique qu'Ethereum était une plateforme au sens de support commun de l'écosystème. Ces pratiques faisaient de la plateforme un modèle générique d'organisation économique : concevoir une plateforme pouvait tout autant être une utilisation B2B ou B2C, dépendant d'un choix politique, commercial et technique. D'autre part, le concepteur de DApp était imaginé comme un travailleur « autonome », seul face à un monde du travail avec lequel il forme une succession de relations contractuelles, que ce soit dans des « organisations décentralisées » ou comme « indépendant ». Les concepteurs cherchaient à faire advenir ces relations de travail par des plateformes. Deux cas de plateformes ont été énoncés, chacun proposant une gouvernance par la formation des transactions : une DApp, et une plateforme type client-serveur. Malgré les différences de gouvernance de la formation qu'elles impliquaient, la plateforme était imaginée, dans ces deux cas, comme une infrastructure qui garantissait à l'utilisateur une capacité de formulation autonome.

Le service LeVote d'Orange témoigne à la fois de la force heuristique de la plateforme dans la conception de services numériques, et de l'ampleur des modalités de gouvernance qu'elle offre. Dès le départ, les concepteurs adoptaient le modèle de la plateforme en imaginant LeVote comme une DApp. Ils alignaient leur plateforme de vote avec Ethereum : les votes étaient imaginés comme des transactions formées « une à une » par Ethereum. Cette formation des transactions les rendaient « transparentes », faisait converger le citoyen-imaginé avec l'utilisateur-autonome. Le travail des concepteurs consistait à rendre le vote paramétrable pour un large éventail de clients, des Élus des différents échelons territoriaux aux délégués d'entreprises, en concevant un *smart contract* et une interface génériques.

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Cette généricité permettait d'imaginer le jeton comme un droit au porteur, commercialisable indépendamment de chaque scrutin et de chaque client.

La robustesse du modèle de la plateforme se comprend par la plasticité des opérations de formation et de formulation des votes. L'alignement entre l'infrastructure publique Ethereum et la plateforme LeVote n'a pas résisté à l'épreuve de l'intéressement des Élus, conduisant les concepteurs à ajuster les opérations de formation et de formulation des votes, sans toutefois renoncer au modèle de la plateforme. D'une part, les Élus attendaient un coût raisonnable, incompatible avec la formation des votes par Ethereum qui devait impliquer Orange pour réduire les coûts. D'autre part, ils étaient incapables de constituer un corps électoral par une liste de courriels qui était nécessaire pour formuler un scrutin selon le cadrage initial. Les concepteurs ont changé de modèle (« disrupté », dans l'extrait ci-dessous) : LeVote restait une plateforme, mais les transactions prenaient de nouvelles significations, aussi bien dans leur formation que leur formulation. Ethereum ne formait plus des votes d'utilisateurs-citoyens, mais des scrutins d'Orange. Les utilisateurs-citoyens s'éloignaient des utilisateurs-autonomes imaginés au départ. De détenteurs d'un jeton dont ils disposaient de manière indépendante, ils étaient enrôlés *via* une application mobile imaginée pour renforcer le lien avec leurs Élus en formulant les scrutins « simplement ».

Geoffrey : *'Attendez, vous avez **un moment qui est un peu off chain** et puis il n'y a pas le secret absolu du vote...'* Attendez, on est sur du consultatif. [...] Là, on fait entrer l'usage... Ce ne sont pas des sujets d'élection de mandat du Président de la République. C'est est-ce que l'on met un pot de fleurs, de l'éclairage, ou on met un sens interdit sur l'avenue, donc **on souffle un coup, on se détend, et l'enjeu est assez faible**. Alors bien sûr, ça concerne notre quartier, mais voilà, ça passe très bien et puis ils se rendent compte aussi que dans le certificat que l'on met, ce n'est pas déconnant, c'est **un vrai arbre de Merkle avec les hashes de tous les bulletins, il y a quand même du taf**, mais on mutualise, en one shot sur la blockchain.

Clément : *Du coup, ça, tu le discutes avec les clients ou pas ?*

Geoffrey : *Non.*

Clément : *Pour eux, c'est transparent ?*

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Geoffrey : C'est transparent, ils ne vont jamais aussi loin.

L'échec du MVP s'explique par une différence de problématisation entre les concepteurs d'une part, et les Élus et citoyens, d'autre part. Les concepteurs problématisaient le processus démocratique lui-même, en opposant à ses formes actuelles un contrôle de bout-en-bout : l'utilisateur devait être capable de vérifier, de manière autonome, que son action était bien totalisée, de manière « transparente » ; comme les acteurs de l'écosystème qui problématisaient l'émancipation de structures formelles contrariant leur indépendance et leur autonomie, les concepteurs de LeVote projetaient sur le système démocratique une méfiance vis-à-vis d'organisations qui dépassent la toute-puissance individuelle. Pour les concepteurs, il était central de séparer formation et formulation des transactions pour assurer « unicité » et « transparence ». Or, ce problème n'était pas celui des Élus et des citoyens qui ne problématisaient pas le processus démocratique : « ils n[']allaient] jamais aussi loin » (extrait ci-dessus). Eux cherchaient une solution sûre, craignant la fragilité des outils numériques en général, et voyaient la blockchain comme la meilleure garantie, éventuellement espéraient en faire un outil simple de lien régulier.

Des travaux de sociologie politique montrent que le caractère secret du vote est le résultat temporairement stabilisé de transformations continues dans le temps et dans l'espace des pratiques et des dispositifs (Crook & Crook 2011, Garrigou 2012). Si le secret du vote paraît naturel, son instauration en France n'a rien d'évident. Le principe a été énoncé à la Révolution, mais il a fallu attendre la fin du XIX^e siècle pour qu'il soit instauré. Cette innovation ne peut pas se comprendre sans l'apparition de dispositifs comme l'isoloir et le bulletin officiel, ni sans des règlements stricts, par exemple interdisant au président de bureau de vote de toucher l'enveloppe du votant. Ces règles visaient à empêcher différentes irrégularités (fraude, corruption, pression) à une époque qui découvrit le suffrage universel masculin.

Aux yeux des concepteurs, le vote « consultatif » paraissait plus simple *a priori* que l'« électif », car ce dernier nécessitait de remplir un cahier des charges strict. En pratique, la conception du vote consultatif s'est heurtée à un problème d'un autre ordre. Les épreuves

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

auxquelles ont été confrontées les concepteurs témoignent du caractère politique des tissus d'inscriptions qui font exister les relations. Un scrutin n'existe que par différentes chaînes d'inscriptions constituant ce que Jérôme Denis appelle des « infrastructures scripturales » (Denis 2018), de l'inscription des électeurs sur des listes électorales au dépouillement des bulletins. La gouvernance par la formation et la formulation dans le MVP garantissait le secret du vote mais ne se superposait pas avec l'infrastructure scripturale de vote réelle, avec laquelle les Élus raisonnaient.

Conclusion du chapitre

Ce chapitre montre que les différentes organisations économiques imaginées avec Ethereum (B2B et B2C) désignaient des modalisations d'une technologie de gouvernance qui rendait ajustable le contrôle sur les relations par deux opérations, la formation et la formulation des transactions. Les entreprises ou institutions réunies en consortia étaient à la fois les formatrices et les formulatrices des relations. La formulation des relations était connue à l'avance (le cas d'usage, le besoin « métier », ou le « point de douleur »), le problème étant de former les relations ou de « prouver le concept » de la blockchain en fonction des impératifs de contrôle par l'infrastructure. Avec les utilisations B2C, les startups et d'autres acteurs économiques (comme Orange) imaginaient réduire leur rôle à la formulation de transactions, la formation étant déléguée à l'infrastructure publique à la gouvernance *ad hoc*. La manière de former les transactions était posée en avance, la formulation restait à inventer suivant des tendances (« Web3 » ou « finance décentralisée ») ou de manière spécifique, comme le fait Orange avec LeVote.

Ces deux types d'agencements économiques avaient en commun le modèle de la plateforme. L'écosystème était constitué de concepteurs de plateformes quelle que soit l'utilisation de la technologie, en B2C ou B2B. Les processus de conception ne posaient pas toujours d'emblée une manière de former les transactions, ou d'inscrire, comme le font les plateformes numériques traditionnelles à la main d'une société qui ouvre une part de programmabilité à des acteurs extérieurs *via* des API. Ces plateformes étaient des mises en œuvre d'une technologie de plateformes, qui rendait ajustable la manière de former et de formuler les transactions, c'est-à-dire de gouverner les relations par les inscriptions et par les fonctions. Ainsi, la distinction que je fais entre ces deux types d'opérations avec Ethereum peut être utile à l'analyse de la gouvernance de relations par les plateformes du Web, mais aussi à d'autres plateformes moins visibles. Elle pourrait par exemple être utile pour analyser la gouvernance de plateformes structurant la finance mondiale. Analyser leurs innovations en matière de formation et de formulation des transactions pourrait informer sur leur politique. À titre d'exemple, la société de conseil Accenture et la banque Société

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

Générale se sont associées dans une joint-venture, à laquelle était déléguée la gestion du *back-office* de la banque ; c'est-à-dire, l'ensemble des processus de formation des transactions formulées par différentes entités ou clients.

Le vocabulaire analytique proposé dans ce chapitre troque le point de vue de l'utilisation (quelle organisation économique est conçue avec Ethereum) celui des opérations objet du processus de conception. Les utilisations B2C et B2B se développent en même temps et de manière intriquée. Ces développements sont le résultat d'un travail de constitution de l'écosystème au sein duquel circulent des pratiques entrepreneuriales et technologiques.

Ce chapitre s'est concentré sur le rôle de ConsenSys, dans son entreprise de technologisation de l'infrastructure (section 1) ainsi que dans la diffusion des pratiques dans les meetups (section 2). Ces développements permettent de relire des éléments présentés au Chapitre 2. Les jetons d'ICO, utilisation canonique B2C, sont émis sur l'infrastructure publique. Avec le Dauriel Network, ConsenSys proposait à des institutions de faire des jetons des titres financiers ou *security tokens* en ajustant formation et formulation simultanément. Le standard ERC-1400 était conçu pour faciliter la formulation de manière homogène à l'échelle de l'industrie financière, et de l'améliorer en étendant leur connaissance de leurs actifs aux détenteurs de leurs titres. Différentes manières de former les transactions étaient imaginées, mêlant inscription sur l'infrastructure publique et préparation des transactions dans des infrastructures séparées pour apporter confiance et fiabilité à des institutions qui devaient contrôler leurs émissions.

Deux utilisateurs étaient imaginés dans la conception des plateformes. L'un était spécifique au service imaginé, l'autre était un utilisateur générique d'Ethereum. Le travail de ConsenSys était orienté par la généralisation de cet utilisateur dans le développement de briques et de produits d'infrastructure à différents acteurs de l'économie numérique (section 1). Dans la conception du service LeVote, cet utilisateur générique (utilisateur-autonome) participait à définir le script d'un citoyen-imaginé. Ce dernier jouait un rôle actif : c'est sur son modèle qu'était développé le MVP. Malgré son incapacité à payer les concepteurs, à la différence des utilisateurs en chair et en os qu'étaient les Élus et par leur intermédiaire les

Chapitre 3. Technologie de plateformes, modalisations de la gouvernance

citoyens, cet utilisateur-autonome continuait à se faire entendre : d'une part, les concepteurs continuaient de chercher à jouer un rôle minimal dans la formation des transactions en faisant d'Ethereum la chambre d'enregistrement du scrutin dans son ensemble sur l'infrastructure publique, bien que techniquement intermédiaire ; d'autre part, ils continuaient de le faire exister en se lançant dans la conception d'un service de vote « électif » susceptible de permettre à l'utilisateur-autonome d'enregistrer directement son vote, cette fois sans intermédiaire.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Introduction : l'autonomie de l'infrastructure comme objet plutôt que principe

Les blockchains sont généralement vues comme des dispositifs « autonomes », par là susceptibles de devenir de systèmes contractuels indépendants des régimes juridiques des États. Ce chapitre analyse cette autonomie comme le résultat d'associations temporairement stabilisées entre différents acteurs. La « communauté Ethereum » était au cœur de ce processus de stabilisation. Cette introduction détaille ces éléments et énonce la question qui guide ce chapitre. Enfin, l'argument et le plan du chapitre sont présentés et annoncés.

Les smart contracts, des « lois »

La formule « la loi est code » (*law is code*) ramasse la promesse des *smart contracts* du point de vue du droit : remplacer les lois des États et des gouvernements (De Filippi & Hassan 2016). De manière comparable à l'apprentissage profond (*deep learning*), la blockchain serait une technologie de production de règles ayant force de loi, en automatisant son application (Hassan & De Filippi 2017). Les gouvernements pourraient eux-mêmes s'emparer de ces objets pour favoriser le développement de « normes sociales » vis-à-vis de la technologie ou directement pour mettre en œuvre et appliquer des lois sur une plateforme de *smart contracts* (De Filippi & Wright 2018, 2019). Ainsi, les *smart contracts* auraient les qualités d'« accords légaux » d'une forme nouvelle. À ce titre, il ne faudrait « pas les décourager » (Raskin 2017), témoins de l'importance du droit des contrats dans nos sociétés (Werbach & Cornell 2017).

« *Law is code* » renverse la formule du juriste Lawrence Lessig qui, au tournant du millénaire, nommait par « *code is law* » l'importance nouvelle et grandissante de

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

l'architecture technique, des protocoles, des standards ouverts d'Internet et du Web balbutiant, dans la régulation des communications numériques (Lessig 2000). Ce renversement n'est pas nouveau. Lionel Maurel le pointait déjà en 2014 explicitement. L'auteur pointait la tendance à inscrire dans ces objets, bâtis sur des bases antagonistes de celles ceux de la propriété intellectuelle, des lois sur le droit d'auteur avec les *Digital Right Management* (DRM) ou des algorithmes de surveillance comme le ContentID de Youtube (Maurel 2014). Comparée aux DRM, la blockchain a été analysée comme un nouvel instrument de contrôle capitaliste sur les relations numériques remplaçant les lois des États (Käll 2018) ou comme un prolongement des lois sur la propriété intellectuelle (Bodò et al. 2020).

Une vaste littérature transdisciplinaire a pris au sérieux cette formule en interrogeant la capacité des *smart contracts* à être reconnus en lieu et place de contrats légaux. Ce que certains appellent un « nouveau champ juridique » analyse ces instruments « d'ingénierie juridique » en termes de traductibilité du langage juridique en langage calculatoire, pointent l'importance de mécanismes de résolution des conflits ou de conditions d'application de la loi (Goldenfein & Leiter 2018). Cette perspective ramène les contrats légaux à des artefacts techniques qui automatisent des règles, alors que les premiers sont des « ressources sociales » dont la mobilisation ne peut se comprendre qu'en contexte pratique (Levy 2017). Elle rejoint une discussion plus large sur une tendance de l'activité juridique à devenir une activité de « codage » dans la forme d'actifs, étendant les droits de propriété et accroissant les inégalités (Pistor 2019). Katharina Pistor voit dans les blockchains et les *smart contracts* la rencontre entre le code informatique et le « code légal » des juristes. L'originalité de ces objets tient non seulement dans la représentation d'un contrat mais aussi à leur matérialisation par leur capacité « auto-exécutante » à livrer des biens, services, ou monnaie numérique, sans qu'une cour de justice soit nécessaire (Pistor 2019 : 183-204). Des travaux en sciences informatiques participent à cette convergence, par exemple en concevant des dispositifs permettant de tracer les différentes versions d'un smart contrat sur Ethereum afin de rapprocher ces algorithmes des « contrats légaux » du « monde réel », ces derniers devant pouvoir être modifiés (Kafeza et al. 2020). Enfin, des auteurs en sciences de

l'information et de la communication expliquent la « lente adoption » des *smart contracts* par des « écarts » entre l'état du développement informatique et les « impératifs » du droit, qu'ils pointent pour améliorer cette convergence (Drummer & Neumann 2020).

L'autonomie des blockchains, acquise par principe ?

L'autonomie des blockchains est supposée dans la formule « *law is code* » et dans ces différents travaux qui accordent aux *smart contracts* des « capacités » d' « auto-exécution » et d' « auto-application ». Cette autonomie serait garantie par le protocole informatique lui-même :

*With blockchains, people can construct their own systems of rules or smart contracts, enforced by the underlying protocol of a blockchain-based network. These systems create order without law and implement what can be thought of as private regulatory frameworks—which we will refer to throughout the book as *lex cryptographica*. They endow software developers with the power to create tools and services that avoid jurisdictional rules and operate transnationally to coordinate a range of economic and social activities.* (De Filippi & Wright 2018 : 5)

Le protocole est le fondement d'une « *lex cryptographica* » constituée des règles privées des *smart contracts*. Elle serait transnationale et indépendante des systèmes juridiques (Wright & De Filippi 2015 ; De Filippi & Wright 2018, 2019) à la manière de la « *lex informatica* », qui désigne des ensembles de règles contractuelles comme les « *Terms of Use* » régissant les relations entre fournisseurs de services et clients de services Internet, ou les licences des logiciels libres et open source et Creative Commons, en réponse aux règles sur le copyright. Ce concept étend à Internet le principe de « *lex mercatoria* », que les auteurs définissent comme un système universel de règles qui s'appliquent de manière égale à tous, indépendamment de la juridiction, depuis le Moyen Âge¹⁷³ (Wright & De Filippi 2015 : 46).

La « *lex cryptographica* » nous ferait entrer dans un nouveau régime juridique, le « *rule of*

173 Des historiens contestent de voir une continuité historique entre la « *lex mercatoria* » et le commerce au Moyen Âge, comme le font les auteurs, privilégiant l'hypothèse du développement simultané de juridictions commerciales spécifiques aux villes (Volckart & Mangels 1999).

code » (De Filippi & Wright 2018), susceptible de se substituer au « *rule of law* », concept anglo-saxon proche de celui d'État de droit. Selon les auteurs, ce régime ferait advenir une nouvelle organisation économique et sociale, opposée aux « systèmes bureaucratiques et institutions » qui imposent une « gouvernance sociale » s'appuyant sur la loi et la hiérarchie pour structurer la société. Ces analyses juridiques convergent avec des analyses d'économistes de la « nouvelle économie institutionnelle » qui voient les blockchains comme des « ordres constitutionnels », au sens de « systèmes de règles dans lesquels les individus (ou firmes, ou algorithmes) peuvent faire des échanges économiques et politiques » (Berg et al. 2018) ou comme des « catallaxies constitutionnelles », c'est-à-dire des systèmes de coordination excluant toute possibilité de contestation par une quelconque « autorité » qui s'opposerait à la formation de relations sociales fondées sur la seule contractualisation interindividuelle (Berg et al. 2020).

L'autonomie, résultat d'alliances temporairement stabilisées

Or, qualifier d' « autonome » l'infrastructure par la seule existence du protocole revient à prendre au pied de la lettre l'ambition des concepteurs des blockchains (Chapitre 1, section 1). Le développement d'Ethereum et des DApps (applications décentralisées et « autonomes ») résulte en pratique de l'ancrage bien réel des concepteurs de l'écosystème dans le monde où règne la loi des États et des gouvernements. Au Chapitre 2, j'ai pointé les articulations entre différentes formes d'argent qui ont permis de faire circuler et de valoriser les cryptoactifs, lesquels ont fait le succès entrepreneurial et la diffusion des *smart contracts* jusque dans les laboratoires de chercheurs en droit et en économie. J'ai également pointé l'importance pour les représentants de l'écosystème français de préserver les cryptoactifs de définitions réglementaires menaçantes pour leur développement, que ce soit par des activités de lobbying ou par la définition de standards spécifiques. Au Chapitre 3, j'ai indiqué le rôle actif de ConsenSys dans le développement d'Ethereum, développant l'écosystème tous azimuts autour d'outils intégrés dans une « pile », là aussi favorisant l'émergence des *smart contracts* comme des instruments prometteurs pour des acteurs comme Orange.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

En pratique, l'autonomie était le résultat temporairement stabilisé d'alliances entre différents acteurs. Ces alliances étaient régulièrement discutées, notamment à l'occasion des mises à jour du protocole réseau, appelées « bifurcations » (*forks*)¹⁷⁴, par la « communauté Ethereum ». En France, la communauté¹⁷⁵ était représentée par l'association Ethereum France. Ses membres organisaient ou participaient à des meetups et des conférences (comme EthCC), publiaient de la documentation et des articles de vulgarisation en ligne, intervenaient à titres d'experts dans différentes arènes. Par exemple, l'association a organisé un meetup dédié à une problématisation de l'infrastructure importante à cette époque : l'insuffisance de la fréquence d'inscriptions de transactions de l'infrastructure, ou « passage à l'échelle ». Jean expliquait :

Alors, le problème du débat sur la scalabilité c'est, effectivement, on veut plus de transactions par seconde sur notre blockchain, mais on veut surtout pas faire de compromis sur la décentralisation. Et malheureusement quand on a une chaîne avec beaucoup de nœuds, un réseau très dense, on est toujours limités par le nœud le plus faible. Le nœud le plus faible doit toujours recevoir les transactions et exécuter ces transactions. Du coup, ben si le nœud n'est pas suffisamment puissant pour encaisser le flow des transactions, il va ramer et puis vous allez perdre la décentralisation à mesure que vous voulez grossir votre volume de transactions. (Jean, meetup #2, juin 2018)

Ces alliances étaient au cœur des problématizations de l'infrastructure par la « communauté ». À l'époque du verbatim ci-dessus par exemple, Ethereum était victime de son succès. Jean prenait le rôle de porte-parole de la communauté pour poser le problème (« on veut plus de transactions par seconde ») tout en appelant à ne pas perdre de vue ce qui fait la sécurité de l'infrastructure (« on veut surtout pas faire de compromis sur la décentralisation »). Concilier les deux impératifs relevait du casse-tête : des modifications du protocole changeait à la fois les fonctions de la chaîne (comme la fréquence de validation des transactions) mais aussi la manière de mettre les différentes parties prenantes en relation (notamment *miners* et utilisateurs).

174 La liste des principales évolutions était disponible ici : <https://ethereum.org/fr/history/>.

175 Dans ce qui suit et sauf précision contraire, « communauté » employé sans guillemets désigne la « communauté Ethereum ».

La communauté : groupe problématisant la construction de l'infrastructure

Au nom de quoi ces alliances étaient-elles ajustées, et plus généralement, au nom de quoi les acteurs réunis en communauté agissaient-ils collectivement ? Cette question guide ce chapitre dans lequel j'analyse l'autonomie comme résultat d'un effort de mise en relation entre différents groupes. Il nuance la proposition consistant à voir Ethereum comme un système autonome par construction, selon laquelle l'infrastructure serait utilisée et laissée intacte par un écosystème extérieur de concepteurs et d'utilisateurs.

La communauté rassemblait un ensemble d'acteurs aux activités très variées. Derrière le singulier employé avec « la » communauté existaient différentes communautés de développeurs et d'utilisateurs de logiciels open source (comme les logiciels « clients » des *miners* ou les *wallets* des utilisateurs, les standards de *smart contracts* et plus généralement le processus EIP¹⁷⁶), chacune disposant d'outils spécifiques de coordinations (mailing-lists, espaces de discussion en ligne) et d'espaces de rencontres lors de conférences internationales. Au sein de cette communauté existaient également des communautés en ligne de production de pair-à-pair, notamment d'articles de blogs, de documentation technique ou entrepreneuriale. Dans le même temps, cette communauté rassemblait des individus interagissant sur de multiples forums, des membres d'associations locales se retrouvant régulièrement en meetups, ainsi que des passionnés et des entrepreneurs se retrouvant lors de conférences internationales.

Les études sur les communautés de développement logiciels *open source* et de productions collaboratives en ligne ont mis en évidence différentes formes de régulation et d'organisation des activités communautaires (Benghozi 2006 ; Demazière et al. 2006 ; Cardon & Levrel 2009). Ce type d'analyse nécessite de voir le travail organisationnel émerger, typiquement dans des cours d'action (Demazière et al. 2011). Dans ce chapitre, je poursuis un autre objectif. Je suis attentif à la manière dont cette communauté de communauté problématise le développement d'Ethereum dans son processus de

176 EIP désigne les *Ethereum Improvement Proposals*, introduits au Chapitre 2.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

construction, à partir d'observations en ligne et en conférences.

Je comprends la communauté comme ensemble d'individus et d'organisations qui ont participé au développement d'Ethereum au sens d'infrastructure (Star 1999). Leigh Star approche les infrastructures en relation avec des pratiques organisées, en les situant culturellement, de manière à faire émerger le sens qu'elles ont pour les acteurs en présence. Par exemple, pour un cuisinier, le système d'alimentation en eau est une partie de l'infrastructure de production d'un plat ; pour un administrateur municipal du réseau, il s'agit d'une variable à intégrer dans un processus de maintenance. L'étude de la formation et du développement des infrastructures permet à Star d'analyser la politique des acteurs en présence.

Dans ce chapitre, je repère différents problèmes posés par la communauté dans la construction de l'infrastructure. À l'image du court extrait reproduit ci-dessus avec Jean, les problématisations de l'infrastructure étaient politiques, au même titre que les décisions d'encodage ou de standardisation (Star 1999 : 382). Suivre les acteurs de cette communauté plurielle et aux contours flous me permet d'identifier les problèmes pertinents qu'elle se pose, le « pourquoi » du fonctionnement de cette infrastructure numérique (Musiani 2018 : 161), et corrélativement la communauté qui la prend pour objet.

Ces problèmes et les controverses associées concernaient aussi bien les finalités ou fonctions de l'infrastructure (ses usages réels ou imaginés) que les principes d'action collective sur l'infrastructure. Elle agissait comme un « public récuratif »¹⁷⁷ : un groupe qui agit sur les « profondeurs ou les strates » de l'infrastructure pour expliquer les fondements de sa constitution en tant que groupe et travaillant en relative indépendance (Kelty 2008). Christopher Kelty voit chez les publics récuratifs un « imaginaire social » d'un ordre moral et technique au travers duquel sont prises les décisions collectives. Cet imaginaire définit

177 L'anthropologue et chercheur en sciences de l'information Christopher Kelty analyse la signification culturelle du logiciel libre et open source avec la notion de « public récuratif » qu'il définit comme : « *a public that is vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public; it is a collective independent of other forms of constituted power and is capable of speaking to existing forms of power through the production of actually existing alternatives* » (Kelty 2008 : 3)

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

« une relation particulière entre technologie, organes de gouvernance (État, entreprise, ou non-gouvernemental), et Internet » (Kelty 2008 : 12).

Terrain mobilisé dans ce chapitre

Je m'appuie sur des observations de meetups et conférences, en particulier la troisième édition de l'« *Ethereum Community Conference* » (EthCC¹⁷⁸ dans la suite du texte). L'association Ethereum France, organisatrice de l'événement, décrivait EthCC comme un « événement par la communauté, pour la communauté » qui « n'a pas d'objectif commercial ou publicitaire » et « pour seul but de développer l'écosystème », par le « partage et [la] transmission des connaissances comme moyens les plus efficaces pour développer un écosystème bienveillant et durable » (Ethereum France 2020). Les personnes souhaitant intervenir candidaient auprès des organisateurs selon un calendrier fixé par ces derniers. Le jour de l'événement, les interventions se succédaient dans des temps formellement définis. Un temps était prévu pour une présentation, suivi d'une séance de questions-réponses.

Cet événement m'a donné, en quelques jours, une vision panoramique de problèmes de la communauté Ethereum, début 2020. Cette conférence se tenait à la Maison de la Mutualité à Paris pendant trois jours, réunissait 224 *talks*, la plupart du temps donné par des intervenants internationaux physiquement présents (à quelques exceptions près, notamment d'intervenants asiatiques, inquiétés par la naissante pandémie). Les 14 *tracks* témoignent de la variété des thèmes de discussion¹⁷⁹. En pratique, il pouvait s'agir de présentations allant d'expérimentations de nouveaux protocoles réseaux à l'exposé de nouveaux algorithmes cryptographiques, aux pitches de startups vantant une idée révolutionnaire jusqu'aux retours d'expérience d'avocats listant des recommandations pour adopter la « bonne attitude » face à un « régulateur ».

178 Abréviation communément employée par les acteurs, à l'écrit comme à l'oral (prononcée [et si si]).

179 Intitulés des différentes *tracks* (et nombre d'interventions associées) : *Blockchain for Good* (12), *Crypto Economics* (17), *dApps / UX / UI* (17), *Decentralized Finance* (34), *Developer Tools* (30), *Enterprise* (14), *Ethereum 2.0* (12), *Gaming* (11), *Governance / DAO* (16), *Other Blockchains* (7), *Privacy* (14), *Scalability* (19), *Security* (18), *Web3* (16), *French Track* (4). La liste complète des interventions était archivée à l'adresse <https://ethcc.io/EthCC3.html> au moment de la rédaction de ces lignes.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Je m'appuie également sur des publications en ligne. Ces dernières m'ont informé de différentes controverses qui ont animé la communauté. Elles m'ont également permis de parcourir un vaste corpus de textes publié sur le site de la Fondation Ethereum, sur Medium ou sur le site personnel de Vitalik Buterin (VB dans la suite du chapitre). Ces textes circulaient, en particulier ceux de l'inventeur d'Ethereum. Elles participaient à une réflexion sur la bonne gouvernance de l'infrastructure. Ces discussions informent, corrélativement, sur les visions des rapports entre individus participant aux actions collectives. La section 2 s'appuie sur des écrits signés VB, souvent rédigés à plusieurs mains (Buterin 2017b, 2018, 2019b, 2021). Leurs écrits s'appuyaient sur de rares expérimentations de tels mécanismes, ainsi que sur la mobilisation de savoirs à la croisée des mathématiques, de la science économique et de la science politique.

Argument du chapitre et annonce du plan

Ce chapitre analyse la tension entre autonomie de l'infrastructure posée comme principe originel et nécessité d'interventions régulières par la communauté en termes de gouvernement. Il prolonge l'analyse proposée au Chapitre 1 dans lequel je proposais de comprendre le protocole comme une « technologie de pouvoir » (Foucault 2004a). Son principe, que j'ai appelé « mystique », tient dans la proposition suivante : une rupture épistémique autour de l'objet « transaction », entre des *miners* qui voient un objet rentable à inscrire et des utilisateurs qui voient une signification calculée inaltérable.

La communauté gouverne la construction de l'infrastructure selon une « raison gouvernementale » (Foucault 2004a) qui est infrastructurelle. L'infrastructure est l'objet que la communauté gouvernante prend pour objet de développement, d'extension, de renforcement. L'analogie que je propose ici est inspirée du travail de l'analyse du gouvernement autour de l'État moderne de Foucault. La raison infrastructurelle est le principe d'action de la communauté pour conserver l'infrastructure dans son fonctionnement quotidien. Elle définit ce qui est nécessaire et suffisant pour que, non pas la république, mais l'espace peuplé de *wallets* autonomes fonctionne en pratique. L'infrastructure est à la fois un objectif stratégique de la communauté, et le principe

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

d'intelligibilité de ce qui est en pratique dans cet espace.

Cette raison infrastructurelle a des traits similaires avec ce que Foucault appelle la « raison du moindre État » (2004b) : le gouvernement doit être le plus minimal possible. Si ce minimalisme fait largement consensus dans la communauté, la « rationalité infrastructurelle » de la communauté fait débat. Foucault désigne par ce concept les principes régulateurs au nom desquels un gouvernement agit bien ou mal, ce à l'aune de quoi un partage rationnel est établi entre ce qui est à faire et ce qui est à ne pas faire (Foucault 2004b).

Le cas de la controverse dite « TheDAO », détaillée dans ce chapitre, montre que deux « rationalités infrastructurelles » se sont opposées dans la communauté Ethereum. La première, héritée de Bitcoin, est une rationalité calquée sur la mystique du protocole : les pratiques de gouvernement de la communauté doivent se limiter au strict minimum. La mystique sert de critère de « vérité » pour régler l'exercice du gouvernement ; comme ont pu l'être le texte religieux, la révélation, l'ordre du monde, ou dans la gouvernamentalité moderne le marché qui dit le vrai par rapport à la pratique gouvernementale. La seconde a à voir avec ce que Foucault décrit comme un trait de la raison libérale de gouverner : régler la pratique gouvernementale sur les « intérêts » individuels. Autrement dit, la rationalité du gouvernement est trouvée dans la rationalité des gouvernés, ici, les différents *wallets* de l'écosystème que ne réduit pas la mystique.

Cette seconde rationalité infrastructurelle, qui s'est imposée dans la communauté Ethereum, suit une dynamique inverse à la minimalisation de l'action du gouvernement libéral identifiée par Foucault. La communauté d'Ethereum était au contraire confrontée à la nécessité de gouverner un petit peu plus que selon la rationalité héritée de Bitcoin. Ce chapitre prend le cas du « financement des biens publics », objectif de gouvernement fixé par des meneurs de la communauté Ethereum car insoluble dans le libre jeu des intérêts individuels, et qui imposait d'imaginer des pratiques originales de gouvernement.

La première section montre que la communauté problématise la construction de

l'infrastructure de deux manières : à l'aune de la mystique (en termes de « centralisations » techniques et politiques) mais aussi, en la dépassant, au prisme des usages de l'écosystème. Cette deuxième proposition fait controverse, car elle contrevient à la mystique qui pose, par principe, que les usages ne doivent pas être un objet de connaissance et d'action ; leur signification devrait au contraire rester séparée de la production matérielle de l'infrastructure, exclusivement confiée aux *miners*. La communauté et l'infrastructure se fracturent dans cette opposition portant sur l'action communautaire sur l'infrastructure, mais aussi sur la manière de faire communauté. L'autonomie apparaît à cette occasion comme une fonction de l'infrastructure, qui nécessite d'être qualifiée et porte à controverse.

La deuxième section montre que le « bon » gouvernement étendu au-delà du seul maintien de l'infrastructure matérielle au problème du « financement des biens publics » et vise l'ensemble des *wallets* au prisme de la mystique. Cette dernière ne joue plus seulement comme critère d'évaluation du gouvernement minimal sur l'infrastructure ; elle est mobilisée pour gouverner les intérêts des *wallets* eux-mêmes. Ceux-ci ont un « intérêt collectif » à voir les biens publics proliférer mais un « intérêt individuel » à ne pas participer. La mystique est appliquée aux *wallets* dans des mécanismes : leur objectif est de trouver et d'allouer de l'argent aux constructeurs de biens publics indépendamment des intérêts individuels, pour l'intérêt collectif.

1. L'autonomie à l'épreuve de la construction de l'infrastructure

Cette section montre que l'« autonomie » de l'infrastructure est le résultat de négociations au sein de la communauté Ethereum. Au contraire de ce que prévoit la mystique du protocole, la « décentralisation » qui garantit la « sécurité » de l'infrastructure n'est jamais acquise. Elle est l'objet d'efforts permanents de la communauté qui s'érige en garante de son instauration. Ces efforts sont particulièrement visibles quand les usages réels et les fonctions imaginées de l'infrastructure percutent la mystique : l'écosystème s'invite dans le devenir de l'infrastructure. Cette dernière est alors non seulement considérée comme

modèle évaluatif de l'infrastructure, mais aussi prise comme référence pour penser l'organisation et les possibilités d'actions collectives sur l'infrastructure.

1.1. L'instauration d'Ethereum entre mystique du protocole et fonctions imaginées

L'infrastructure d'Ethereum était problématisée de manière variée par les acteurs constituant la communauté. En meetups comme sur les arènes de discussions en ligne, ces acteurs mobilisaient ce que j'ai appelé, au Chapitre 1, la « mystique du protocole ». Cette sous-section distingue deux ensembles de problématisations en fonction du rôle que jouait la mystique. D'une part, l'infrastructure était problématisée par le prisme de la mystique elle-même : elle était comparée à l'instauration théorisée par les principes d'architecture du protocole. Ils jouaient un rôle de modèle : la pérennité de l'infrastructure et la « sécurité » des transactions étaient évaluées en termes d'écart à ce modèle. D'autre part, l'infrastructure était problématisée en réaction aux fonctions imaginées de l'infrastructure, en tenant compte d'acteurs que la mystique ignorait : l'écosystème de concepteurs et d'utilisateurs. Ainsi, la « sécurité » garantie par la mystique n'était plus le seul problème de la construction de l'infrastructure.

« Décentralisation » : mystique et instauration des blockchains

18 heures, un samedi de janvier 2020. Un ancien dépôt d'une gare parisienne récemment transformé en « lieu de vie culturel, indépendant et engagé » accueillait cinq jours durant l'édition « numéro 0 » du *Peer-to-peer Festival*. Cet événement offrait des tribunes à différents projets de développement de logiciels fonctionnant en pair-à-pair. Ethereum était l'un d'eux. Un des membres de l'association représentative de la « communauté » en France, Ethereum France, co-organisait l'événement. Une des conférences, intitulée « Quand décentraliser cesse d'être une bonne idée ? », était libellée « blockchain » sur le programme du festival. Arun, présenté comme un membre de la communauté blockchain, introduisait sa présentation d'une dizaine de minutes par les mots suivants :

*Hello! Yeah, hello everybody. Just you know, I barely see anybody because the light is on me. But, anyways. So, yeah, I mean, **we have been hearing a lot about decentralization**, as a great thing, and often I would always say it's a good thing; it goes with the whole peer-to-peer thing that we should all be able to connect to each other directly. But **there's a difference between decentralized which is a kind of a fixed state, where you can say something is decentralized or not**. So, in the case of blockchains, for example whenever somebody comes up with a new protocol, or a new idea, there's always the controversy, a lot of discussion, around: **is it decentralized enough, you know**. And somebody will find out: no. There's a lot of argument and controversy on that. So, instead of looking at decentralized, which is you know **the idea that, everything is not decided at the same place, like everybody has an equal share, at least they have some kind of direct interaction with the system, a more interesting way to look at is as the process of getting there actually**. (Arun, P2P Festival, janvier 2020)*

Arun constatait que la décentralisation était souvent une grille d'évaluation des activités dans les communautés blockchain. Les protocoles inspirés de Bitcoin tout autant que l'organisation de ces communautés elles-mêmes étaient évalués à la lumière d'un « état fixe » : ces différentes initiatives devaient être vues comme « suffisamment décentralisées ». Arun souhaiter, lui, nuancer ce critère. Plutôt que d'évaluer ces initiatives de manière absolue, il proposait de voir la décentralisation comme un processus : en faire un horizon, une orientation vers laquelle devaient tendre les projets blockchain. Il présentait la décentralisation comme un principe d'action collective.

Ce faisant, Arun distinguait le modèle architectural du protocole de l'instauration concrète des blockchains. Le premier renvoyait à ce que le fondateur d'Ethereum VB qualifiait de « raison d'être » des blockchains ; la décentralisation avait, selon ce dernier, des significations à la fois architecturales et politiques (Chapitre 1, section 2). La seconde faisait au contraire apparaître ce qu'Arun appelait des « paradoxes » entre une décentralisation théorique et des centralisations pratiques. Arun ne dénonçait pas la qualité « décentralisatrice » des blockchains. Il cherchait plutôt à montrer que les écarts entre théorie et pratique participaient au modèle décentralisé lui-même. Selon lui, la centralité de certains points d'une infrastructure participaient à la faire grandir dans son ensemble, attirant de nouvelles personnes jouant le rôle de *miners* ou de développeurs, et ainsi, participait à décentraliser l'infrastructure. Il décrivait ce processus comme une « danse »

entre centralisation et décentralisation, deux principes qui formaient un « yin-yang », qui étaient « mixés » dans un « mouvement » et se comprenaient en termes de « spectre ».

a. La mystique comme prisme de problématisation

Les paragraphes suivants décrivent deux problématisations des blockchains énoncées en termes de « centralisations ». Dans ces deux cas, la mystique du protocole est mobilisée comme un modèle de référence à l'aune duquel l'infrastructure est évaluée. Ces problématisations étaient formulées dans différentes arènes, notamment en meetups et dans des arènes de discussion en ligne de « communautés ». La position défendue par Arun introduit un décalage vis-à-vis du rapport à la mystique. Il pointe une dimension active à la « décentralisation ». Il s'agit d'un principe de développement continu, un modèle positif de développement, pas un simple modèle évaluatif : il faut en permanence évacuer tout « centre » technique, politique, social. Cette tendance se retrouve dans les problématisations en termes de « centralisation » font de la mystique une référence normative, aussi bien au niveau de l'infrastructure que de la communauté participant à l'instaurer.

Les fermes de minage : décentralisation de l'infrastructure matérielle

La problématisation la plus commune formulée en termes de « centralisation » visait les « fermes de minages » (*mining pools*), des assemblages de *miners* contrôlés par une même entité morale ou juridique. Dans ces discussions, Bitcoin était souvent mobilisé comme cas paradigmatique bien qu'Ethereum était également concerné par le phénomène. Début 2022, six d'entre elles contrôlaient plus de 80 % de la puissance de calcul du réseau Bitcoin (btc.com 2022). Dans une publication de 2017, VB s'interrogeait sur la qualité « décentralisée » de Bitcoin en publiant une photo figurant sept individus propriétaires de fermes de minage qui représentaient plus de 90 % de la puissance de calcul du réseau à eux seuls (Buterin 2017a). Ces fermes de minages « centralisaient » le réseau, d'un point de vue architectural comme politique. En effet, leur existence contrevenait au principe de compétition matérielle, par la puissance de calcul, au cœur de la mystique du protocole. Une alliance de quelques-unes de ces fermes de minage aurait pu conduire à la réécriture de

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

l'ensemble du registre au profit de cette alliance de plus de 50 % de la puissance de calcul.

Ce phénomène a été analysé par Donald MacKenzie comme le résultat d'un problème de « *material political economy* » (MacKenzie 2019). L'auteur analyse la centralisation en fermes de minage comme résultat de développements techniques et économiques en contradiction avec ce que l'idéal égalitaire porté par Nakamoto : une participation large et individuelle de chacun à la maintenance de Bitcoin. Son analyse s'appuie sur l'examen des opérations produites par les *miners*. Produire un bloc à ajouter à Bitcoin suppose d'exécuter un algorithme de « hashage », appelé SHA-256. Pour espérer valider un bloc, un *miner* doit l'exécuter jusqu'à obtenir une suite de caractère satisfaisante au sens du protocole de consensus (c'est-à-dire commençant par un nombre fixé de zéros). Le premier *miner* découvrant une suite satisfaisante peut ajouter le bloc et obtenir la récompense. Son succès signifie alors échec des tentatives des autres qui doivent recommencer leurs tentatives au bloc suivant. Ce processus est conçu de manière volontairement coûteuse en puissance de calcul, pour les raisons détaillées au Chapitre 1. Pour maximiser leurs profits en minimisant le temps d'exécution du SHA-256, des entreprises ont développé des machines spécialisées dans le calcul spécifique du SHA-256. La distribution de ces machines dites ASIC, pour *Application-specific integrated circuit*, a participé à augmenter la difficulté de production d'un bloc (le nombre de zéros qui doit être obtenu en exécutant le SHA-256) de manière si significative qu'il paraît désormais difficile pour un individu faiblement équipé d'espérer faire du minage une activité rentable. L'investissement requis doit en conséquence être toujours plus important pour faire face à une concurrence entre *miners* toujours plus grande (le nombre de 0 à obtenir augmentant avec le nombre des *miners* sur le réseau) alors que le montant de récompense par bloc est fixé indépendamment de l'étendue du réseau.

L'analyse critique de MacKenzie et celles d'acteurs de la communauté comme VB ou Arun ont en commun de problématiser l'instauration de Bitcoin à la lumière de la mystique. Dans sa tentative de présenter la centralisation comme un moteur de la décentralisation, ce dernier rappelait qu'à ses tout premiers instants, Bitcoin n'était pas décentralisé : si Satoshi Nakamoto avait attendu que Bitcoin le soit, Bitcoin n'aurait jamais existé. En effet, à son lancement, une seule machine faisait exister Bitcoin. D'autres participants ont ensuite dû

faire confiance à l'inventeur. Il voyait dans les fermes de minage une manière de développer Bitcoin, et de manière performative, d'attirer des individus ou entreprises qui « rejoignent » ces fermes (en investissant dans les entreprises qui les contrôlent) ou en se connectant au réseau. Ainsi, du seul ordinateur de Nakamoto, Bitcoin se serait structuré autour de gros acteurs centralisateurs qui, en attirant d'autres, participaient à une « meilleure » décentralisation.

Protocole et logiciels « clients » : décentralisation de la conception logicielle

Une autre problématisation formulée en termes de « centralisation » visait le processus de développement et d'utilisation du protocole de consensus. Dire qu'un réseau est « décentralisé » supposait que quiconque puisse participer aux opérations de minage. Or, l'accès était limité par les compétences nécessaires à l'activité de minage. L'installation, la configuration, et éventuellement la construction d'une machine performante étaient des opérations qui requéraient des compétences techniques. Ce thème était également discuté par Arun qui, là encore, reconnaissait cette centralisation tout en défendant une position nuancée. Pour lui, ce problème de compétences avait à voir avec une question de « capacités » individuelles qui pouvaient être dépassées, selon des principes « méritocratiques ». Le minage supposait selon lui de se former à la technologie et à l'économie, d'apprendre à calculer son investissement dans du matériel de minage. Tout le monde n'était pas « compétent pour comprendre » comment administrer un nœud du réseau *a priori*, comment le coordonner aux autres nœuds, mais aussi comment « légitimer » le processus.

Cette notion de « légitimation » pointe une dimension politique dans l'activité de minage, propre aux contingences de l'instauration d'un réseau. La mystique suppose que le protocole est figé ; or, en pratique, il évolue. L'activité de minage supposait d'exécuter la même version du protocole de consensus que les autres pairs du réseau. Dans le cas contraire, et même si le *miner* parvenait à construire un bloc, ce dernier ne serait pas accepté par les autres pairs. Or, cette adhésion ne tenait pas seulement à une mise à jour technique : elle signifiait adhésion à une certaine manière de valider des blocs, à une

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

certaine manière d'instaurer le réseau. Ces versions étaient communiquées *via* les logiciels dits « clients », installés sur chaque *miner*. Ainsi, configurer un *miner* supposait des connaissances techniques, savoir installer du matériel spécialisé mais aussi savoir manipuler un terminal pour choisir quelle mise à jour du protocole installer ou non ; c'est-à-dire, accepter ou pas de valider les blocs d'une certaine manière. Les compétences techniques vont avec une compétence politique : installer une mise à jour signifie approuver une décision politique proposée par d'autres membres de la communauté.

Les développeurs de logiciels « clients » représentaient eux-mêmes un problème de « centralisation ». Plusieurs équipes de développement de logiciels clients développaient des versions concurrentes, dans différents langages, du protocole Ethereum. Au moment de l'enquête, trois versions étaient utilisées en même temps, codées en Go, en C++ et en Python. Le principe de compétition au cœur de la mystique était déplacé du niveau matériel de l'infrastructure (son architecture) au niveau logiciel : il s'agissait de se prémunir de l'introduction d'une modification « centralisée » du protocole qui serait suspecte par hypothèse. Ainsi, il fallait éviter qu'un logiciel client devienne majoritaire sur l'infrastructure pour le protéger d'une modification malveillante ou résultant d'une erreur de la communauté de développement spécifique à un logiciel client donné.

Des auteurs ont dénoncé la « centralisation » au sein des équipes de développement du protocole de Bitcoin (De Filippi & Loveluck 2016), ou de Bitcoin et d'Ethereum (Li 2020). Ainsi, ces auteurs problématisaient eux-mêmes, dans leurs travaux, la construction des infrastructures au prisme de la mystique. Du point de vue de recherches en informatique, la « centralisation » du processus de développement et de contribution au code source de Bitcoin et d'Ethereum est vue comme un risque majeur pour la « sécurité », car celle-ci est posée comme garantie par la « décentralisation » (Li 2020). La même prémisse est posée par Primavera De Filippi et Benjamin Loveluck dans leur analyse de la gouvernance de Bitcoin (2016). Les auteurs reconnaissent, à la lumière d'une littérature prenant pour objet des communautés de développement *open source*, qu'il n'est pas original qu'une petite élite de développeurs contrôle le code. Leur analyse tient plutôt dans l'opposition entre une gouvernance « par l'infrastructure », qui assurerait « l'auto-gouvernement et l'auto-

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

entretien », promesse de la mystique du protocole, et une gouvernance « de l'infrastructure » à la main d'une poignée de développeurs exerçant une « politique invisible ».

Le vocabulaire est ici particulièrement intéressant : les membres de ces communautés appellent eux-mêmes les développeurs du protocole les « développeurs centraux » (*core developers*, ou usuellement « *core dev* »). Leur « centralité » est affichée. Durant mon enquête sur Ethereum, je n'ai pas observé de problématisation de la centralisation de la production du code du protocole. En revanche, j'ai occasionnellement observé certaines voix qui critiquaient Bitcoin pour l'opacité du processus de développement du protocole. Au moment de l'enquête, les *core dev* d'Ethereum étaient au centre d'une communauté de développement logiciel appelée *Ethereum magicians*. Cette communauté était organisée, de manière très classique pour les communautés open source, sur un forum en ligne. Elle affichait son ouverture¹⁸⁰.

b. Au-delà de la mystique : l'infrastructure au prisme de sa fonction imaginée

Les fonctions imaginées de l'infrastructure participaient à problématiser la construction d'Ethereum en complément de la mystique. Les paragraphes qui suivent s'appuient sur l'examen de la controverse posée par l'augmentation de la « taille des blocs » pour montrer que le principe de « décentralisation », impératif de la mystique, était négocié. Cette négociation portait sur la manière de tenir compte des acteurs inscrits dans le protocole lui-même (*miners*, utilisateurs ou *wallets*).

Le problème de la « taille des blocs » s'est posé dans un débat plus large au sein des communautés Bitcoin et Ethereum, appelé le « problème du passage à l'échelle ». D'un point de vue technique, ce problème était posé par une insuffisante capacité d'inscription

180 « *Ethereum Magicians is a forum for the crypto community to have a place where anyone can join, create topic and discuss mainly about EIPs and technical difficulties of Ethereum ecosystem. Or in another words "Ethereum Magicians forum is a place on the internet where your voice will be heard and your contributions to the Ethereum will matter". Ethereum Magicians is a group of individuals working and contributing to the Ethereum.* » (Ethereum magicians 2023)

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

d'une blockchain (le nombre de transactions validé dans une unité de temps donnée) en regard de son utilisation réelle (le nombre de transactions signées par des utilisateurs dans cette même unité de temps).

La réponse la plus évidente à ce problème consistait à augmenter la taille des blocs formés par les *miners*. Toutefois, cette proposition a fait débat. Deux problématisations de la construction de ces infrastructures s'opposaient. Une première problématisation posait que l'utilisation serait favorisée par une plus grande capacité d'inscription de l'infrastructure : en acceptant plus de transactions pour une même unité de temps, les frais payés par les utilisateurs pour « inciter » les *miners* à choisir leurs transactions dans le prochain bloc seraient diminués. Ainsi, augmenter la taille des blocs permettrait de favoriser « l'adoption », en rendant l'inscription des transactions meilleur marché et plus rapide.

Une seconde problématisation opposait la mystique : elle associait l'augmentation de la taille des blocs à une menace pour la décentralisation du réseau, donc à sa sécurité. Dans la communauté Ethereum, j'ai rencontré trois arguments contre l'augmentation de la taille des blocs (promus par des acteurs qui, souvent, reconnaissent eux aussi l'insuffisante capacité d'inscription). Premièrement, augmenter la taille des blocs favorisait les *miners* les plus puissants¹⁸¹ comme les fermes de minage, en augmentant leurs chances de valider un bloc. Par conséquent, de plus gros blocs excluraient les plus « petits » *miners*, en contradiction avec la mystique qui pose une compétition maximale entre différents *miners* comme principe de sécurité. Deuxièmement, augmenter la taille des blocs favoriserait l'apparition de « conflits » entre *miners* : plus la taille d'un bloc est importante, plus il est probable que deux *miners* valident un bloc en même temps. Ces situations conduisent non seulement à des pertes de revenus pour les *miners* en question, mais aussi à des problèmes de « finalité »

¹⁸¹ Pour que le réseau décentralisé se maintienne (c'est-à-dire que les différents nœuds restent synchronisés), chaque nœud doit individuellement inscrire toutes les transactions qui ont été inscrites dans un bloc. Augmenter la taille des blocs signifie que chaque nœud doit, dans une même unité de temps, produire plus d'opérations de mise à jour de sa version locale de la blockchain – un fichier de plus de 300 gigaoctets au début de 2021, qui ne cesse de croître à mesure que de nouveaux blocs sont inscrits. Cette augmentation de calcul nécessaire à chaque bloc deviendrait obligatoire pour proposer un nouveau bloc. Or, cet effort est marginalement plus faible pour des *miners* disposant de plus de puissance des *miners* ; les *miners* les plus puissants accordent une part de leur puissance de calcul plus faible à la mise à jour de leur version de la blockchain, et augmentent ainsi un peu plus leurs chances de valider un bloc.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

des inscriptions¹⁸². Enfin, proposer une augmentation de la taille des blocs pourrait ne pas être acceptée par les *miners* eux-mêmes, attirés par des frais de transaction élevés, et qui sont pourtant ceux qui actent une évolution du protocole de consensus en mettant à jour leurs logiciels clients.

Ces différentes problématisations opposaient des points de vue différents concernant les fonctions imaginées de ces dispositifs. La première posait que Bitcoin devait être un moyen de paiement étendu au plus grand nombre de personnes possible. Elle répondait aux commentateurs qui comparaient Bitcoin à des systèmes de paiements électroniques traditionnels, comme Visa et Mastercard, en termes de capacité de transactions. Alors que Bitcoin n'a jamais dépassé les 400 000 transactions quotidiennes, le seul réseau Visa en totalisait, en 2020, autour de 500 millions (Nilson report 2022). La seconde problématisation posait, renvoyait au contraire Bitcoin à ses origines mythologiques (décrites au début de la section 1 du Chapitre 1) : un or numérique dont la valeur était corrélative à sa rareté. Selon ce point de vue, il était moins urgent d'augmenter la fréquence d'inscription des transactions que de favoriser la plus grande décentralisation, garantie de sa sécurité et de la valeur de son unité.

Ainsi, les acteurs des communautés s'érigeaient en porte-paroles des acteurs en présence : aussi bien des utilisateurs (Bitcoin comme système de paiement ou comme or numérique) que des *miners* (garantissant la « décentralisation »). Le prisme des fonctions donnent une explication alternative aux « intérêts » qui seraient propres aux *core dev*, en capacité d'imposer leurs points de vue en raison d'une structure leur conférant un « pouvoir » important pour expliquer les controverses sur la taille des blocs (De Filippi & Loveluck 2016). Il suppose de ne pas poser *a priori* que « Bitcoin est une monnaie et un système de paiement décentralisés ».

182 Un bloc plus gros nécessite plus de temps pour circuler dans le réseau. Avec l'augmentation de la taille, la situation dans laquelle un *miner* travaille à valider un bloc sans savoir que l'état de la blockchain sur lequel il travaille est dépassé (c'est-à-dire une situation dans laquelle un autre *miner* a déjà validé un bloc correspondant à cet état de la blockchain) devient plus probable. Or, dans ces cas-là, le protocole sélectionne le bloc validé avec l'horodatage (*timestamp*) le plus ancien, générant une perte sèche pour un *miner* qui aurait validé un bloc finalement non retenu. Les acteurs appellent ces blocs des « oncles ». Les transactions incluses dans ces blocs « oncles » imposent également des délais supplémentaires de validation pour les utilisateurs qui les ont signées, désignés comme problèmes de « finalité ».

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Mes observations des controverses sur Bitcoin et Ethereum indiquent que les acteurs pris en compte étaient spécifiques aux dispositifs et à leurs communautés. À la différence de Bitcoin, Ethereum a par exemple intégré dans le protocole de consensus un mécanisme permettant aux *miners* d'ajuster eux-mêmes la taille des blocs en « votant » à l'ajout de chaque nouveau bloc, dans une limite fixée par le protocole. Ces spécificités semblaient spécifiques à la fonction de chaque dispositif ; et comme le montrera la suite de cette section, cette fonction était elle-même controversée.

En particulier, avec Ethereum, la problématisation par les fonctions imaginées faisait exister, au sein de la communauté, un ensemble d'acteurs absent chez Bitcoin : l'écosystème. Durant le meetup indiqué en introduction de ce chapitre, Jean présentait le problème du passage à l'échelle à la lumière de l'activité de l'écosystème¹⁸³. Il était à la fois un représentant de l'écosystème, directeur des services aux entreprises chez ConsenSys (« Solutions »), et de la communauté, en tant que président de l'association Asseth (ancien nom d'Ethereum France). Jean articulait le problème du « passage à l'échelle » avec certains épisodes du développement de l'écosystème. Il expliquait que le plafond de la capacité d'Ethereum avait été atteint lors de pics d'utilisation marqués par des emballements soudains, notamment les ICO (Chapitre 2) aux tous premiers jours de 2018, puis avec l'emballement pour les CryptoKitties, des chats numériques à collectionner sous forme de jetons¹⁸⁴. C'était le développement de l'écosystème, qu'il s'agisse de chats à collectionner ou d'ICO, qui faisait se rassembler la communauté parisienne pour exposer et réfléchir aux différentes options possibles pour « passer à l'échelle » dans les mois ou années à venir.

183 Ce meetup visait également à indiquer pourquoi l'augmentation de la taille des blocs était « naïve » (trois arguments résumés ci-dessus), et présentait les projets en cours visant à faire passer Ethereum à l'échelle, parmi lesquels le changement de protocole de consensus au « Proof Of Stake », finalement décidé en septembre 2022.

184 Les propriétaires des chats possédaient des jetons inscrits sur Ethereum *via* la DApp de l'entreprise qui les avait conçus. Les chats pouvaient être vendus ou accouplés de pair-à-pair, « sans intervention » de l'entreprise en question. Ils étaient d'un type appelé « collectibles » à l'époque, plus tard renommés « *non fungible tokens* » ou NFT.

1.2. Constitution de la communauté et développement de l'écosystème

Cette sous-section s'appuie sur des récits de la constitution de la communauté Ethereum par des portes-paroles. Ces récits montrent que la « communauté » n'est pas un groupe formellement coordonné ; il s'agit d'un concept vernaculaire utile pour désigner généralement les personnes ou entreprises intéressées ou participantes à l'utilisation ou au développement d'Ethereum. Surtout, ces récits pointent le rôle de l'écosystème dans la constitution de la communauté. D'une part, son développement donne une identité collective « *tech focused* » à la communauté, notamment par opposition aux spéculations sur le prix des cryptoactifs. D'autre part, le développement de l'écosystème fait controverse au sein même de la communauté Ethereum. Des oppositions internes se dessinaient : les différences de problématisation de l'infrastructure correspondaient à différentes visions de l'écosystème à faire advenir.

Deux points de vue sur la communauté Ethereum

Evan van Ness (EvN) assurait le premier *talk* de la deuxième journée d'EthCC dans le prestigieux grand amphithéâtre de la Maison de la Mutualité. EvN était connu pour ses newsletters hebdomadaires qui donnaient un résumé des actualités de la semaine en lien avec Ethereum¹⁸⁵. Le *talk* était intitulé « *The Ethereum Community in 2020* ». En vingt minutes, l'orateur donnait un aperçu de « l'histoire [d'Ethereum] dans la perspective de la communauté », esquissait un tableau de la communauté, puis présentait des « défis » que la communauté devrait surmonter avec des conseils pratiques. EvN décrivait une communauté qui s'était construite de manière « décentralisée ». Ce faisant, il construisait un « *master narrative* » de la communauté Ethereum, une « voix qui ne problématise pas la diversité » (Star 1999 : 384). Il donnait une forme de cohérence au développement de la communauté

185 Ces newsletters contenaient des résumés en quelques mots des actualités des derniers développements logiciels, de projets de recherche, ainsi que des faits jugés importants dans les développements de l'écosystème. À ces descriptions étaient associés des liens vers des sites Web externes. L'auteur tirait des revenus de son activité en insérant des publicités pour des entreprises de l'écosystème, ou en publiant des offres d'emplois pour quelques centaines d'euros les 70 caractères. Les *newsletters*, envoyées les dimanches soir, étaient archivées sur le site <https://weekinethereumnews.com/>.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

en reprenant le vocabulaire correspondant non seulement de la forme de l'infrastructure, mais aussi à l'éparpillement habituel des communautés de développement de logiciels *open source* ou de production communautaire par Internet (Benghozi 2006 ; Demaziere, Horn & Zune 2006 ; Lazzaro 2008).

L'histoire de la communauté était racontée comme une succession d'événements qui avaient marqué le succès d'Ethereum. Dès ses origines, Ethereum était raconté comme un processus émergent, fait de rencontres sans centre. Après la publication du *whitepaper* en 2013, VB rencontrait l'entrepreneur Joseph Lubin à Toronto. En 2014, la communauté Ethereum « commençait à se former » à la *Bitcoin Conference* qui se tenait à Miami. EvN indiquait que ces premiers passionnés dépensaient beaucoup d'argent pour faire voyager des émissaires d'Ethereum autour du monde pour « donner des meetups », parfois simplement pour une vingtaine de personnes¹⁸⁶. À ces tentatives de fédérations locales s'ajoutaient des espaces numériques communs, en particulier sur la plateforme Reddit¹⁸⁷. La Fondation Ethereum, formée en Suisse la même année se capitalisait grâce aux ethers créés dans le processus d'ICO d'Ethereum (« *pre sale* ») : les fonds collectés avant le lancement de la blockchain allaient donner droit à un nombre fixé d'ethers lors du lancement effectif du réseau¹⁸⁸.

Début 2020, la communauté « était décentralisée » pour EvN. Il la décrivait comme un assemblage de différentes communautés, chacune organisée autour de projets de standards de développements ou de projets entrepreneuriaux spécifiques. Cette décentralisation organisationnelle s'observait selon lui dans la diversité des arènes de discussion : Twitter était une plateforme de discussion généraliste ; les développeurs avaient leurs forums de

186 Je n'ai pas de données sur l'origine de cet argent. Je suppose qu'il vient de la « *pre sale* » d'Ethereum, lancée à l'été 2014 (Buterin 2014c) : en échange de bitcoins, des investisseurs se voyaient alors promettre la dotation d'ethers une fois que le réseau serait lancé.

187 Reddit est décrit sur Wikipedia comme « un site web communautaire américain d'actualités sociales fonctionnant *via* le partage de signets permettant aux utilisateurs de soumettre leurs liens et de voter pour les liens proposés par les autres utilisateurs » (consulté en février 2021). C'est par exemple sur Reddit que les premiers échanges sur le lancement d'Ethereum étaient dispensés par les cofondateurs. Une session dite AMA (« Ask Me Anything »), c'est-à-dire de questions-réponses, était par exemple organisée pour la *pre-sale* (Buterin 2014c).

188 La Fondation Ethereum a été capitalisée selon un processus dit de « *pre mine* », pour dire « ethers émis avant que le processus de minage existe ». Des ethers ont directement été alloués à un *wallet* de la Fondation Ethereum avant que la chaîne soit créée.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

discussion (comme OpenZeppelin, le subreddit r/ethdev, Ethereum magicians) ; des communautés Ethereum se développaient dans différentes langues, comme Ethfans en Chine ; des plateformes comme Slack, Discord ou Telegram permettaient à chaque projet d'avoir sa « petite communauté ». Les rencontres annuelles, comme EthCC ou Devcon pour « *Developper Conference* », rassemblaient des développeurs et d'autres personnes influentes. Elles étaient promues par la Fondation Ethereum. EvN expliquait que depuis deux ans, quiconque avait la possibilité de participer à ces conférences, pour lesquelles le nombre de billets avait souvent été bien inférieur au nombre de candidats. La Fondation Ethereum avait selon lui multiplié par 80 la capacité d'accueil des DevCon en six ans, et adapté sa méthode de distribution des tickets.

Pour Bob Summerwill (BS), la communauté était d'abord constituée d'individus. Son *talk* matinal, intitulé « *A call for an end to tribalism in Ethereum — 2 years later* », était programmé dans une salle plus confidentielle du dernier étage de la Maison de la Mutualité. BS racontait l'histoire de la communauté Ethereum comme une « histoire d'égos et de perspectives conflictuelles, mais avec une direction commune et englobante vers la liberté individuelle et la décentralisation ». Il connaissait bien la communauté et l'écosystème : BS avait travaillé à la Fondation Ethereum, à ConsenSys ainsi qu'à l'*Enterprise Ethereum Alliance* (EEA)¹⁸⁹, principales organisations formelles de la construction d'Ethereum ; respectivement de l'infrastructure, et d'Ethereum comme logiciel (Chapitre 3).

*Think about incentive mechanisms, **what kind of person would be incentivized to build a trust minimization system? And well, it's somebody who's got trust issues! That does not trust the world!** You know, [who] is scared or paranoid. And that's actually, that's not a negative label either. It's actually **very rational to be scared in the world** at the moment, right? But what you end up with is, the kind of people who start these sort of activities are not necessarily the best as you get further down the line when you get toward mainstream. Because **they're not necessarily very good at working with other people**, you know there may be very introverted don't have good interpersonal skills, don't like politics, and so on. (BS, EthCC, 5 mars 2020)*

189 Consortium technologique qui a participé à la « technologisation » d'Ethereum (Chapitre 3), rassemblant de grandes institutions financières et de sociétés de développement logiciel, dans lequel ConsenSys a joué un rôle moteur.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Pour BS, les membres de la communauté partageaient l'ambition de construire des dispositifs organisationnels minimisant la confiance. Ils avaient en commun un tempérament de « *weirdos* » et de « *nerds* », qu'il étayait de nombreux adjectifs : « autistes, sociopathes, égocentriques, souffrant d'anxiété chronique, de dépression sévère, suicidaires, cupides, égoïstes, narcissiques, paranoïaques, et à la fois géniaux, altruistes, visionnaires, désintéressés, intrépides », des personnes « profondément obsédées par certains problèmes de manière malade qui trouvent des solutions à des problèmes ». BS voyait une filiation avec de grandes figures de « *geeks* » entrepreneurs de la Silicon Valley, comme Bill Gates, Steve Wozniak ou Mark Zuckerberg.

Selon ces deux visions, la communauté n'était pas formellement coordonnée, elle émergeait à partir d'individualités ou de communautés elles-mêmes organisées par des points de vue particuliers sur Ethereum ; par exemple, un axe de recherche, un logiciel participant à sa construction, ou des affinités locales ou langagières. La même idée d'une communauté composée d'éléments indépendants traversait la présentation d'Arun, selon lequel il n'existait pas de problème politique lié aux formes « centralisées » du développement de Bitcoin ou d'Ethereum, car ce qui était « important » était nécessairement une donnée individuelle et personnelle, pas un problème à résoudre collectivement.

Un groupe constitué à l'épreuve du développement de l'écosystème

Le récit d'EvN faisait de la communauté un ensemble constitué vis-à-vis d'un extérieur : en lien avec l'écosystème, en réaction du reste de l'univers crypto. Cet ensemble avait une identité « *tech focused* » dès le lancement d'Ethereum. Ce slogan, répété plusieurs fois par EvN et par d'autres orateurs durant EthCC (« *we love the tech* »), résumait une identité collective construite en réaction à des pratiques contemporaines dans le milieu des cryptoactifs et de Bitcoin : d'une part, l'opacité de la gouvernance des forums de discussion en ligne et la saturation des discussions par les questions liées au prix et à la promotion des cryptoactifs (voir Chapitre 2, section 1.3), et d'autre part, la « centralisation » du développement des logiciels clients.

*The idea was to **split the anything price talk and market related, to another forum**, and a lot of a Ethereum came out of the, the, what we saw as the problems with Bitcoin. So at the time like Bitcoin had, well I guess still has, a big censorship problem and... like beyond that it was also just like price talk and memes, and so, the thought was like well we will put that in a separate subreddit and we will **keep Ethereum to be tech focused**. A different one that also was a reaction to Bitcoin was that **we wanted to have multiple clients**, for governance issues, **so that there was decentralization**, and there were three client teams led by Jeff, led by Vitalik, and by Gavin, so that Go, the Python and the C++ client respectively. And you know that's important for, you know, those three folks really led their own client teams, they're in charge of their client. (EvN, EthCC, 3 mars 2020)*

Cette organisation « décentralisée » d'une communauté « *tech focused* » passait par une pluralisation des forums de discussion et par le développement simultané de différents logiciels « clients ». D'une part et par exemple, les discussions sur les prix, la spéculation et la promotion sur les cryptoactifs étaient bannies du subreddit¹⁹⁰ « r/ethereum », provoquant la création d'un autre forum au contraire dédié à ces discussions¹⁹¹. D'autre part, pour assurer que la construction d'Ethereum soit « décentralisée », il fallait que le processus de développement du code le soit lui-même. EvN expliquait, comme indiquait à la sous-section précédente, que trois logiciels différents étaient développés en parallèle par trois équipes différentes, dans trois langages différents, pour se prémunir de la position « centrale » de « *core dev* ».

Dans le même temps, la consolidation de la communauté s'articulait à l'émergence de l'écosystème. EvN vantait l'apparition de différents meneurs ainsi que l'extension de la communauté dans différentes parties du monde dès ses premiers développements en 2015. Outre les meneurs du développement technique, des meneurs « *non-dev* » comme le français Stéphane Tual étaient érigés en porte-parole du projet Ethereum dans son ensemble. Londres était la principale « *Eth city* ». En 2016, des projets comme Digix, Augur ou Maker « commençaient à se former » ; vus en 2020, ce sont des applications qui ont participé au succès d'Ethereum. Le cas de Digix a été rencontré au Chapitre 2 ; Augur et Maker ont joué un rôle important dans le développement de la finance décentralisée à

190 Un subreddit est un espace communautaire, ou forum créé sur Reddit. Le subreddit r/ethereum était accessible à <https://www.reddit.com/r/ethereum/>.

191 Ce subreddit était spécifiquement orienté sur les questions de prix et du marché de l'ether (et plus tard, des jetons) : r/ethtrader à <https://www.reddit.com/r/ethtrader/>.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

partir de 2019-2020. EvN évoquait une période de forte croissance entre 2015-2016, avec l'arrivée dans la communauté de nouveaux membres, et de nouvelles « *Eth cities* » renforcées par le développement d'organisations internes à la communauté : New York avec la fondation de l'entreprise ConsenSys par Joseph Lubin en 2015, Berlin avec l'installation du « *dev office* » de la Fondation Ethereum.

*the rise of a million Slack channels which from a community perspective was sort of like the first like branching out from Ethereum, like **it used to just all be on Ethereum** and then you know... It was a sort of thing where you started seeing for the first time **people that maybe were like active in some specific slack channel but they weren't necessarily in the broader Ethereum community**, which is definitely something that has happened a lot since then. (EvN, EthCC, 3 mars 2020)*

Le développement rapide de l'écosystème à partir de 2017 était une épreuve pour le développement de la communauté : « tout est devenu fou » avec des millions de canaux du logiciel collaboratif Slack et l'apparition de « nombreuses arnaques aux jetons ». EvN opposait aux envolées des cours de l'ether et aux phénomènes de spéculation une communauté d'ingénieurs et de développeurs orientée par un projet stable qui restait « *tech focused* » et participait à structurer l'écosystème. D'une part, le succès des hackatons mondiaux à cette période confirmaient l'importance grandissante d'une communauté internationale de développeurs de DApps, et d'autre part, la finance décentralisée, dont l'importance grandissante dans la communauté apparaissait nettement à partir du deuxième semestre 2019, naissait à San Francisco et non pas dans des « centres financiers » comme New York ou Londres.

Toutefois, EvN reconnaissait des limites entre des développements orientés par la « *tech* », et un dehors intéressé par les perspectives financières liées aux cryptoactifs. Il regrettait qu'en dépit de la « décentralisation » des médias, des pratiques, des espaces physiques et géographiques, la « qualité » des discussions se soit dégradée à partir de 2017. Selon lui, on ne parlait plus autant de « *tech* » qu'avant, à l'image de *subreddits* de la communauté qui étaient trop souvent investis par des discussions portées sur la spéculation, ou « hostiles » à Ethereum. Selon mes observations, cette « hostilité » correspondait à des incursions

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

d'individus dénigrant le développement d'Ethereum au profit de communautés alternatives que ces intrus promouvaient.

Le problème pointé par EvN est celui posé au Chapitre 2 : l'emballement pour les cryptoactifs comme objets d'investissements assimilait l'ether à n'importe quel autre cryptoactif. Du point de vue de la communauté, cette tendance aurait appauvri les discussions ; il ne serait par exemple plus possible pour un débutant d'espérer obtenir des réponses « détaillées et techniques » à des questions naïves, que ce soit directement sur des forums envahis de *memes* sur les prix, ou indirectement *via* les media spécialisés tant les « clickbaits medias » distribuaient des informations de mauvaise qualité à partir de titres sensationnalistes¹⁹². EvN incitait ses auditeurs à revenir aux fondamentaux pour retrouver le chemin d'une communauté aminée (« *vibrant* ») en « travaillant » : chacun devait « essayer chaque dApp » et proposer des retours d'expérience aux concepteurs, en termes techniques pour les développeurs, ou d'expérience d'utilisation pour les autres ; chacun devrait voter sur Reddit pour aider à identifier les posts de bonne ou de mauvaise qualité ; chacun devrait retourner à son « *local meetup* », sinon en organiser un lui ou elle-même.

Un groupe fragile à l'épreuve du développement de l'écosystème

Le récit que BS proposait de l'histoire de la communauté Ethereum tranchait avec la version d'EvN, qui mettait en avant la « *tech* » comme identité agrégative d'une communauté décentralisée. Au contraire, BS racontait l'histoire d'une communauté traversée par des luttes intestines. Il convenait que les premières conférences d'Ethereum en 2014, époques des premières annonces publiques d'Ethereum, étaient des « jours heureux ». Dès sa descente de la scène de la *Bitcoin Miami Conference* en janvier 2014 depuis laquelle il annonçait Ethereum pour la première fois physiquement après la publication du *whitepaper*, VB fut rapidement entouré d'une foule d'enthousiastes¹⁹³. À cette époque, la communauté balbutiante s'organisait en ligne et se retrouvait occasionnellement lors de

192 Les médias spécialisés de ce genre étaient nombreux, comme ceux présentés au Chapitre 2, par exemple : cryptoast.fr, cryptonaute.fr, cryptonews.com, cointelegraph.com journalducoin.com.

193 BS racontait que le succès rencontré par VB fut tel qu'une foule le suivit après sa présentation. Le présentateur qui lui succéda pour la présentation suivante se retrouva face à une salle vide.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

conférences organisées par la communauté Bitcoin, comme à Miami (Figure 25), puis à la *Bitcoin Expo* de Toronto (avril 2014), laquelle coïncidait avec la création de la Fondation Ethereum.

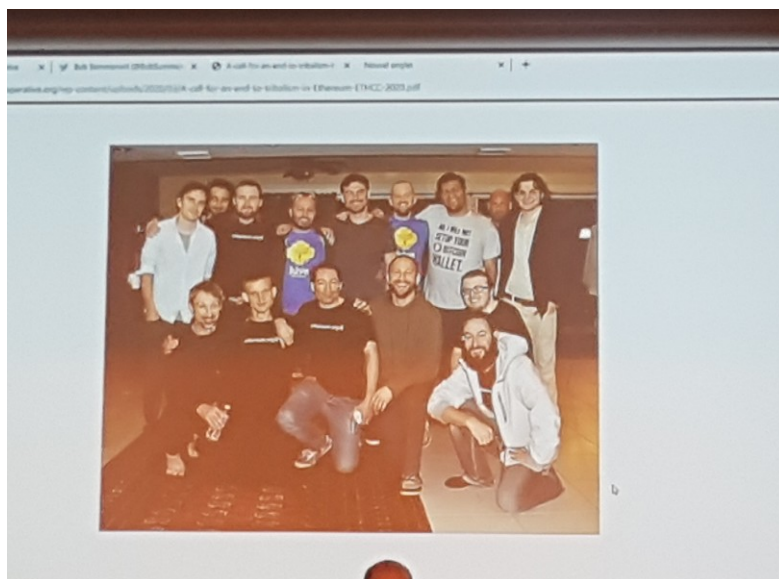


Figure 25 : Photo d'une diapositive de BS intégrant une photo du premier cercle d'enthousiastes présents à la Miami Bitcoin Conference, parmi lesquels V. Buterin, C. Hoskinson, J. Lubin, G. Wood

Toutefois, BS expliquait que cette fraternité n'était qu'apparente. Peu après ces premières rencontres, des guerres d' « égos » prirent le dessus. Il s'indignait. Impressions d'écran à l'appui, il dénonçait que l'annonce d'origine d'Ethereum sur le forum *Bitcointalk*, principal espace de discussion en ligne pour les cryptomonnaies à l'époque, avait été modifié dès les mois qui suivirent afin d'invisibiliser certains protagonistes (Figure 26).

Pour BS, ces guerres d'égos étaient la conséquence d'un malentendu originel sur ce que devait être Ethereum : « Vous aviez un rêve, et différentes interprétations personnelles de ce rêve ». Il racontait qu'en raison de cette incompréhension latente, ces enthousiastes rêveurs s'étaient fracturés dans une série de « schismes ».

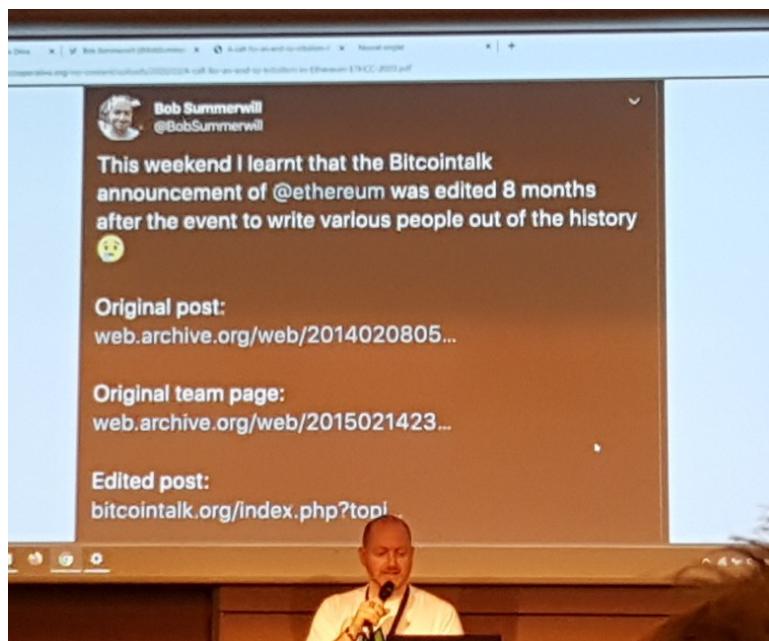


Figure 26 : Tweet de BS dénonçant la réécriture de l'annonce publique d'Ethereum

Le premier schisme cristallisait une divergence sur le modèle économique d'Ethereum et sa forme de gouvernance. Certains voyaient Ethereum comme un « *crypto Google* [...] une société à but lucratif qui produit le code de base d'Ethereum ». Charles Hoskinson et Joseph Lubin étaient de cette ligne : Ethereum devait être rentable, devait donc attirer des fonds de *venture capital* et disposer d'une structure organisationnelle formelle et forte. D'autres, comme VB et Gavin Wood, voyaient plutôt un « *crypto Mozilla* [...] collaboratif et sans but lucratif dès le départ ». Cette deuxième ligne s'imposant, Charles Hoskinson quitta le projet. Au contraire, Joseph Lubin s'accommodait de cette ligne en fondant ConsenSys à ce moment-là comme un « *startup studio* » (voir Chapitre 3, section 1).

D'autres « schismes » suivirent. D'abord, avec la création de ConsenSys. Les partisans de la ligne « *crypto Mozilla* » voyaient l'entreprise comme « franchement atroce [*god-awful*] [...] qui ne se préoccupe que du profit, un bras *marketing* ». Un autre schisme survint quand Gavin Wood, meneur de l'équipe de développement du « client » Parity (développé en Python à l'époque), quitta la Fondation Ethereum qu'il avait cofondée. Selon BS, certains meneurs se seraient inquiétés que Wood nuise à Ethereum en représailles en

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

introduisant du code malveillant dans la construction de Parity. Cette crainte était à l'origine de l'attention de la communauté pour le développement simultané de différents logiciels clients (sous-section 1.1. de ce chapitre). BS situait un autre schisme au moment de la création de l'EEA, organisation qui produisait des versions « entreprises » du code d'Ethereum adaptées pour les réseaux privés de grandes entreprises institutionnelles (voir Chapitre 3, section 1), participant à l'émergence de réseaux B2B.

*[people said] all of these enterprise things are trying to co-opt Ethereum for the banks in the status quo. You know when I left the Foundation, to work at ConsenSys on helping to set up the enterprise Ethereum Alliance and spent a year on that, you know, a lot of people could not understand that **“why on earth would you do that: we're trying to get away from the banks! How can you work with them?”** and I mean all of these that they're just demonizations. Because that's how human brains work. It's very hard for us to understand that other people have **different world views** than us, they have different perspectives, different priorities, and that they may be thinking different ways than us, and they have different goals and aims. But nearly **all of the time that kind of demonization is really very very self-defeating**. I mean if you look at pretty much any project within the whole of blockchain, the end goals of the people involved are all pretty much the same probably, **90 to 95 percent of what we're trying to do is aligned**, you know **we're trying to build better systems for trust minimization and for collaboration**. (BS, EthCC, 5 mars 2020)*

Deux remarques sur ce verbatim en conclusion de cette sous-section. D'une part, il indique explicitement que les différents schismes sont les conséquences de « visions du monde » portant sur ce que devrait être l'écosystème pour les acteurs de la communauté. Pour BS, ces questions étaient secondaires par rapport à ce qu'il voyait comme essentiel : des individus partageant une identité collective dans la construction de « meilleurs systèmes minimisant la confiance et la collaboration ». C'est en ce sens qu'il faut comprendre le titre de son intervention à EthCC, qui appelait à une « fin du tribalisme » dans la communauté Ethereum¹⁹⁴. Néanmoins, le problème persistant dans la communauté Ethereum était la qualité de cet écosystème : la question de l'inclusion des banques, le développement d'Ethereum comme une entreprise ou un projet open source, ou encore comme un projet open source qui se donne pour objet une infrastructure ou un logiciel comme le proposait

194 Je n'ai jamais observé ce « tribalisme ». À EthCC, l'EEA était très peu évoquée, et Joseph Lubin était accueilli comme une vedette, aussi bien par Jean qui assurait l'entretien (matériau mobilisé au Chapitre 3, section 1) que par la salle. Les débats que racontait BS étaient anciens.

l'EEA.

D'autre part, la communauté Ethereum que désignait BS n'était pas tout à fait celle au sein de laquelle j'enquêtais en 2018-2020. En effet, un autre « schisme » particulièrement important s'est produit en 2016, suite auquel la communauté et l'infrastructure se sont divisées en entités. BS était dans le camp minoritaire, dont l'infrastructure s'est appelée « Ethereum Classic », un nom en réaction à la communauté et à l'infrastructure majoritaires qui ont conservé le nom « Ethereum ». Au moment de son *talk*, BS était directeur de l'Ethereum Classic Cooperative. À la manière de la Fondation Ethereum, cette organisation coordonnait et finançait des développements d'une infrastructure jumelle et concurrente d'Ethereum, Ethereum Classic.

La sous-section suivante analyse l'événement à l'origine de la rupture (communautaire et infrastructurelle) entre Ethereum et Ethereum Classic. Ce cas montre que les controverses infrastructurelles problématissent simultanément les fonctions des infrastructures et les possibilités d'action collective de la communauté.

1.3. L'autonomie, une fonction infrastructurelle

La fonction de l'infrastructure était discutée quelques mois après sa création. En 2016, de nombreux meneurs de la communauté appelaient à une intervention collective en réaction à l'événement qui avait conduit au « schisme » entre Ethereum et Ethereum Classic. Or, le principe même d'une action collective était en contradiction avec la mystique du protocole qui garantissait l'« autonomie » de l'exécution des *smart contracts*, ces « lois » auto-appliquées et auto-exécutées (voir Introduction de ce chapitre). Appuyée sur l'examen de cette controverse, cette sous-section montre que les modalités d'action collective étaient discutées en même temps que les fonctions de l'infrastructure.

TheDAO, un « hack » ?

TheDAO était une « organisation autonome décentralisée » (*decentralized autonomous organisation*, DAO) créée en 2016 par la société Slock.it. Son principe de fonctionnement était similaire à celui de DigixDAO (voir Chapitre 2, section 1) : une organisation dont les membres interagissaient *via* un site Web à l'aide de jetons dits « de gouvernance », administrés et distribués selon des règles codées dans un *smart contract*. TheDAO était conçue comme un fonds d'investissement dont les décisions étaient prises par ces jetons, et par eux seuls. Ils avaient été distribués contre des ethers qui capitalisaient TheDAO. Ils permettaient de se prononcer sur des décisions de gestion, par exemple proposer des projets auxquels allouer les fonds levés par TheDAO, de manière similaire aux prises de décisions d'actionnaires mais sans structure juridique. À l'époque, Slock.it était vue comme un acteur fiable dans le jeune écosystème Ethereum, notamment en raison de la participation de Stéphane Tual¹⁹⁵ à son conseil d'administration.

Au départ, TheDAO eu de succès. Mais quelques mois après sa capitalisation, un individu dit « hacker » parvint à transférer une part importante de la somme collectée dans le *smart contract* vers son propre *wallet*. Cette opération fut qualifiée de « vol » par une partie de la communauté Ethereum, en particulier par des investisseurs pris de panique en observant leurs fonds méthodiquement drainés vers le *wallet* de cet anonyme. Très vite, l'inquiétude se propagea à l'ensemble de la communauté Ethereum. En effet, l'événement ne menaçait pas que l'organisation « autonome » TheDAO. En effet, TheDAO avait réussi à attirer 14 % de tous les ethers en circulation à l'époque. Le larcin avait donc une grande valeur marchande (chiffré à l'époque en centaines de millions de dollars aux taux des *exchanges*). En réaction, les *exchanges* bloquèrent les transferts de fonds provenant du *wallet* du hacker. Face à cette situation, la valeur de marché de l'ether dégringolait sur ces mêmes *exchanges*. Ainsi, l'événement prenait une signification existentielle pour Ethereum : que resterait-il de l'écosystème naissant après un tel événement ?

Étant donné ces enjeux, l'événement fut rapidement problématisé comme un « vol » par

195 Ce dernier était vu comme meneur de ce qu'EvN appelait la « *non-dev community* ».

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

différents membres de la communauté qui s'exprimaient dans les arènes de discussion en ligne. Après quelques jours, VB et la Fondation Ethereum proposèrent une solution radicale : annuler le vol. Il s'agissait de réécrire la blockchain, *via* une mise à jour des logiciels clients exécutés par les *miners*, qui transférerait tous les fonds qui étaient détenus par TheDAO vers un *smart contract* tiers. Cette proposition était formulée au nom du développement de l'écosystème : ne pas intervenir aurait pu décourager investisseurs et entrepreneurs doutant de la sécurité de l'infrastructure ou face au probable effondrement du cours de l'ether.

Cette proposition fut elle-même vivement contestée par une autre partie des membres de la communauté, selon lesquels le principe d'intervention était illégitime. Il leur semblait absurde, tant il était contraire à la mystique qui était affirmée par les adjectifs « autonome » et « décentralisé » jusque dans le nom de TheDAO. Aucune intervention humaine ou communautaire n'était souhaitable : l'exécution autonome d'Ethereum garantissait que les *smart contracts* seraient exécutés tels qu'ils avaient été originellement codés. Ainsi, cet événement n'était pas un « *hack* », mais une « prouesse » ou « exploitation » (*exploit*), c'est-à-dire une utilisation habile du code déployé par Slock.it sur Ethereum. Aucune autre considération morale ou stratégique ne devait conduire à une quelconque intervention coordonnée pour modifier le registre, ce qui correspondrait à une falsification, à une « attaque ».

Finalement, la proposition défendue par la Fondation Ethereum fut largement suivie par les *miners*. Ceux qui la refusèrent se séparèrent d'Ethereum : le protocole ne connectait plus l'ensemble des *miners*, mais seulement ceux fonctionnant sur l'ancienne version. Ainsi, le réseau « bifurquait » en deux (« *fork* ») : Ethereum se séparait d'une partie de ses *miners* qui formaient un nouveau réseau appelé Ethereum Classic.

Clivage : prendre en compte l'écosystème dans l'action collective ?

Cet événement a problématisé de manière éclatante les formes d'action collective possibles dans la construction de l'infrastructure. BS, directeur de l'*Ethereum Classic Cooperative* à

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

l'époque de son *talk* à EthCC, était parmi ceux qui voyaient l'événement TheDAO comme une « prouesse » et qui avaient défendu le *statu quo* en 2016. Signe de l'importance de l'événement dans l'histoire d'Ethereum, BS s'est présenté comme représentant du « côté obscur » à la poignée d'auditeurs qui étaient venus l'écouter à EthCC. *A posteriori*, il analysait l'événement comme un révélateur de tensions entre deux « philosophies ».

*When did we have two Ethers? The conventional answer is: we had two Ethers after TheDAO. But the answer is actually: "No! We have two Ethers from the very damn beginning, but we didn't know that." Because **at the beginning we had two philosophies at the same time, one was this notion of Code is Law, then there was this other philosophy, this notion of a World Computer**. This was Vitalik's pet child, he loved this idea. The idea that you could have a universal infrastructure, that one day would get rid of Amazon EC2, and get rid of all these other things, and this thing would be this beautiful layer, this computation layer to be added to the Internet, as ubiquitous as BitTorrent or something else, and that computer would just work. You could deploy your apps on it, dApps on it; these kind of things. Here is the fundamental problem, Code is Law and World Computer. These things are philosophically so different that they can't coexist at the same time. **When you're the World Computer you have to fork a lot, you have to embrace mutability, you have to have a lot of flexibility in your platform. When you're Code is Law, you're like Bitcoin, where you set the principles, whether they're good principles or bad principles you just set them up, live with them, and build on top of them.** They're like artificial laws of physics, in a certain respect. If you're a mountain climber, you cannot suddenly say "boy! Gravity is inconvenient for me, it would be so nice if gravity would stop for a moment, and give me a break." You can't do it. (BS, EthCC, 5 mars 2020)*

Ce passage indique que les « interprétations personnelles » du « même rêve » étaient élaborées collectivement : depuis le début, Ethereum était traversé par deux « philosophies » qui « coexistaient » jusqu'au « hack » ou « prouesse ». Chacune de ces deux « philosophies » cadrerait les possibilités d'actions collectives sur l'infrastructure.

D'une part, la « philosophie » libellée « *Code is Law* » prônait l'application rigoureuse de la mystique héritée de Bitcoin. TheDAO ne devait pas faire exception au principe fondamental que j'ai analysé au Chapitre 1 comme rupture épistémique dans l'objet transaction. En d'autres termes, TheDAO était rien de plus qu'une transaction. Or, une transaction est factuelle par factuelle : elle n'a de signification que pour ceux qui l'ont demandée au départ, libres d'en définir les termes. Ainsi, une action collective sur la chaîne

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

voulait dire accorder une signification collective à une transaction, c'est-à-dire rompre le fondement même de la « sécurité » de l'infrastructure.

BS expliquait que les « principes » fixés dans le protocole étaient comme des « lois artificielles de la physique », avec lesquelles il fallait nécessairement composer. À la manière d'une escaladeuse qui devait s'accommoder de la gravitation en toute circonstance, la communauté devait s'accommoder du protocole tel qu'il avait été fixé. Selon cette perspective, l'événement n'était pas un vol mais une utilisation parmi d'autres du *smart contract* de TheDAO.

D'autre part, « *World Computer* » prônait l'intervention au nom d'un avenir désiré : faire advenir un écosystème de concepteurs et d'utilisateurs de DApps. Cet avenir était résumé par la métaphore d'un ordinateur mondial accessible par Internet capable de calculer de manière autonome. Or, souligne BS : un ordinateur se maintient en raison de sa fonction, qui suppose une intervention active. Cette métaphore de l'ordinateur était régulièrement mobilisée pour décrire Ethereum :

*Ethereum, c'est une blockchain qui veut parler **ordinateur**. Donc on se sert de la blockchain comme étant le **disque dur** de l'ordinateur. Et du coup ça pose plein de problèmes parce qu'on a besoin d'avoir un **processeur** pour exécuter ce qui se passe dans la blockchain. Et on a aussi besoin de **sauvegarder** ce qui s'est passé quelque part. Donc essayez de garder en tête que la blockchain Ethereum c'est un ordinateur dans lequel les blocs font les **transitions de l'état** de l'ordinateur vers **l'état suivant**. Et ça nous permet justement d'avoir des smart contracts, c'est-à-dire des **logiciels** qui sont déployés dans la blockchain et que tout le monde peut utiliser. (Jean, meetup #9, avril 2019)*

Cette métaphore, proposée à l'origine par VB, était largement relayée par les membres de la communauté pour expliquer le fonctionnement d'Ethereum et les problèmes posés par sa construction. Par exemple, Jean déployait la métaphore lors du meetup #9 qui regroupait des représentants de différentes associations francophones, dont Bitcoin et Ethereum¹⁹⁶ pour expliquer le fonctionnement et l'ingénierie d'Ethereum à un public plus familier du modèle

¹⁹⁶ Ce meetup, tenu en avril 2019, rassemblait différents acteurs représentants des associations des blockchains et cryptoactifs francophones, dont Adli Takkal Bataille du Cercle du Coin rencontré au Chapitre 1, Sylvain pour la ChainTech rencontré au Chapitre 2, et Jean pour l'Asseth rencontré depuis le Chapitre 2.

de Bitcoin.

Références épistémiques pour l'action collective

« *Code is Law* » et « *World Computer* » s'appuyaient sur des références épistémiques différentes. « *Code is Law* » suggérait une stricte application de lois, à la manière de lois formulées en termes mathématiques comme celles de la mécanique newtonienne. J'ai par ailleurs remarqué lors de différents épisodes d'enquêtes que les promoteurs de Bitcoin aimaient témoigner de leur fascination pour la « beauté » des mathématiques et des règles inscrites dans Bitcoin, pour leur « simplicité » et leur « transparence » technique et politique. Ce goût était visible dans la formule « *Vires in Numeris* », souvent érigée en « devise » de Bitcoin. Elle signifie « les forces dans les nombres ». Cette fascination était souvent articulée à la règle d'émission des bitcoins, dont le nombre produit à chaque bloc était fixé et exponentiellement décroissant, jusqu'à ce qu'un total de 21 millions de bitcoins soit émis d'ici une dizaine de décennies.

Au raisonnement mathématique selon un ensemble de « lois » données, c'est un raisonnement d'ingénierie des systèmes computationnels que véhicule la métaphore « *World Computer* ». Par exemple, VB mobilisait des références d'analyse des systèmes pour préciser les sens de « décentralisation » (Chapitre 1, section 2), aussi bien « architecturaux », « politiques » et « logiques » dans la production d'un nouvel Internet qu'il s'agit de construire.

*[T]oday we call those two visions ETC and ETH2, and ETC is no longer a process coin with developers, so really it's is this this thought that you've you have **Bitcoin with smart contracts**, in which '**Eth is money**'. And you know you know you have this second vision which is "**World Computer**" which is really, "**No Eth is not money, it's an application platform**" so then really what you had at the time of the DAO fork was depending on which of these visions you liked, which was the thing that spoke to you, because both of these visions were used you know if you, if you, if you looked at all the presentations at the time, both of these were given, everyone was talking about both of these, but there wasn't really a recognition, that the two of them were mutually irreconcilable. You know **they were trying to both happen within the same project**. Because yeah, **I mean if you're if you're Bitcoin with smart contracts and Ethereum is money, well, of course you don't***

intervene! You know it's money, you then you're being a [inaudible] you're moving people's money around! If you are a World computer, you know, ***if Ethereum is a world computer to you, well there's a bug in the application platform, of course you fix the bug. It's a bug. Like Eth isn't money, it's, it's just fuel!*** So I mean what that means, is that while you have the most kind of you know socially painful split at the time of the DAO fork, the two projects are not, you know then, it's not a zero something that, they're different and you know, that they are both useful visions. (BS, EthCC, 5 mars 2020)

Les deux « visions », ETC et ETH2, soulignent une différence de rapport au temps pour l'action collective. D'une part, un rapport limité à l'action présente des *miners* avec ETC qui désigne Ethereum Classic¹⁹⁷, une sorte de « Bitcoin avec des *smart contracts* ». D'autre part, un rapport futur orienté vers des évolutions profondes du système. ETH2 désigne « Ethereum 2 », un projet d'évolution majeur d'Ethereum¹⁹⁸ intégrant une transformation de la méthode de validation des transactions. Selon ce projet, les transactions ne seraient plus validées par des *miners*, mais par des *stakers*. Le changement de rôle des validateurs visait à préserver la mystique, en changeant l'unité sur laquelle établir la compétition. La « preuve de travail », fondée sur une dépense d'énergie électrique, serait remplacée par une « preuve d'enjeu », fondée sur les ethers « gagés » (*stake*). Ainsi, la mystique serait préservée mais améliorée pour permettre de « passer à l'échelle ».

Enfin, ces différences de visions de l'action collective se lisent dans le regard porté sur l'unité de compte du réseau, l'ETC pour Ethereum Classic, et l'ETH (ether) pour Ethereum. La controverse sur TheDAO a en effet muté en d'autres termes : « est-ce que l'ether est de l'argent ? »¹⁹⁹ (*is ether money ?*). Les partisans de « *Code is Law* » soutenaient que « l'ether [était] de l'argent », en donnant à « argent » la signification monétariste héritée de Bitcoin : l'ether devait avoir une valeur intrinsèque, conférée par l'autonomie de toute politique monétaire autre que celle inscrite dans le code informatique. Au contraire, les partisans de « *World Computer* » voyaient plutôt l'ether comme du « fuel », un carburant qui était brûlé dans le calcul nécessaire à l'exécution des *smart contracts*. Selon cette conception, la fin de

197 Le trigramme est également utilisé pour désigner la devise utilisée par la chaîne issue de la bifurcation, pour le distinguer de l'ether, ETH.

198 Ce projet s'est traduit en transformation concrète de l'infrastructure à l'automne 2022.

199 Cette controverse est devenue si visible que différents membres de la communauté affichaient leurs positions dans leurs profils, sur des arènes de discussion en ligne ; sur Twitter, on pouvait par exemple voir le compte de Vlad Zamfir intitulé « Vlad 'eth is money' Zamfir »

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

l'ether n'était pas sa thésaurisation, mais une marchandise spécifique à l'exécution des DApps.

| <i>Infrastructures</i> | Ethereum Classic | Ethereum |
|-----------------------------------|--|--|
| <i>Problématisation de TheDAO</i> | « Prouesse » (<i>exploit</i>) | « Vol » |
| <i>Métaphore</i> | « <i>Code is Law</i> » | « <i>World Computer</i> » |
| <i>Vision de l'infrastructure</i> | « Bitcoin avec des <i>smart contracts</i> » | Ethereum 2, plateforme de DApps |
| <i>Vision de l'unité</i> | ' <i>eth is money</i> ', or | ' <i>eth is not money</i> ', fuel |
| <i>Savoirs</i> | Mathématiques, lois naturelles | Informatique, sciences expérimentales |
| <i>Interventions</i> | Changements rares, priorité à la stabilité par les core devs / <i>miners</i> | Prise en compte du développement de l'écosystème dans l'instauration |

Tableau 14 : Récapitulatif des principes de connaissance et d'intervention sur Ethereum et sur Ethereum Classic

L'autonomie de l'infrastructure : un concept défini en situation

C'est comme un « échec » que l'événement naturalisé comme « *hack* » est discuté dans la littérature (DuPont 2018 ; Morrison et al. 2017 ; Shier et al. 2019). TheDAO est analysée comme cas de DAO, décrit comme une forme de gouvernance d'entreprise prometteuse. Les DAO seraient des structures permettant de formaliser ses actionnaires (*wallets* des participants), ses modes de prises de décisions (code du *smart contract*), ses capitaux (jetons, *wallet* du *smart contract*). Ces travaux cherchent à évaluer la promesse communément prêtée aux DAO : leur transparence, leur efficacité, leur justesse algorithmique et leur caractère radicalement démocratique. Elles promettraient de débarrasser les entreprises des activités de gestion qui ne nécessiteraient pas d'intervention humaine en dehors du vote des actionnaires. Les DAO ont ainsi été associées à une promesse de désincarnation humaine des processus de gestion des organisations, dans des littératures touchant souvent à l'économie institutionnelle, aux études institutionnelles de la finance, et aux sciences des systèmes informatiques (voir par exemple Beck et al. 2018 ;

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Kondova & Barba 2019 ; Yue 2020).

Ces travaux voient une contradiction entre l'autonomie annoncée des *smart contracts* et ce qui apparaît comme une nécessité d'intervention en situation d'urgence. Cet événement montrerait que la gouvernance automatisée et décentralisée contredit la « rhétorique utopique » déployée par les promoteurs des DAO et des blockchains (DuPont 2018 : 173). Une dissonance similaire est pointée par Morrison et ses co-auteurs, pointant l'importance, selon des degrés divers en fonction des formes que pourraient prendre les DAO, de la « confiance » dans des organisations qui prétendent s'en affranchir (Morrison et al. 2017 : 12). Ces travaux soulignent l'intervention d'un nombre important d'acteurs « humains », en dehors des règles établies dans le *smart contract* de TheDAO. DuPont souligne par exemple que de nombreux acteurs s'indignaient dans les arènes de discussions en ligne de la proposition d'une solution « centralisée » (notamment par VB) pour résoudre un problème de gouvernance supposée décentralisée.

L'examen de controverses au sein de communautés montre que l' « autonomie » est le résultat d'un travail de conception d'infrastructures et de constitution des communautés qui n'est jamais acquis. L'autonomie est qualifiée, temporairement stabilisée selon des modalités d'intervention collectives sur l'infrastructure. L'autonomie fait partie des fonctions de l'infrastructure. Les règles du protocole ne réduisent pas l'activité des individus peuplant les communautés à l'exécution de rôles prédéfinis ; l'action collective, ou interventions concertées sur l'infrastructure, existent y compris chez Bitcoin ou avec la ligne « *Code is Law* » avec l'activité des *core dev*.

Le cas d'Ethereum avec TheDAO montre que l'autonomie est elle-même controversée : alors que la ligne « *Code is Law* » réduit l'autonomie à la mystique, « World Computer » embarque des entités qui lui sont étrangères, par exemple avec la préoccupation pour le maintien du prix de l'ether sur les *exchanges* ou la crainte de faire fuir des entrepreneurs et des investisseurs. Ce faisant, l'action collective de « bifurcation » affirmait qu'Ethereum était indissociable d'un écosystème bénéficiaire de cette « autonomie ».

2. Gouverner le développement de l'écosystème au prisme de la mystique

L'imaginaire d'une infrastructure autonome ne résistait pas à son développement pratique qui nécessitait des interventions régulières : minimales selon la perspective « *Code is Law* », étendues à la prise en compte de l'écosystème avec « *World Computer* ». Cette section analyse la prise en charge l'extension du gouvernement de l'infrastructure par la communauté au-delà de la seule construction de l'infrastructure matérielle.

La première sous-section s'appuie sur le cas de la controverse TheDAO pour proposer une grammaire de l'action collective en termes de décisions et de délibérations. Elle montre que l'infrastructure est le support incontournable de toute décision collective légitime, et que la « bonne » délibération suppose une anthropologie moutonnaire. La deuxième sous-section s'appuie sur l'extension du gouvernement au « financement des biens publics ». Elle montre que la « bonne » gouvernance est dépouillée de toute forme d'organisation formelle, suspectes par hypothèse de toute forme de favoritisme envers certains membres de la communauté. La troisième sous-section répond à la seconde. Le « bon » gouvernement est un ensemble de mécanismes automatiques pensés selon la mystique : ils doivent produire une action collective (financer des « biens publics ») indépendamment de l'inclinaison rationnelle de chacun à les contourner. Enfin, la dernière sous-section expose une condition essentielle du fonctionnement de ces mécanismes. Les individus doivent agir « authentiquement » par le vote, c'est-à-dire penser leur intérêt individuel à la lumière de l'intérêt collectif, de la même manière que ce que prescrit la mystique aux *miners* qui doivent être indifférents aux significations des transactions.

2.1. Actions collectives sur et par l'infrastructure

La controverse autour de TheDAO informe sur les possibilités d'actions collectives, elles-mêmes controversées. Dans cette sous-section, je propose une grammaire de l'action collective à partir de cette controverse en termes de « décision » et de « délibération ». Je

propose ces termes pour analyser le regard que les acteurs portent sur leurs propres actions en tant que groupe ; eux parlent plutôt d'actions « sur » ou « hors » de la blockchain (« *on chain* » ou « *off chain* »). Puis, à partir d'écrits de l'inventeur d'Ethereum, je pointe l'anthropologie sous-jacente aux formes d'actions collectives vues comme légitimes, qui suppose une anthropologie moutonnaire.

Grammaire de l'action collective : le cas de la controverse TheDAO

La controverse qui s'est jouée autour de TheDAO a montré des divergences au sein de la communauté concernant les entités à faire compter dans l'action collective : la ligne « *World Computer* » tenait compte d'agir au nom du développement de l'écosystème quand la ligne « *Code is Law* » excluait toute intervention concertée sur la blockchain au nom de la mystique (section 1.3 de ce chapitre). Quatre types d'actions collectives différentes peuvent être identifiées ; ils sont résumés dans le Tableau 15 ci-après. Chaque ligne propose un type d'action collective, décrit à partir du cas dans la controverse TheDAO, le groupe constitué dans cette action, et les conséquences de cette action vues par le groupe concerné.

« Décider sur la chaîne ». TheDAO était construite comme un fonds d'investissement dont le fonctionnement attendu était d'être « autonome » car les décisions collectives étaient exécutées par un *smart contract*. Les investisseurs participant à TheDAO votaient pour des propositions d'allocations des ethers levés en commun *via* des jetons de gouvernance, émis en proportion des ethers fournis, à la manière d'un fonds d'investissement dont les décisions étaient traduites par des votes *via* ce *smart contract* qui exécutait ces décisions en transférant les ethers vers les bénéficiaires. Ce mécanisme était l'utilisation « normale » de TheDAO (Tableau 15, Ligne 1).

« Délibérer de la chaîne ». Quand est survenu l'événement qui devenait qualifié de « vol » ou de « prouesse », un processus de délibération s'est déployé sur différentes arènes de discussions en ligne, et certainement (je n'enquêtai pas à l'époque) dans des espaces physiques comme les meetups ou les conférences internationales. Ce processus de

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

délibération informel engageait des individus, identifiés ou anonymes, ainsi que organisations (comme des groupes de développeurs ou des startups). Différentes personnes influentes ont notamment mis tout leur poids dans la décision de bifurcation de TheDAO²⁰⁰ (Morisson & al 2017, DuPont 2018). Le mécanisme de décision « normal » qui postulait l'autonomie de TheDAO (Tableau 15, Ligne 1) était au cœur de ces discussions portant sur la chaîne elle-même : il était question de savoir si elle devait être réécrite ou non (Tableau 15, Ligne 2).

| | Type | on/off chain | Action collective | Groupe | Conséquences |
|---|--------------------------------------|--------------|--|---|---|
| 1 | Décider sur la chaîne | on chain | Gouvernance normale de TheDAO : gestion du fonds et leur exécution | Les détenteurs de jetons de gouvernance | Transferts d'ethers dans le <i>smart contract</i> de la DAO |
| 2 | Délibérer de la chaîne | off chain | Délibérations publiques (forums, meetups, etc.) | L'écosystème | Progression du débat public |
| 3 | Délibérer sur la chaîne de la chaîne | on chain | CarbonVote : délibération formalisée par un vote | Les détenteurs d'ethers | Expression d'un avis majoritaire |
| 4 | Décider de la chaîne | on chain | Mise à jour des logiciels clients : réécrire la blockchain ou non | Les <i>miners</i> | Séparation entre Ethereum et Ethereum Classic |

Tableau 15 : Types d'actions collectives dans la controverse TheDAO

« Décider de la chaîne ». À la différence des discussions auxquelles quiconque pouvait participer *via* les arènes de discussion en ligne, la décision finale revenait aux seuls *miners* qui ont choisi de mettre à jour leurs logiciels clients (joignant ainsi le réseau reconnu comme « Ethereum » en « bifurquant ») ou non (joignant alors « Ethereum Classic »). Ce mécanisme consistait à décider de la chaîne elle-même, chaque *miner* participant à former

²⁰⁰ La réputation de ces dernières s'observe notamment par leurs rôles ou fonctions (dans les équipes de développement d'Ethereum, à la Fondation Ethereum ou chez ConsenSys, dans les équipes qui ont lancé TheDAO chez Slock.it) mais aussi en fonction de métriques : nombre d' « *upvotes* » sur Reddit ou nombre d' « *applauses* » sur Medium. Ces votes propres à des plateformes sur lesquelles les débats avaient lieu ont eu de l'importance.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

une des deux chaînes issues de la bifurcation. Ce mécanisme est listé dans le Tableau 15, Ligne 4.

« Délibérer sur la chaîne de la chaîne ». Un mécanisme de délibération par votes a été mis en place *via* un site Web²⁰¹ et un *smart contract* dédié, en pleine controverse et avant la décision de bifurcation, courant juin 2016. Tout détenteur d'ethers pouvait « voter » pour ou contre la bifurcation d'Ethereum. Selon la page web du site, l'initiative était lancée par la communauté chinoise Ethfans, ainsi que par trois organisations nommées Cryptage, ConsenLabs et StoneLedger²⁰². L'interface Web affichait les règles de fonctionnement du *smart contract* par lequel les voix étaient comptabilisées ; un vote « pour » (respectivement, « contre ») devait être exprimé comme une transaction (de montant nul) vers une adresse donnée (respectivement, vers une autre adresse). CarbonVote affichait les résultats de ce vote en temps réel ; le résultat est reproduit en Figure 27. Ce mécanisme est listé dans le Tableau 15, Ligne 3.

Ce mécanisme était mobilisé par les partisans de la bifurcation (de la réécriture de la blockchain) qui y voyaient une expression nette de la communauté pour la bifurcation. Ce vote ne déclenchait aucune décision : il participait au débat public sur l'opportunité de réécrire la chaîne ou non. Mais à la différence du débat public tous azimuts sur les différentes arènes de discussion (« délibérer de la chaîne », Ligne 2), il était présenté comme représentatif de l'ensemble des porteurs d'ethers. Ce raisonnement s'appuyait sur la forme de ce vote : il était organisé *via* un *smart contract* pour affirmer la légitimité du vote. Le vote par *smart contracts* permettait, au moins en théorie, de limiter les votes aux détenteurs d'ethers et de garantir l'unicité de « votes » qui étaient proportionnels à la quantité d'ethers détenus.

201 Le site était toujours accessible début 2022, à l'adresse : <https://v1.carbonvote.com/>.

202 À partir du site de l'Internet Archive *Wayback Machine* qui donne accès à des clichés de pages Web enregistrées à différentes dates : je n'ai obtenu aucune information sur Cryptage (le nom de domaine était en vente aux deux dates les plus proches où des clichés ont été pris, en janvier 2016 et en octobre 2016), ConsenLabs semble avoir été une organisation qui affichait dans ses principaux succès le soutien à Ethfans et la participation à la mise en place de CarbonVote, et StoneLedger semble avoir été la vitrine d'une société de prestations de services dont l'authenticité pose question (nom du cofondateur laissé par défaut en « Name », profils d'employés en « John Doe »...).

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

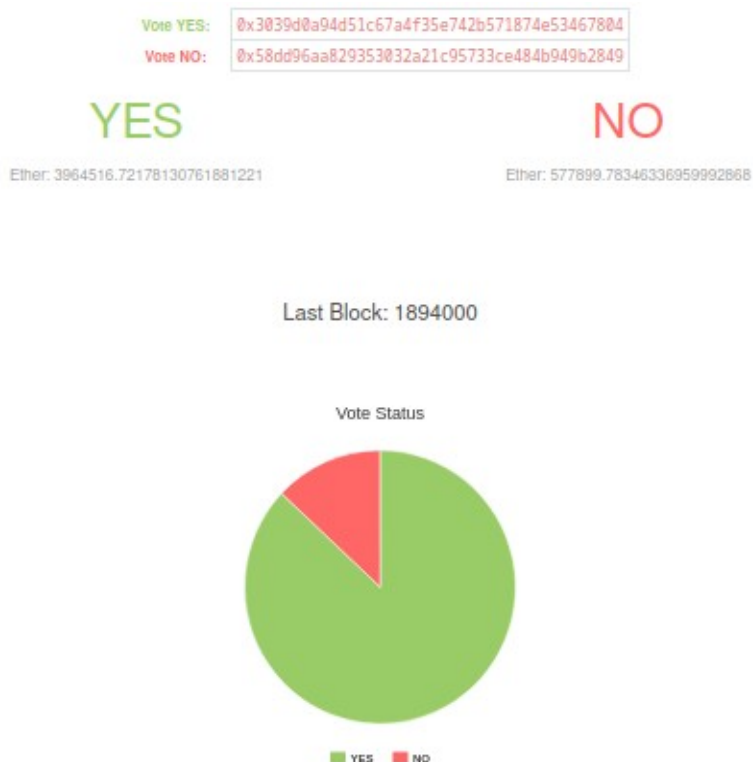


Figure 27 : Résultat affiché du vote (CarbonVote 2022)

Au contraire, les détracteurs de ce mécanisme dénonçaient son principe et la représentativité des porteurs d'ethers (phyro 2018). D'une part, ce mécanisme était vu comme illégitime par principe, comme toute tentative de coalition visant à changer les seuls faits valables : le blockchain. C'était la ligne « *Code is law* » ; une action collective visant à modifier l'exécution d'un *smart contract* revient à contredire le fondement de la souveraineté individuelle par des contrats auto-exécutants par une quelconque intervention humaine, c'est-à-dire ne plus se prémunir de « politique » (Idle 2016).

D'autre part, en plus d'être dénoncé pour son illégitimité de principe, ce vote était vu comme non représentatif : le mode de scrutin « 1 ether = 1 voix » avantageait les acteurs qui faisaient campagne pour la bifurcation (comme la Fondation Ethereum ou l'entreprise Slock.it qui avait créé TheDAO). Différents arguments ont été avancés en ce sens. Premièrement, les votes exprimés étaient concentrés entre peu d'humains : un seul *wallet* Ethereum comptabilisait près d'un quart de tous les ethers en circulation, donc des voix, en

faveur de la bifurcation. Deuxièmement, moins de 6 % des ethers en circulation avaient servi au vote, soit par manque d'information sinon par ignorance du processus de vote. Troisièmement, les investisseurs de TheDAO étaient plus incités à participer au vote (et à voter pour la bifurcation) que les autres détenteurs d'ethers. Comme dans le cas des « bifurcations » portant sur un logiciel et non sur une infrastructure comme dans le cas présent, différentes parties prenantes ignorent le problème ou les enjeux du débat (Demazière, Horn & Zune 2006). Ces deux dernières critiques étaient illustrées sur un graphique reproduit en Figure 28. Il figurait à la section (ironiquement) intitulée « *Democracy in Action* » d'un document publié par un opposant à la bifurcation.

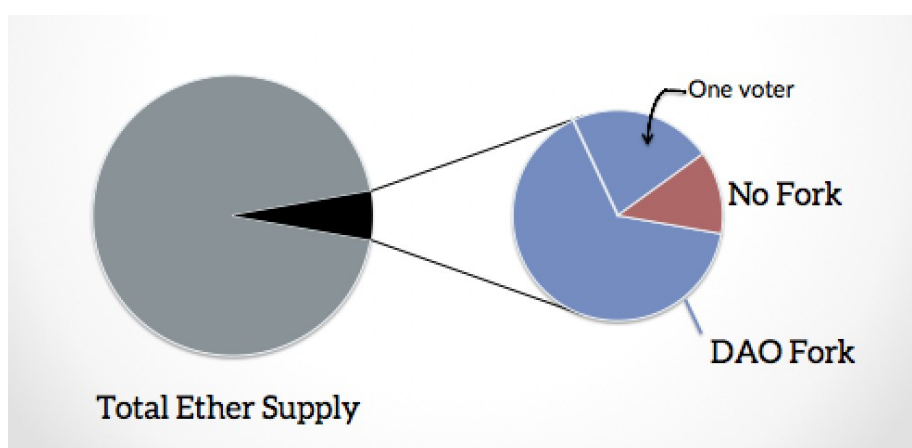


Figure 28 : Graphique critique de CarbonVote, produit par un opposant à la bifurcation (Idle 2016)

Délibération : nécessité et théorisation vernaculaire

Le cœur de la controverse autour de TheDAO portait sur les raisons et les groupes au nom desquels il était légitime d'agir sur l'infrastructure. La grammaire résumée dans le Tableau 15 montre que « décision collective » prend toujours la signification d'inscription sur la chaîne ou « *on chain* » dans le langage des acteurs. Cette inscription est vue comme un fait, elle matérialise les conséquences de l'action collective (transferts de jetons dans le cas de la gouvernance « normale » de TheDAO en Ligne 1, ou réécriture de la chaîne dans le cas de la Ligne 4). Il est intéressant de remarquer que cette « factualité » de l'inscription est exportée dans le cadre de ce que j'ai appelé « délibération » (Ligne 3), et de préciser les

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

antagonismes de rapports à la légitimité à l'action collective entre les partisans de « *Code is Law* » et de « *World Computer* ».

« *Code is Law* » était opposée à toute forme de délibération sur l'évolution de l'infrastructure qui remette en cause une décision préalablement prise *on chain*. C'est en ce sens que « *code is law* » : le code d'un *smart contract* ne doit pas être remis en question. Les partisans n'étaient pas opposés en principe à une mise à jour des logiciels clients par les *miners* ; par exemple, cette position était compatible avec le fait d'être pour l'augmentation de la taille des blocs. Le problème ici relevait de cette mise à jour là (Ligne 4), proposée au nom de la réécriture d'une décision (Ligne 1) qui était par définition vraie ou factuelle. Pour eux, l'état de la chaîne était authentique en vertu de la mystique, qui était contredite par les différents processus délibératifs qui faisaient du code du *smart contract* de TheDAO un problème collectif d'intervention sur l'infrastructure (Lignes 2 et 3).

Leurs contradicteurs reconnaissaient eux aussi le caractère incontestable des décisions prises sur la chaîne (*via les smart contracts*), mais en principe seulement ; ils opposaient dans ce cas précis une raison d'un ordre supérieur : la survie de l'infrastructure, dépendante d'un ensemble dont ils faisaient un acteur de la politique de l'infrastructure, l'écosystème. La construction de ce problème d'ordre supérieur se distingue selon les corps politiques participant à la délibération et la force donnée à l'action de délibération : d'une part, un processus de délibération collective ouverte à propos de la chaîne, c'est-à-dire la problématisation publique d'un objet jugé incontestable par principe (Ligne 2) ; d'autre part, une tentative de rendre légitime (car inscrite sur la chaîne, *via le smart contract* de CarbonVote) la délibération publique consistant à s'écarter exceptionnellement de la mystique. Je comprends cette dernière action comme tentative d'ériger les porteurs d'ethers en souverains : au nom de ces derniers pouvant voter *via CarbonVote*, les *miners* deviendraient les exécutant de la décision d'une nouvelle chaîne.

VB étaient de ceux-là. Plusieurs mois après cette séquence, il reconnaissait la nécessité de délibérer au sein de la communauté pour des évolutions de l'infrastructure, en particulier touchant aux évolutions du protocole de consensus et au financement des « biens publics »,

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

notion qui sera précisée à la sous-section suivante (Buterin 2017b, 2021). Toutefois, les mécanismes de délibération légitimes devaient être « *on chain* », comme le vote organisé *via* CarbonVote dont il reconnaissait à la fois les limites pointées par les détracteurs et sa légitimité de principe. Notamment, l'auteur pointait la nécessité de délibération dans l'élaboration même des mécanismes *on chain*. Avec d'autres meneurs, il s'opposait à l'idée « d'expurger complètement » les « intuitions et sentiments humains doux et mous en faveur d'une gouvernance entièrement algorithmique » (Buterin 2017b, 2018 ; Zamfir 2017).

Ce que j'appelle « délibération » apparaît sous la plume de VB avec la notion de « gouvernance ». Elle désigne la nécessité collective d'orienter l'action de chaque individu supposé être en situation de « jeu coopératif ». La théorie des jeux coopératifs est une branche de la théorie des jeux qui postule que les individus (« joueurs ») agissent (« jouent ») à la seule lumière de leur intérêt individuel, ce dernier prenant en compte la possibilité d'alliance avec d'autres individus. Ces situations se distinguent des jeux non-coopératifs, dans lesquelles les joueurs n'ont pas de possibilité de construire des alliances autres que des accords entre deux joueurs, lesquelles tiennent tant que les deux joueurs maintiennent cet accord. La théorie des jeux coopératifs se donne comme objectif d'étudier quelles coalitions se forment en fonction d'un problème (ou « jeu ») donné. Les actions d'un groupe sont décrites en termes de bénéfices (*payoffs*) collectifs. Avec Ethereum et pour Buterin, les utilisateurs et les *miners* sont en situations de jeux coopératifs, libres de passer des transactions ou de participer à l'exécution du protocole de consensus en fonction de leurs intérêts.

Cette orientation des actions individuelles passe par ce que VB appelle des « institutions de coordination » dont le rôle est de lever des « drapeaux de coordination » (*coordination flags*). C'est ainsi que VB comprend les logiciels « clients » des *miners* : ils font une « levée de drapeaux », quand une bifurcation a lieu : ainsi, les *miners* qui font confiance aux développeurs des clients peuvent suivre la nouvelle chaîne selon leur « propre intérêt » car ils comprennent que les autres *miners* la suivront aussi. Ils peuvent donc faire alliance avec eux en mettant à jour leur logiciel client. CarbonVote est explicitement cité par VB comme exemple d'instrument participant à une « levée de drapeaux » ; dans la controverse

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

TheDAO, le site servait en effet à faire émerger un avis majoritaire que les autres puissent suivre. Le rôle de ces institutions est de « créer des points focaux » indiquant aux acteurs « comment se comporter pour mieux coordonner leur comportement » :

*You can think of coordination institutions as putting up **green or red flags in the air saying "go" or "stop", with an established culture that everyone watches these flags and (usually) does what they say.** Why do people have the incentive to follow these flags? Because everyone else is already following these flags, and **you have the incentive to do the same thing as what everyone else is doing.** (Buterin 2017b)*

Cette proposition contient une hypothèse anthropologique : les individus partagent une « culture » qui les fait « regarder » ces drapeaux ; chacun est « incité » à « faire la même chose que les autres ». Ainsi définie, la gouvernance est l'art de former des coalitions d'individus par des signaux qui conduisent chacun à agir tel qu'il imagine que la majorité du groupe auquel il appartient agira. Ces institutions de coordination visent à produire des comportements collectifs moutonniers. VB explique ce phénomène à l'aide d'une métaphore : ces institutions de coordination doivent agir comme un général d'armée suivi par son armée, face à une ville ennemie. Le général qui lève un drapeau a pour intention de rassurer chaque soldat sur le fait que tous les autres soldats se sentent « courageux et excités » et qu'ils chargeront eux aussi, de sorte que chaque soldat individuellement soit « rassuré » sur le fait que les autres suivront et qu'il ne « se suicidera pas en chargeant seul ».

2.2. Le financement des « biens publics » : cas de problématisation de l'action collective

Le financement de choses susceptibles de bénéficier à un ensemble indiscernable de personnes était assuré par des organisations comme ConsenSys ou la Fondation Ethereum. En problématisant leur rôle, l'inventeur d'Ethereum posait le problème du bon gouvernement de l'infrastructure. L'enjeu n'était pas d'agir collectivement à un instant donné, mais de définir les bonnes manières de gouverner l'infrastructure, au sens de garantir le financement des choses qu'il appelait les « biens publics ». Cette sous-section

montre que ce bon gouvernement était d'abord envisagé par la négative : il ne devait pas être incarné par une organisation formelle. La sous-section suivante s'intéresse à la manière dont ce bon gouvernement était imaginé positivement.

Financer les « biens publics » de l'écosystème : un problème de gouvernement

Une explosion de rires accueillait la référence orale et visuelle à l'URSS (Figure 29) lors du *talk* intitulé « *Funding ecosystem public goods* » de VB, première tête d'affiche d'EthCC. À ce moment de climax, l'influent inventeur d'Ethereum décrivait l'écosystème comme un pays et ConsenSys et de la Fondation Ethereum les bureaucraties gouvernementales de ce pays. Le mot d'humour de VB faisait vibrer une corde sensible de la communauté : le rejet d'acteurs « centraux » gouvernant le développement d'Ethereum.

*So the status quo of **public goods funding in crypto** is largely that you have a small number of bureaucracies [that] handle it. So in countries, you know the bureaucracies are basically the government. **In the Ethereum ecosystem you have the Ethereum Foundation, you have ConsenSys, and then you have a couple of other groups that kind of varying sizes [...]** So we have a bunch of bureaucracies, and let's call them **Central Capital Coordinators for Public Goods**. We can call them **CCCPs**. (VB, EthCC, 3 mars 2020)*

Ce faisant, le meneur d'Ethereum posait un problème de politiques publiques à l'échelle de la communauté : comment financer toutes ces choses qui bénéficient à tout l'écosystème ? Ces choses étaient aussi diverses que la « sécurité du réseau », la recherche en sciences informatiques et économiques, le développement d'interfaces avec le dispositif technique (logiciels clients pour les nœuds ou *miners*, *wallets* pour les utilisateurs), le développement de protocoles de « deuxième couche »²⁰³, la documentation en ligne, la formation et la communication, ou encore l'audit de *smart contracts*.

VB appelait ces choses « biens publics »²⁰⁴. Cette notion est à comprendre au sens de la

203 Il s'agissait notamment de protocoles fonctionnant *via* des *smart contracts* pour améliorer le « passage à l'échelle ».

204 Cette notion peut aussi se comprendre au sens que l'économiste Paul Samuelson donnait aux « biens de consommation collective », dont la consommation par tout individu (en fonction de ses préférences

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

théorie économique : des bien non rivaux (dont la consommation n'affecte pas la quantité disponible pour les autres) et non-excluables (ils bénéficient à quiconque) entre acteurs de l'écosystème. Avec cette notion, VB voyait la nature informationnelle de ces choses comme un problème qui imposait une « conduite », une « prise en main » (« *handling* »)²⁰⁵ collective.

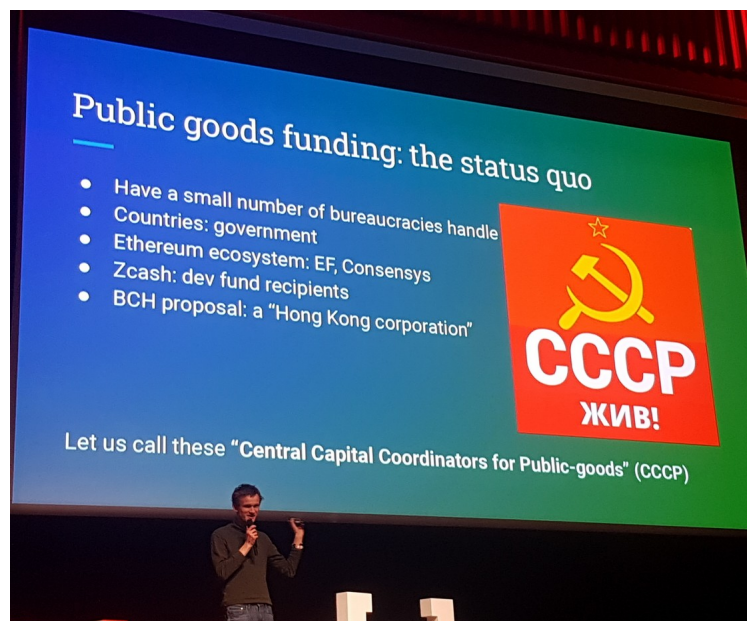


Figure 29 : Vitalik Buterin pose le problème de financement des « public goods » comme un problème de gouvernement

Cette nécessaire prise en main était conséquente de l'insuffisance des mécanismes de marché pour assurer le développement à long terme de ces biens informationnels : il n'existait pas de rencontre entre offre de ces biens au sein de la communauté et demande rémunératrice de l'écosystème. Ce problème était décrit par Paul Samuelson en termes

ordinales) n'empêchait pas la consommation de ce même bien par d'autres. Ces biens s'opposent aux ordinaires « biens de consommation privée », qui sont répartis entre différents individus (Samuelson 1954).

205 Verbatim du passage : « So, just because, if Ethereum is a part of cyberspace and cyberspace is fundamentally about information, and most informational things just tend to be public goods of some form or another. Ethereum ecosystem, just has a lots and lots of public goods that... And another public good is possibly even larger than the number of private goods in the ecosystem. And so we need to have some way of handling them. »

d' « effets externes » intrinsèques à la notion de « biens de consommation collective », impossible à régler par les mécanismes « ordinaires de prix de marché » (Samuelson 1954 : 389). Buterin cadrerait le financement de ces biens comme un problème d'allocation.

« Biens publics » et communauté de joueurs rationnels

Cette situation était expliquée par la situation typique de Bob, « bâtisseur de biens publics » confronté à un dilemme (Figure 30). L'activité de Bob était de construire des biens publics d'un genre particulier : du code *open source*. Bob était dans une situation de « jeu », au sens de la théorie des jeux : il évaluait les bénéfices qu'il pouvait tirer de son action de construction d'un bien public. Bob ne comprenait pas que l'écosystème l'ait rémunéré 545 dollars pour trois mois de travail alors que, dans le même temps, des « arnaqueurs ICO »²⁰⁶ obtenaient un milliard de dollars avec un jeton. Ce faisant, VB battait en brèche l'hypothèse d'un financement par des dons sur lesquels misaient, selon lui, les développeurs de logiciels *open source*. Avec l'illustration par les excès des ICO, VB expliquait qu'il était inconcevable que les personnes susceptibles de participer au développement de ces choses qui bénéficiaient à tous continuent d'être incitées à le faire avec des dons largement en deçà des opportunités propres à l'écosystème. Ce faisant, il faisait de Bob un individu seul, dont la tâche était accomplie de manière isolée plutôt que de manière communautaire, un mode de production qui n'est pas nécessairement monétaire sans toutefois reposer sur le don ou l'altruisme (Gensollen 2004).

Sans politique de financement, à laquelle appelait VB dans son *talk*, Bob resterait confronté à l'alternative entre travail gratuit et saisie des opportunités de l'écosystème. La première possibilité dite « altruiste » n'était pas représentée à l'écran. Cette invisibilité n'avait rien d'anodin : comme dans la théorie des jeux, l' « altruisme » était une hypothèse théorique qui n'entrait pas dans l'analyse puisque, par définition, elle n'apportait pas de bénéfice monétaire. Ainsi, Bob devait saisir les opportunités de l'écosystème pour bénéficier de son action de construction des biens publics. Il avait deux options offertes par l'écosystème, conduisant à « deux problèmes ». La première option consistait à se financer par l'émission

206 Voir le Chapitre 2 pour une analyse du phénomène des ICO.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

de jetons (ICO). Ce mécanisme était raillé par VB : il moquait la posture d'un Bob contraint de prétendre que son jeton « n'est absolument pas un titre financier » en dépit du fait qu'il représente des « parts de revenus futurs de [sa] camelote propriétaire » dont il contrôlera le développement futur²⁰⁷. Cette moquerie fait écho à la section 2 du Chapitre 2, qui indiquait que les portes-paroles de l'écosystème avaient travaillé à enrôler les autorités publiques pour rester maîtres de la signification des jetons d'ICO, ce qui soulevait des interrogations au sein même de la communauté. Ce passage montre que, près de deux ans plus tard, le scepticisme sur la signification des jetons d'ICO demeurait au sein de la communauté.

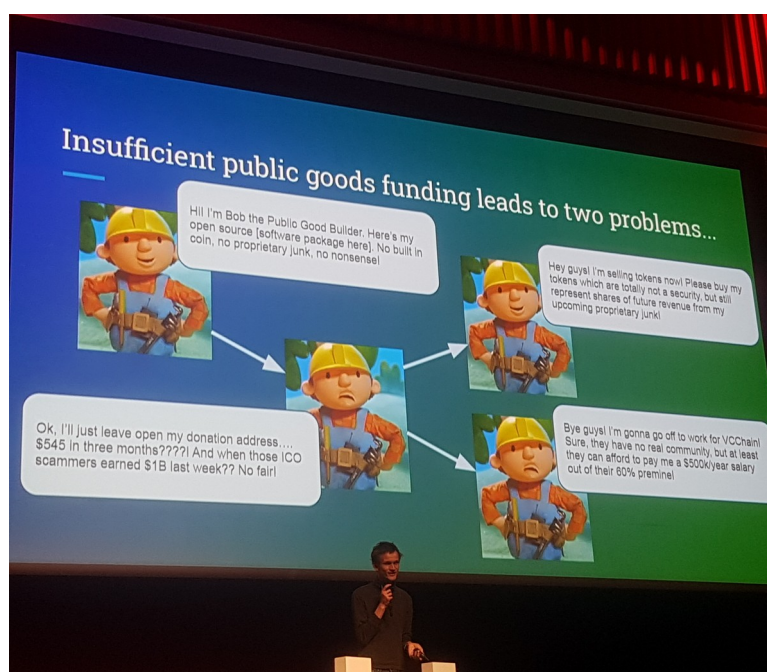


Figure 30 : Vitalik Buterin explique le problème de la rémunération des « public goods builders »

La seconde option offerte à Bob consistait à rejoindre la dynamique B2B décrite au Chapitre 3 : se faire embaucher pour 500k\$ par an par un consortium de banques ou d'entreprises, sinon par un fonds de capital-risque finançant une blockchain publique mais contrôlée par ce dernier²⁰⁸. Cette seconde option était présentée comme encore plus

207 La diapositive indique : « Hey guys! I'm selling tokens now! Please buy my tokens which are totally not a security, but still represent shares of future revenue from my upcoming proprietary junk ! »

208 La diapositive indique : « Bye guys! I'm gonna go off to work for VCChain! Sure, they have no real community, but at least they can afford to pay me a \$500k/year salary out of their 60% premine! »

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

défavorable pour Bob, contraint de quitter la communauté²⁰⁹.

Ainsi, VB cherchait à tracer un chemin alternatif au modèle du don ou aux modes de financement des utilisations B2C comme B2B. Il pointait une tension entre la rémunération d'une activité de l'écosystème (dynamiques B2B et B2C) et la rémunération d'une activité au service de l'écosystème (biens publics). Cette problématisation formule de manière originale la question de l'articulation entre les concepteurs de services numériques (ici, les DApps dans les utilisations B2C ou les *consortia* dans les cas B2B) et les communautés de développement de logiciels open source. Cette question a récemment été analysée, dans des cas de rapports entre grands acteurs du numérique (en lieu et place de l'« écosystème » ici) et communautés de développements libres et open source par l'angle de la participation contre-intuitive des seconds à la construction de l'offre de services des premiers, assimilés à des représentants du capitalisme numérique (Cohen 2019 ; Broca 2021). Ici, VB ne thématise pas de tension entre communauté et écosystème ; il n'y a pas de tension entre communs et partage, d'une part, et capitalisme et extraction, d'autre part. Le cadre théorique de VB dissout cette tension : chaque Bob de la communauté (individu ou organisation) est placé face à un choix individuel et rationnel.

Ce chemin partait du cadrage de la communauté comme un ensemble de joueurs cherchant à maximiser leurs bénéfices par l'activité de construction de biens publics. Il décomposait le problème du financement en deux sous-problèmes. D'une part, le problème de l'origine des financements (d'où vient l'argent ?) ; d'autre part, le problème d'allocation des financements (à qui allouer l'argent ?). Ces solutions envisagées à ces deux problèmes sont analysées à la sous-section suivante (2.3).

L'enjeu de ce travail était d'imaginer des réponses à ces deux questions sans implication d'organisations comme ConsenSys ou la Fondation Ethereum qui finançaient en effet le développement de « biens publics », mais incarnaient un « gouvernement » exerçant une « coordination centrale » qui était incompatible avec les principes d'actions collective de la communauté. Les paragraphes suivants montrent, avec le cas de l'« *ethereum support*

209 À l'écran : « *Hey guys!* » avec un Bob souriant pour la première option, contre « *Bye guys!* » avec un Bob qui semble triste pour la seconde.

program » de la Fondation Ethereum, que le rejet de ces formes de « coordination centrale » était réfléchi au sein même de ces organisations. Leurs porte-paroles minimisaient leur propre pouvoir de décision en se donnant un rôle procédural au sein de l'écosystème.

Le financement par les organisations : suspect par hypothèse

Le problème des « bureaucraties » tenait à leur capacité d'action unilatérale, tant dans les critères que dans les modes d'allocation des financements dont elles disposaient. Autrement dit, le problème n'était pas qu'elles financent peu, mais qu'elles puissent mal financer.

Ainsi, VB donnait à voir un nouvel angle de controverse à propos de ConsenSys. Nous avons vu que l'entreprise était controversée en raison de ses alliances stratégiques avec les banques, à l'origine d'un « schisme ». BS relatait une critique de ConsenSys vis-à-vis de son objet : faire d'Ethereum une technologie utilisable pour des utilisations B2B plutôt que pour des utilisations B2C sur l'infrastructure publique. En entretien, Jean comprenait la controverse sur le rôle de ConsenSys au sein de la communauté comme une tension entre deux approches du développement informatique : un *open source* radical prôné par les critiques, contre le pari de ConsenSys d'une compatibilité entre développements *open source* et DApps par son « *startup studio* ». Jean voyait ce pari comme celui d'un « fonds »²¹⁰, selon un modèle plus proche de celui des grands acteurs du numérique dans le financement de l'open source. Alors que les critiques du rôle de ConsenSys étaient exprimées de l'extérieur de l'entreprise, les représentants de la Fondation Ethereum les avaient eux-mêmes intégrées.

Kim, employé de la Fondation Ethereum, cherchait à répondre aux critiques sur le rôle de la Fondation Ethereum lors d'un *talk* à EthCC. Pour cela, il les relayait et tentait de montrer que la Fondation Ethereum travaillait de manière sérieuse. Toute sa présentation relevait de l'équilibre entre affirmation du soutien financier et relationnel de la Fondation Ethereum au

210 « Aujourd'hui tu as un startup studio qui a vraiment financé à pertes pendant cinq ans dans l'écosystème et qui maintenant se dit, « ok on se frotte les mains, ça a marché ! C'est trop bien ! » C'est pareil que la vie d'un fonds quoi. » (entretien Jean)

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

développement de l'écosystème et minimisation de l'ampleur de l'influence de l'organisation sur les bénéficiaires de son soutien. Par exemple, Kim indiquait que les différentes actions de la Fondation Ethereum étaient bien d'actualité en dépit de « rumeurs » annonçant leur fin. Parmi ces actions figuraient le programme de bourse (*grants*), le financement de projets s'appuyant sur Ethereum 1 (et pas seulement sur Ethereum 2, comme certaines rumeurs le laissaient également penser), et que, de manière générale, l'argent de la Fondation Ethereum était destiné à financer l'écosystème, pas à être thésaurisé. Kim expliquait que la Fondation Ethereum avait offert plus de 50 millions de dollars à plus de 200 projets entre 2018 et début 2020.

Encore, Kim rappelait que la Fondation Ethereum ne faisait pas de favoritisme et était entièrement consacrée au soutien à la communauté dans son travail de construction de biens pour l'écosystème. L'organisation se demandait « à quels défis fait face la communauté ? » plutôt que « que doit-on financer ? ». L'allocation de financements était un des différents dispositifs de « soutien » de la Fondation Ethereum au développement de l'écosystème, soutien qui pouvait être non-matériel et individualisé : conduite de projet (assistance technique, génération d'idées, élaboration d'un planning ou d'un budget), réseautage, retours de la communauté, identification de sources de financements spécifiques (par exemple gouvernementaux, de capital-risque, ou d'autres fondations comme l'*Open Technology Fund*), mise en visibilité (dans des événements comme EthCC, DevCon, ou Eth Global), ou crédits pour l'utilisation de services cloud. Kim expliquait :

*We have developers all across the globe, and they all have individual challenges. So the question is: **how do we actually use where the EF²¹¹ sits as this neutral party? And if we take as example of constellations, right, we're just one star and everyone else is their own star.** How do we make sure the gravitational pulse is continually kind of going around? And we can connect all these constellations together. Who do you need to talk to? Do you know who that person is? If not, maybe we know. And if I don't know, maybe someone else knows. **We know so many other people within the space.** So it's not just one connection, right. It's interweaving this giant web of the Ethereum community. (Kim, EthCC, 4 mars 2020)*

L'organisation était « une étoile » dans une « constellation » peuplée de développeurs aux

211 Acronyme pour Ethereum Foundation (Fondation Ethereum).

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

« défis individuels » qu'elle soutenait au cas par cas. Les soutiens, monétaires ou non, étaient attribués sur candidature *via* un unique point d'entrée : <http://ecosystem.support>. Chaque candidat au soutien de la Fondation Ethereum commençait par rencontrer un « guide ». La candidature était suivie d'un processus d'évaluation par les pairs (*peer review*) non précisé, après lequel l'équipe de l'*ecosystem support program* proposait un type de soutien parmi deux possibles. D'une part, les bourses demandaient la constitution d'une candidature complète (*full application*), qui conduisait à un entretien, puis à un nouveau processus d'évaluation par les pairs. Suite à ce processus, un entretien technique puis une dernière étape d'évaluation et de définition des objectifs était mise en œuvre avant qu'une décision finale soit finalement apportée par la Fondation Ethereum. D'autre part, les demandes d'autres types de financement, les demandes de collaborations, de présentations (*showcasing*), de conseils, de connexions ou autres ressources étaient évaluées au cas par cas.

Les demandes de soutiens monétaires étaient soumises à un processus beaucoup plus formel que les autres formes de soutiens. Pour Kim, le bon soutien n'excluait aucun candidat dans la mesure où seule comptait la recherche de « résultats désirés » :

*So, what are we looking for? This is a, I guess, most people say it's a mystery. But it's kind of weird because we try to articulate this and almost everything we do. **We like to ask ourselves, you know, what are the overarching goals that we want to accomplish, right?** And what more precisely are we trying to do here? What does the ecosystem support program actually providing here? How do we hope to accomplish this? **And what it is... what are the desired outcomes for this, right?** How do we make sure that every step of the way we're always marching towards, goal? So some of the high-level allocation categories. We've "grow usage". **They're very vague, and intentionally so. We want to make sure we are not pigeon-holing any team or project ourselves.** Five minutes. Okay so, "grow usage", "grow community", "grow developer base", "research capabilities", "improve developer output", "support resource development that makes Ethereum tomorrow a reality". Let's make sure we can actually get to that point. (Kim, EthCC, 4 mars 2020)*

Or, ces « résultats désirés » étaient volontairement laissés incertains. Kim insistait sur l'interrogation continue de la Fondation Ethereum sur ce qui devait être accompli, sur la nature des projets qu'elle devait soutenir. Ces interrogations conduisaient la Fondation

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Ethereum à formuler des objectifs « intentionnellement vagues » pour assurer que le soutien n'était pas dirigé vers des équipes ou projets spécifiques. Comme VB, Kim revenait aux jetons pour illustrer cette préoccupation : il indiquait que la Fondation Ethereum n'aiderait d'aucune manière à vendre ou à faire monter (*pump*) le prix de jetons. Cette neutralité allait jusqu'à hésiter dans la réponse à un auditeur qui faisait remarquer le manque de connaissance « *business* » des développeurs souhaitant lancer une DApp. Kim reconnaissait que les modèles d'affaires sur lesquels faire émerger le Web 3.0 restaient inconnus début 2020 :

*I think Web 3 space is extremely interesting because **we don't know what the right business model is going to be.** Yeah. if you kind of just preach out there, like “this is it! we're just gonna take fees!” you just **essentially become a rent taker again, so what's what's the point?** but you know that's not wrong, right? so profitability, sustainability, these are all hard questions that I don't think we have answered yet.*
(Kim, EthCC, 4 mars 2020)

Ainsi, le jeu d'équilibriste de Kim montre que le problème dans le rôle de la Fondation Ethereum tient à son pouvoir de décision au sein de la communauté. Kim montrait que le rôle de la Fondation Ethereum n'était pas au service de certains en particulier, que l'organisation se donnait pour ambition de connecter des réseaux d'humains ou de connaissances²¹², de faire circuler des ressources, d'allouer des ressources par un processus hautement procédural qui devait garantir le sérieux et l'objectivité du processus d'allocation.

212 C'est également le rôle que me décrivait un entrepreneur à Singapour en février 2018. Pour lui, la Fondation Ethereum était « là pour eux », développeurs de dApps. Il m'expliquait qu'il était très commode d'avoir la Fondation Ethereum « de l'autre côté de la rue », que ses représentants étaient attentifs aux « besoins » des entrepreneurs de l'écosystème.

2.3. Mécanismes : le gouvernement automatique et participatif

Le bon financement des biens publics aurait dû correspondre à un transfert d'argent entre les utilisateurs et les producteurs de ce bien. Puisque le marché ne permettait pas ce type de transfert avec les « biens publics », la communauté imaginait des « mécanismes » exécutés sur la blockchain donc valant décision (*on chain*). Les réflexions sur la conception de ces mécanismes montrent que le bon gouvernement devait être automatique pour s'appliquer sans arbitraire ni possibilité de contournement (ce qui serait « rationnel »).

Le financement idéal : automatiser origine et allocation de l'argent

L'idéal aurait été de financer les biens publics uniquement par ceux qui en profitent réellement, à la manière d'une allocation par le marché. Mais « la logique économique de la propriété privée et des marchés » était « optimisée » pour des activités qui peuvent être « décomposées » en interactions d'individu à individu, ce qui n'était pas le cas d'activités comme la « production et la consommation » de biens publics – des activités que Buterin compare à l'art et à la science (Buterin 2021). Les mécanismes de marché ne permettaient pas de résoudre le problème de financement des biens publics, car la consommation individuelle de ces derniers ne passait pas par un prix facturé au consommateur. Les biens publics n'avaient pas de modèle d'affaire, ils ne pouvaient pas être financés par le prix comme signification d'une appétence pour un bien.

La « sécurité du réseau » faisait exception : VB proposait de la voir comme un « bien public » financé directement par le protocole du réseau. Les financements (le protocole lui-même par l'émission monétaire, les utilisateurs qui paient des frais de transaction) étaient automatiquement alloués aux financés (les mineurs). En théorie au moins, le seul type d'action nécessaire pour que le bien public (la sécurité du réseau) émerge de l'action de chaque acteur (des mineurs qui minent, des utilisateurs qui paient) était que chacun exécute le code informatique en fonction de son rôle (le client pour un nœud de minage ou gestionnaire de *wallet* pour un utilisateur)²¹³. Les acteurs qui participaient au financement

²¹³ Les frais fixes dépendaient du nombre de *miners* participant à la validation des blocs, les commissions déterminent l'ordre de priorité dans la validation des transactions. Si en théorie les commissions étaient

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

de ce bien public, comme ceux qui en bénéficiaient, n'avaient pas à agir autrement qu'en fonction de leurs « intérêts » ou de leurs préférences : demander l'exécution d'une transaction pour un utilisateur, attendre un profit pour les mineurs. Pour les premiers, il était « naturel » de payer pour que leur transaction soit exécutée ; pour les seconds, il était « naturel » d'attendre un bénéfice pour leur investissement.

VB proposait d'étendre ce principe d'allocation directe à des acteurs qui n'étaient pas prévus par le protocole : les acteurs de l'écosystème qui développaient un autre type de bien public, des « librairies » utilisées par les *smart contract*. De manière générale, les DApp utilisaient des *smart contracts* qui étaient déjà déployées sur la blockchain Ethereum (« on utilise tous nos trucs ensemble », disait Jean au Chapitre 3). Ces librairies étaient des bouts de code qui permettaient de bâtir des DApps « sans avoir besoin de réinventer la roue », en utilisant du code qui avait déjà été éprouvé par d'autres développeurs (ethereum.org 2022). La proposition consistait à diriger une partie des frais de transaction payés par chaque utilisateur de DApps aux développeurs qui avaient participé au développement de ladite DApp. Pour cela, il proposait que les librairies soient plus largement rendues publiques et que les développeurs associent leurs *wallets* à ces librairies.

Toutefois, ce mécanisme posait un problème de « contournement » : le code d'une librairie ou d'un *smart contract* pouvait être republié de manière à éviter de payer des frais. Pour éviter ce phénomène, VB proposait de faire évoluer la rémunération liée à l'utilisation d'un bout de code donné en fonction du nombre d'utilisation de ce bout de code selon une fonction qui ferait dépendre la rémunération non seulement du nombre de lignes du bout de code (mesurant l'effort produit), mais aussi selon le nombre de fois où ce bout de code avait préalablement donné lieu à rémunération, de manière à ce qu'un bout de code donné rapporte d'abord peu, puis de plus en plus, jusqu'à atteindre un gain plafonné pour un grand nombre d'utilisations (Buterin 2019b)²¹⁴. Ainsi, le mécanisme intégrerait dans son fonctionnement la possibilité que des acteurs cherchent à le contourner.

fixées librement par les utilisateurs (plus on paie, plus la transaction est validée rapidement), en pratique, les logiciels servant d'interface avec Ethereum (et a fortiori les bourses d'échange) établissaient eux-mêmes cette commission.

214 Voir « scheme 2 » dans Buterin (2019a).

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

L'allocation directe entre producteurs et financeurs d'un bien public faisait reposer la qualification de « biens publics » sur les financeurs, en liant signification de la transaction (quelle librairie ou quel *smart contract* était utilisé) au producteur du bien public (la librairie ou le *smart contract*). Or, ce type de traçage n'était en pratique que rarement envisageable, car l'utilisation d'un objet vu comme bien public est elle-même rarement observable. Ainsi dans la plupart des cas, la qualité biens publics nécessitait une appréciation humaine. Par exemple, comment juger si un article de blog avait la qualité de « bien public » ? Différents mécanismes étaient envisagés, d'une part des mécanismes de collecte (trouver l'argent), d'autre part des mécanismes d'allocation (distribuer l'argent collecté).

Des mécanismes indépendants des significations des transactions

Collecter les financements des biens publics passait par des mécanismes : des procédures techniques indépendantes de transactions particulières, à la manière de taxes ou d'impôt universels. À l'inverse des dons qui relevaient de la générosité ou de l'« altruisme » dans le langage de la théorie des jeux, les mécanismes étaient vus comme des manières de collecter de l'argent sans que les « joueurs » aient la possibilité d'évaluer le gain possible qu'ils pourraient obtenir de leur propre contribution au financement des biens publics. VB imaginait trois types de mécanismes de collecte d'argent sur la scène d'EthCC.

Le premier mécanisme de collecte consistait à émettre de l'ether spécifiquement pour le financement des biens publics, comme pour la « sécurité » du réseau, c'est-à-dire l'activité de minage. L'ampleur de cette manne se mesure en comparaison avec le budget de ConsenSys ou de la Fondation, les « CCCPs » (Buterin 2021). Environ 13 500 ethers (40 millions de dollars) étaient émis quotidiennement par Ethereum. S'ajoutaient 1500 ethers (4,5 millions de dollars) de frais de transactions payés par les utilisateurs pour rémunérer directement les *miners*. La Fondation Ethereum et ConsenSys disposaient d'un budget allant de 30 à 60 millions de dollars par an, et à celui de ConsenSys, du même ordre de grandeur. Selon ces chiffres, le processus de minage fournirait et allouerait plus de 300 fois le montant de l'ensemble des financements de la Fondation Ethereum pour tous les autres

types de biens publics.

Le second mécanisme de collecte était imaginé comme une convention sociale. VB se référait à une proposition de l'écrivain promoteur de l'anarcho-capitalisme et théoricien libertarien David Friedman à propos du comportement des clients de restaurants états-unis. Ce dernier expliquait que les clients donnaient systématiquement et « volontairement » 15 à 20 % de leur addition au serveur. Or, le service à table pouvait selon lui être considéré comme un « bien public » dans la mesure où il profite non seulement à celui qui paye le pourboire mais aussi aux futurs clients du restaurant. Friedman voyait l'« obligation » que chacun ressent de manière « interne » comme un « contrat implicite » : quelle que soit la qualité du service, rares sont ceux qui osent ne pas verser de pourboire. Les pourboires seraient un exemple de financement de biens publics intermédiaire entre « méthodes économiques normales » et « association caritative » (Friedman 1973 : 132), entre l'opération caritative (verser un pourboire quel que soit le service, par principe, de manière désintéressée) et un mécanisme économique (la rémunération comme incitation, reconnaissance, pour la qualité du service proposé).

Sur ce modèle, VB imaginait des « dons aux valeurs par défaut socialement acceptées »²¹⁵ s'imposant comme taxe sur toutes les transactions qui serait introduite par les développeurs de clients (pour les *miners*) et de *wallets* (pour les utilisateurs). Pour pouvoir fonctionner, VB signalait que ce principe devrait devenir une « norme communautaire » selon laquelle chacun ne chercherait pas à éviter ces frais²¹⁶ et soutiendrait les changements de protocoles qui favoriseraient ces frais. En clair : la culture communautaire devrait célébrer et souhaiter amplifier les taxes. Elle deviendrait ainsi l'équivalent du « contrat implicite » que remarque Friedman pour le pourboire. La condition « socialement acceptée » est centrale car, en pratique, toute transaction pourrait être signée sans verser de frais en utilisant une version d'un logiciel client ou de gestion de *wallet* contrevenant à la « culture » souhaitée par VB. Ces logiciels ayant leur code ouvert, il y aurait fort à parier que des versions sans contribution « volontaire » apparaissent. Avec cette idée de « norme sociale », VB cherchait

215 Des « *donations with socially agreed defaults* ».

216 Double négation dans la présentation orale et dans la présentation de ce principe sur Twitter.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

à mécaniser ce qui relevait de relations de face-à-face.

Le troisième mécanisme était imaginé comme une taxe sur l'activité de certains *miners*, jugée immorale. Cette activité découlait de la capacité des *miners* à choisir les transactions à inclure dans un bloc en constitution. Sous l'angle de la mystique, cette capacité était essentielle : elle permettait aux *miners* de privilégier les transactions aux commissions les plus élevées, et ainsi réguler la demande de transactions par les prix sur le « marché » de l'offre et de la demande de transactions entre *miners* et utilisateurs. Mais cette capacité permettait également aux *miners* de choisir en priorité leurs propres transactions dans la constitution d'un bloc. Or, cette priorisation était particulièrement utile quand « transaction » sur la chaîne signifiait « transaction financière » dans les DApps de la « finance décentralisée ». Elle conférait aux *miners* une possibilité d'« arbitrage », au sens de la finance de marché traditionnelle : profiter de hausses ou de baisses sur un (crypto)actif en étant parmi les premiers à acheter ou à vendre. Cette activité pouvait être particulièrement lucrative lorsqu'un mouvement général de marché s'amorçait : être le premier à vendre en situation baissière permet de racheter le même actif à plus bas coût quelques blocs plus tard.

Cette source de revenu illégitime ou stratégies « malhonnêtes » appelées « valeur extraite par les *miners* » (*miner extracted value*, MEV) pouvaient être mises aux enchères pour financer les biens publics (Buterin 2019a). Le caractère « malhonnête » n'était pas attaché à une identité (qui extrait) mais à un comportement permettant de capter la MEV (comment on extrait) : réorganiser les transactions différemment d'un ordre de transactions qui était jugé « correct » ou juste. Autrement dit, il était contraire à la mystique que les *miners* organisent les transactions dans leur propre intérêt car cela contredisait la rupture épistémique entre inscription du calcul et signification du calcul : la transaction à inscrire était choisie en fonction de sa signification. Pour VB, la solution à cette injustice n'était pas de produire un ordre qui serait « correct » selon un critère fixé à l'avance, mais plutôt de réguler la priorisation de l'inscription des transactions (capacité de réorganiser le contenu d'un bloc de transaction) par un mécanisme d'enchères. Ainsi, le gagnant de l'enchère deviendrait légitime pour capter toute la « valeur extraite par les *miners* » en introduisant

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

dans un bloc donné sa propre transaction, en échange d'ethers utilisé pour financer les biens publics.

Sur la scène d'EthCC, Buterin était préoccupé par la légitimité de ces différents mécanismes. Ils étaient pensés comme des instruments qui devaient être automatiques et incontournables. Cette anxiété pour les possibilités de contournement était la conséquence du cadre de pensée général posé au départ : il serait tout à fait rationnel d'éviter de participer au financement des biens publics. Les mécanismes doivent donc prendre ces possibilités en compte. Le premier mécanisme évitait le problème de contournement ; il était idéal car il fonctionnait sans possibilité de calcul individuel en situation de jeu : le protocole de consensus était incontournable par définition, puisqu'il était la référence à toute action dans cet espace. Par ailleurs, l'émission monétaire ne prélevait pas directement d'argent aux acteurs en présence comme le faisait la taxe sur la « valeur extraite par les *miners* », bien qu'il soit posé que cette valeur n'appartenait pas aux *miners* et devait être ouverte à tout l'écosystème par le mécanisme d'enchères. Le problème du contournement se posait au contraire de manière nette avec le deuxième mécanisme qui appelait à l'instauration de normes qu'il faudrait respecter au nom de la responsabilité de chacun : l'incompatibilité entre l'intérêt individuel (contourner la taxe) et le principe d'une politique s'appliquant à toutes et à tous apparaît de manière flagrante.

L'allocation délibérée : « décider sur la chaîne » des biens publics à financer

La question de l'allocation des fonds devait répondre aux questions suivantes : à qui, par qui, comment et pourquoi devraient être alloués les fonds constitués automatiquement *via* les mécanismes de collecte d'ethers ? À la différence de la « sécurité » du réseau financée par le protocole qui faisait de la dépense de puissance de calcul un « travail » (algorithme dit de « preuve de travail », voir Chapitre 1), le travail de construction d'un « bien public » était nécessairement inventif. Rédiger de la documentation, écrire un bout de code informatique ou entreprendre des actions de promotion pour l'écosystème était un travail créatif qui nécessitait une qualification. Allouer des fonds nécessitait de prendre une

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

décision qui ne pouvait pas être elle-même automatisée : il fallait, au coup par coup, identifier quels humains produiraient quelle tâche.

Dans sa présentation à EthCC comme dans ses publications, VB s'opposait à une solution passant par des organisations, conformément à sa dénonciation des « CCCPs ». À cette époque, d'autres communautés blockchain finançaient pourtant leurs « biens publics » via des organisations qui distribuaient les *coins* collectés par émission du protocole. Cet argent était directement dirigé vers un *wallet* contrôlé par une organisation similaire à la Fondation Ethereum. ZCash, un *coin* dont le protocole est codé à partir de Bitcoin mais permettant de formuler des transactions anonymes (sans divulgation de la « clé publique »), prévoyait par exemple un « fonds pour développeurs » crédité de 20 % des rémunérations des récompenses émises à chaque bloc. Ce « fonds » était divisé en différentes organisations. La Zcash Open Major Grants recevait 8 % de la récompense émise à chaque bloc, qu'elle distribuait en bourses à des développeurs. L'Electric Coin Corporation recevait 7 %, qu'elle distribuait à des projets de recherche et de développement, d'ingénierie, de « relations réglementaires » ou lobbying et plus généralement d'actions en faveur de la promotion de Zcash. Enfin, la Zcash Foundation recevait les 5 % restants et disait mettre ces fonds au service des utilisateurs de ZCash pour bâtir une infrastructure financière respectueuse de la vie privée.

La seule solution conforme à l'absence d'organisations décisionnaires passait par une décision collective « sur la chaîne », c'est-à-dire par l'intermédiaire d'une DAO. Le principe était le même que l'organisation de DigixDAO ou que celui de TheDAO dans son fonctionnement « normal » (Tableau 15, Ligne 1), à la différence près que le groupe des décideurs serait l'ensemble des détenteurs d'ethers (plutôt qu'un jeton *ad hoc*) représentant l'ensemble des parties prenantes de l'écosystème.

Cette DAO aurait en charge le travail de qualification des biens publics en allouant les ethers à des constructeurs, en fonction des votes de l'ensemble des détenteurs d'ethers, de manière à ce que chacun dans l'écosystème participe à la décision d'allocation. Le groupe était le même que celui qui était constitué avec CarbonVote (Tableau 15, Ligne 3) ; mais

alors que cette initiative était une délibération (visant à donner une image collective de la volonté de l'écosystème), la DAO prendrait ici une décision d'allocation. Ainsi, l'ether prenait une nouvelle fonction : un droit de vote sur le financement des biens publics. Ce type de mécanisme correspondait à ce que VB appelait une « gouvernance décentralisée » (Buterin 2021). Dans ce mécanisme, les membres de l'écosystème s'exprimeraient en fonction de la taille de leurs portefeuilles en ethers. Les décisions d'allocation de financement ne répondraient pas au principe « une personne = une voix », mais au principe « un ether = une voix ».

2.4. La mystique du protocole appliquée à la décision collective

La mystique du protocole, principe de la décision collective des *miners*, guidait la réflexion concernant les mécanismes de prises de décisions collectives entre porteurs d'ethers ou de jetons. La bonne décision était définie comme l'agrégation d'actions individuelles : chacun votant indépendamment de ses propres intérêts, comme les *miners* qui inscrivaient les blocs sans connaître la signification des transactions. Décider collectivement signifiait « qualifier » l'objet de la décision ; notamment, le vote était imaginé comme expression individuelle participant à définir ce qu'est un « bien public », comme les *miners* définissent quelle est la chaîne vraie ou factuelle en ajoutant les blocs de transactions.

Par conséquent, la bonne décision collective reposait sur une participation large, active et « authentique » au sens de séparation des intérêts personnels du point de vue sur l'objet de la décision. À la différence de biens communs pour lesquels les règles sont inventées entre individus en contact, la qualification des biens publics est ici le résultat de votants isolés dont les alliances sont vues comme corruptrices de la « bonne » définition de ces « biens ». Pour maintenir cette hypothèse de départ et produire la décision collective par des mécanismes, les auteurs imaginaient de limiter les objets de décision en donnant au vote la signification de « prédiction », ou d'instituer un mécanisme de gestion des identités des individus.

Qualification des « biens publics » par le vote

Le vote par ethers ou par jeton était la forme de décision collective naturelle ; « sur la chaîne » selon la grammaire proposée plus haut, comme toute décision. Le vote était la seule solution au problème d'allocation de financements aux biens publics, *via* une DAO (sous-section précédente). Le vote par *ether* ou par jetons était également expérimenté dans d'autres cas visant à favoriser la production de « biens publics ». Par exemple, le « fil » /r/ethtrader²¹⁷ du forum Reddit a expérimenté un mécanisme d'incitation des utilisateurs à écrire des commentaires par un jeton appelé « donut » : les utilisateurs recevaient une proportion des donuts émis chaque semaine en proportion des « *upvotes* » que leurs posts avaient reçus. Ces donuts servaient ensuite de droits individuels pour décider du contenu de la bannière publicitaire en haut de la page web ou pour voter dans des sondages de la communauté (Basoosh 2020).

Ces mécanismes devaient définir les « biens publics » en articulant au cas par cas recherche d'une récompense pour les producteurs à l'agrégation de votes de l'ensemble d'un groupe donné. Les utilisateurs de Reddit qui « *upvote* » un post participaient à définir la qualité du commentaire en question tout en récompensant son auteur. Les jetons que ce dernier recevait lui permettait de se distinguer sur le forum : voter lui-même avec plus de poids pour des commentaires postés par des membres de la communauté, donner des « pourboires » aux autres utilisateurs, publier des GIF²¹⁸ dans les commentaires, afficher son nom avec des couleurs spéciales, acheter des badges et même acheter le contenu de la bannière en haut de la page du forum (qui pouvait être utilisée à des fins publicitaires). Dans le cas de la DAO envisagée pour allouer des financements collectifs, le vote devait permettre de qualifier les projets correspondant aux grandes priorités de l'ensemble de l'écosystème, et à inciter les candidats à répondre aux préoccupations de l'écosystème.

Or, les hypothèses de conception de ces mécanismes rendaient cette articulation soit impossible, sinon limitée à des cas très particuliers. L'inquiétude des auteurs portait sur

217 Le fil était accessible à l'adresse : <http://reddit.com/ethtrader>. Comme indiqué à la section précédente, ce fil avait été créé pour concentrer les discussions portant sur les prix des actifs.

218 Acronyme de « *Graphics Interchange Format* » : format d'image couramment utilisé sur le Web.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

l' « authenticité » des votes par ethers ou par jetons, à la lumière de deux ensembles de théories qui guidaient la conception de ces mécanismes. D'une part, les auteurs reprenaient les hypothèses de la théorie du choix social pour poser le problème de l'action collective : des individus ayant des opinions ou des préférences fixées devaient être exprimées par un vote (transaction en ethers ou en jetons) et combinées pour exprimer une décision collective (*via un smart contract*). D'autre part, ils voyaient chaque porteur d'ethers ou de jetons comme un « joueur » au sens de la théorie des jeux ; autrement dit, ils assimilaient les opinions ou les préférences des individus à l'évaluation individuelle des bénéfices tirés individuellement du vote.

À quoi bon voter pour un « bien public » ?

Ainsi, chaque votant était supposé agir selon ses propres intérêts tout en exprimant ses préférences individuelles vis-à-vis d'un problème collectif, à l'échelle de l'ensemble de l'écosystème ou d'un forum comme Reddit.

Or, pour les auteurs, il était *a priori* impossible de s'assurer en avance que chacun voterait « authentiquement » en faveur de ce qui devait relever d'un « bien public » plutôt que pour d'autres raisons ; l'option offrant le meilleur bénéfice individuel serait systématiquement préférée par les « joueurs » en situation de voter. Ce constat découlait de l'hypothèse qui présidait à l'élaboration de ces mécanismes, que VB théorisait comme « alignement » des intérêts pour « résoudre » la « tragédie des communs » (Buterin 2019b, 2021). Cette notion est une référence directe au concept développé par Garrett Hardin pour décrire les dommages que des actions individuelles peuvent infliger à l'environnement (Hardin 1968). Il décrit des situations dans lesquelles des individus ayant un accès libre à une ressource sans être gênés par des structures sociales partagées ou des règles formelles qui régissent l'accès et l'utilisation agissent indépendamment et selon leur propre intérêt. Chaque action individuelle contribue rationnellement donc inéluctablement à l'épuisement de la ressource par l'action non coordonnée. L'exemple typique de ce type de situation est l'exploitation d'une ressource naturelle, comme les poissons d'un lac amenés à être pêchés.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Elinor Ostrom a obtenu le prix Nobel d'économie en 2009 pour ses travaux sur les communs. Pour elle, la « tragédie des communs » est une fiction (Ostrom 1990). À partir de nombreuses études de cas, elle montre que les membres d'une communauté d'utilisatrices d'une ressource développent des règles pour préserver l'accès à la ressource commune dont elle propose une catégorisation. Ce sont précisément de telles règles qui sont exclues par hypothèse par VB et ses coauteurs. Le concept même de « biens publics » ne prévoit pas, à la différence du concept de « biens communs », l'émergence de règles communes définies au sein d'une communauté ayant pour objectif commun de préserver une ressource commune. Au contraire, VB pose l'élaboration de règles comme un problème préalable qui doit être résolu *a priori* par les mécanismes, eux-mêmes chargés de définir ce qu'est un « bien public ». Alors que la régulation des communs est le résultat d'une intelligence collective à partir du contact direct entre personnes et avec un « commun », l'identification et le financement des « biens publics » est imaginé comme résultat d'actions coordonnées par un mécanisme qui agrègent la maximisation des bénéfices individuels.

L'impossibilité d'éviter les « attaques » par « collusion »

Toute coordination externe aux mécanismes de vote eux-mêmes mettrait en péril l'authenticité de la décision collective, pour ces auteurs. « Collusions » et « attaques » sont des concepts vernaculaires centraux. Ils indiquent par la négative la charge morale associée à la situation d'isolement des votants, selon laquelle chacun doit agir indépendamment de ses pairs : toute forme d'alliance est vue comme une collusion attaquant l'ensemble du groupe, mettant en péril le bon déroulement de la décision collective (typiquement, de la désignation du « bien public ») qui repose sur une expression individuelle, pure, sans interférence avec le reste du groupe. Par ce prisme : les mécanismes de vote présentent une faiblesse : ils ne permettent pas de garantir que les membres d'un groupe ne puissent pas communiquer et s'influencer dans leur vote. Ce type de coordination est vu comme un détournement du mécanisme au profit d'un sous-groupe.

Exprimé dans les termes de la théorie des jeux, ceux qui associent leurs ethers ou jetons changent la nature du jeu cadré par le mécanisme en mettant leurs jetons en commun. Pour

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

les auteurs, ces collusions prenaient typiquement la forme de « pots-de-vin » (*bribe*). Le pot-de-vin est une attaque qui consistait, de manière générale, à offrir à un individu (supposé intéressé avant tout par son propre bénéfice) plus que ce qu'il perdra en conséquence de l' « attaque » (qui affecte la chose commune, donc les intérêts de l'individu qui a reçu le pot-de-vin également). Selon ce raisonnement détaillé par les auteurs, les votes, comme les conséquences des votes, sont évalués en termes monétaires (gains ou pertes), conformément à la théorie des jeux.

Les pots-de-vin pouvaient être « explicites », en raison du caractère transférable de l'ether ou des jetons qui pouvaient être achetés ou prêtés spécifiquement pour influencer un vote. Ce type de pratique peut être rapproché des pratiques d' « arbitrage de dividende » qui ont fait scandale au début de 2023 (affaire des *CumEx Files*). Un *smart contract* pouvait en effet être programmé comme un contrat de prêt de cryptoactifs : par exemple, un utilisateur pouvait en théorie recevoir un cryptoactif en prêt pour voter, en échange d'une rémunération et en gageant un cryptoactif (ethers, bitcoins, ou tout jeton émis sur Ethereum) via un *smart contract*, servant de collateral à son prêteur (au cas où l'emprunteur ne rende pas l'actif prêté). Typiquement, différentes DApps associées à la « finance décentralisée » permettaient ce type de transactions. La plus populaire était Compound. Ce type de prêt temporaire d'actifs était codé suivant un principe similaire aux instruments financiers appelés « accord de rachat » (« *sale and repurchase agreement* » ou « *repo* » en anglais).

Les collusions comme « pots-de-vin » pouvaient également être « implicites ». Les auteurs voient par exemple les *exchanges* (comme Binance ou Coinbase, voir Chapitre 2) comme des corrupteurs en puissance. En effet, puisque les *exchanges* conservent les ethers et les jetons de leurs utilisateurs (en « *custody* »), ils peuvent les utiliser pour voter à leur place. Mes utilisateurs n'ont en effet pas libre accès à leurs cryptoactifs : ils doivent demander à l'*échange* d'effectuer les transactions pour eux. Ainsi, le pot-de-vin peut être implicite en incitant les utilisateurs à laisser leurs ethers ou leurs jetons sur la plateforme. Ce type de phénomène préoccupait les organisateurs de votes dans des cas pratiques. Par exemple, l'équipe qui avait codé CarbonVote avait instauré une « liste noire » de certains *wallets*

connus comme teneurs de comptes pour tiers, parmi lesquels différents *exchanges*.

La nature « ploutocratique » du vote

Plus un individu détient un grand nombre de jetons, plus il est susceptible d'être impliqué dans le vote et de chercher à distribuer des « pots-de-vin » pour imposer son point de vue : cette nature « ploutocratique » des votes par ethers ou jetons était vue comme un second type d'« attaque ». Sans employer ce terme, les critiques de CarbonVote avançaient ce type d'argument à différents niveaux (phyro 2018) : ceux qui avaient investi dans TheDAO au départ et qui espéraient récupérer leurs ethers étaient plus « incités » à voter que les autres, et un seul *wallet* détenait près d'un quart des jetons.

Ce phénomène était vu comme conséquence du processus de vote lui-même : une personne ou une organisation disposant d'un nombre important de jetons (généralement appelés « *whales* ») était non seulement en capacité d'influencer significativement la décision collective, mais en plus significativement incitée à le faire. En conséquence, celles qui possèdent moins d'ethers ou de jetons étaient moins incitées à participer au vote, conscientes que leur vote n'aurait qu'une faible influence sur la décision finale. Ainsi, les premières étaient directement incitées à chercher à modifier les « jeux » en leur faveur, « faussant » la décision collective.

En effet, en « votant pour eux-mêmes » (*self-voting*), les individus les plus dotés détournent les mécanismes : le vote ne visait plus une décision collective authentique, mais le bénéfice individuel d'un acteur ou d'une collusion d'acteurs. VB rapprochait cette stratégie de celles de *miners* qui, dans l'application du protocole, avaient un comportement dit « égoïste » (*selfish miners*) permis par leur position dominante dans le réseau. Ce phénomène était également décrit comme « attaque » dans la littérature (Eyal & Sirer 2013) : alors que le protocole indique de diffuser un bloc dès qu'il a été trouvé, ce comportement consistait à ne pas diffuser immédiatement un bloc en misant sur l'avance statistique conférée par la taille de la ferme, pour différer la diffusion du bloc afin de commencer à miner le bloc suivant avant les autres.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Les attaques étaient vues comme consubstantielles aux mécanismes en conséquence de la nature potentiellement « coopérative » des votes, qui devait pourtant être évitée pour que le vote exprime l'agrégation de préférences purement individuelles. Bien entendu, il n'était pas question d'imaginer une quelconque loi ou norme pour éviter ce problème, comme les lois anti-cartels ou anti-corruption, en principe incompatibles avec l'absence d'institutions, et en pratique impossible à faire respecter.

Le vote comme prédiction, ou la création d'identités ad hoc

Lors de l'écriture de ces lignes, les débats théoriques et expérimentations concernant les bonnes manières de définir et de financer les « biens publics », et plus généralement de décider collectivement, continuaient d'être proposées. Deux approches étaient envisagées pour instituer ces mécanismes de décisions collectives par la coordination de préférences antagonistes tenant compte des problèmes indiqués ci-dessus.

Premièrement, les auteurs proposaient de lier la valorisation du jeton servant au vote au résultat de la décision. Ainsi, le problème des collusions serait évité puisque chacun verrait un bénéfice monétaire dans l'amélioration de la valeur de ses propres jetons ou en gagnerait de nouveaux ; les pots-de-vin ne seraient plus compétitifs. Ce type de mécanisme prolonge l'anthropologie moutonnaire indiquée plus haut : pour améliorer la valeur de leurs jetons, les votants auraient individuellement intérêt à voter en faveur de la décision qu'ils imaginent que l'ensemble du groupe prendra.

Dans ces cas-là, incitation signifie « prédiction » : le vote est un pari sur la décision collective qui sera choisie. À l'issue du vote, le votant obtient une récompense ou une pénalité en fonction de la proximité de son vote avec la décision collective. Par exemple, VB imagine un mécanisme permettant de juger de la qualité de posts de blogs. Cette qualité pourrait être arbitrée par un panel d'experts à partir du vote de chaque joueur chargé de deviner la décision finale du panel ; en cas de vote correct, le votant recevrait une récompense en jetons, et dans le cas contraire, serait pénalisé. Le mécanisme participerait non seulement à former la décision collective et à inciter chacun à participer. Ainsi, la

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

prédiction (dont l'enjeu est individuel) résoudrait la tension entre intérêt individuel et collectif, en recentrant l'individu sur son propre bénéfice plutôt que sur l'incertitude liée à la distribution d'argent à une personne tierce, qui ne présente pas d'intérêt immédiat du point de vue d'un « joueur ».

Faire des votes des paris était plus généralement le fondement du principe de « futarchie », un mode de gouvernement dans lequel les politiques (ici, les mécanismes de décisions collectives) sont des marchés prédictifs (ici, en jetons). VB mobilise ce concept en référence à l'économiste américain Robin Hanson. Ce type de vote était envisagé dans différents cas. Premièrement, ils pourraient qualifier une décision collective à l'échelle d'un projet de DApp organisé en DAO. Les votants s'engageraient à l'avance à acheter un nombre de jetons à un prix fixé, typiquement inférieur au prix de marché si la décision collective est l'option pour laquelle ils ont voté ; dans le cas contraire, ils seraient contraints d'acheter les jetons de leurs « opposants ». Deuxièmement, ce même type de mécanisme pourrait être utilisé pour qualifier, à l'échelle d'un projet de DApp, les productions (déjà réalisées) de « bien public », de manière « rétroactive ». Le vote passerait par l'achat de « jetons de projet », les ethers collectés étant alloués aux auteurs des productions. On parle alors de « financement rétroactif » (*retroactive funding*).

Deuxièmement, plutôt que de les fonder sur la détention d'ethers ou de jetons, ces votes pourraient être liés à une « identité ». Toutefois, l'identité, au sens de compte sur un site Web, posait un problème de « collusion » : une identité numérique pouvait être vendue ou achetée. VB faisait à ce titre notamment référence aux techniques d'influences, par exemple sur les réseaux sociaux, mobilisant des armées de mercenaires louant leurs centaines de faux profils pour des causes variées. Le fonctionnement de Gitcoin, mécanisme de financement d'initiatives communautaires, utilisait par exemple le mécanisme d'identité du forum Reddit, ce qui était vu comme une importante fragilité.

Ainsi, la stratégie consistait à imaginer des mécanismes d'identité qui rendraient le plus compliqué possible la location ou la vente d'identités. Ces systèmes devaient prévoir un système de révocation : de cette manière, même en cas de menace, chacun pouvait céder

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

son compte puis le réinitialiser unilatéralement. Certaines initiatives comme la startup française Argent (application mobile permettant de gérer ses cryptoactifs) intégraient un système d'identité avec révocation et ré-identification par des pairs sélectionnés en avance : lors de la demande création d'une nouvelle identité, des pairs (eux-mêmes identifiés par l'application en question et en nombre fixé à l'avance) témoignaient de la correspondance entre le demandeur physique et l'identité en question. VB indiquait que cette identification ou cette ré-identification devait être faite « en personne » pour éviter les problèmes d'achat et de vente d'identité, et voyait les meetups et les conférences comme de bons candidats.

Conclusion du chapitre. L'infrastructure, processus constitutionnel

Ce chapitre propose de ne pas réduire la « constitution » (Berg et al. 2018, 2020) de l'autonomie des blockchains au protocole. L'autonomie de ces infrastructures est le résultat d'efforts qui concourent à maintenir en pratique ce que la mystique du protocole prescrit. L'autonomie de ces infrastructures tient tant que les *miners* inscrivent en méconnaissance de cause ; maintenir l'autonomie consiste à prolonger la rupture épistémique pointée au Chapitre 1, ce qui se traduit par exemple avec le problème des fermes de minage ou la multiplication d'équipes de développement des logiciels « clients ». Mais l'infrastructure est également problématisée au prisme des usages : les controverses sur la taille des blocs montrent une tension entre développement au prisme de la mystique et des usages de l'écosystème. Cette tension se lit également dans le développement de la communauté elle-même, tiraillée entre une identité « pour la *tech* » et un rapport délicat à l'explosion du prix des cryptoactifs.

La bifurcation consécutive à la controverse TheDAO était un « coup d'infrastructure », par analogie avec l'analyse de Michel Foucault du « coup d'État » (Foucault 2004a) : d'ordinaire, la raison d'État respecte les lois ; avec le coup d'État, elle ne s'incline plus devant les lois instituées, morales, naturelles ou divines. De manière analogue, le « coup d'infrastructure » ne s'embarrasse plus de la mystique qu'il piétinait en faisant des significations des transactions un motif d'intervention sur l'infrastructure. Comme pour le coup d'État, ce coup d'infrastructure était justifié par sa « nécessité » au nom du salut de l'infrastructure elle-même qui perdrait sa raison d'être en cas d'évanouissement de l'écosystème naissant. Comme pour le coup d'État, il était également violent, au moins pour l'individu qui avait réalisé une « prouesse » selon les « lois » en vigueur (« *Code is Law* »), sacrifié sur l'autel de l'action nécessaire. Enfin, comme le coup d'État, ce coup d'infrastructure était théâtral, sa nécessité immédiatement reconnue par exemple par les *exchanges* qui ont bloqué les transferts incriminés et par les *miners* qui ont très majoritairement mis à jour leurs logiciels clients.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

Cet événement a été un « moment constitutionnel » pour la communauté. Il a clarifié l'ambition d'origine d'Ethereum, bâtir une plateforme de *smart contracts*, en une fonction infrastructurelle. « *World Computer* » allait avec une conception de l'ether comme du « fuel », « pas de l'argent », ouvrant à des possibilités d'interventions au-delà de la mystique. Plutôt que par la définition de règles et leurs inscriptions dans une interface comme l'ont fait les wikipédiens (Cardon 2015), cette constitutionnalisation est passée par une scission infrastructurelle. Elle affirmait une culture politique dans une communauté de communautés pensée pour être « décentralisée » entre de nombreuses géographies, projets de développement informatique ou affinités langagières. Par exemple, les acteurs regroupés autour de DigixDAO (cas mobilisé au Chapitre 2, section 1) ont publiquement légitimé la bifurcation en affirmant que les jetons DGD reconnus par Digix seraient ceux de la chaîne Ethereum, pas ceux d'Ethereum Classic (Digix Writer 2016b).

Les réflexions et expérimentations de « financement des biens publics » étendaient les possibilités de gouvernement de la communauté. Cette rationalité infrastructurelle issue de la ligne « *World Computer* » avait la mystique comme principe régulateur, comme celle issue de « *Code is Law* ». Mais à la différence de cette dernière, elle s'intéressait aux intérêts des *wallets* de l'écosystème, pas uniquement aux formes matérielles de l'infrastructure. En effet, une nouvelle rupture épistémique devait être imaginée pour que les individus ne parviennent pas à contourner les décisions prises au nom de l'intérêt de tous (financer les biens publics). Cette rupture devait nécessairement passer par des mécanismes pour ne pas être arbitraire, comme l'était nécessairement au moins un peu les organisations formelles comme la Fondation Ethereum. Mais si l'automatisation évitait ces problèmes, elle ne pouvait pas empêcher que les *wallets* se coalisent. Or, ce comportement était inacceptable, car il aurait « faussé » le « jeu », le détournant de l'intérêt collectif qui, par hypothèse, ne pouvait pas résulter d'alliances. Autrement dit, les coalitions contredisaient le principe de la mystique appliqué à l'ensemble des *wallets* qui ne devaient agir qu'isolément, en voyant l'intérêt général par le seul prisme de leur intérêt individuel. Il s'agit très précisément de la situation créée dans les laboratoires de micro-économie :

Le jeu de bien public est l'un des jeux standards les plus utilisés en laboratoire.

Chapitre 4. Autonomie gouvernée : rationalités de l'action communautaire

*En voici la configuration habituelle. De douze à vingt participants, convoqués par tirage au sort dans une base de données de volontaires, sont réunis dans un laboratoire expérimental. **Chacun est affecté aléatoirement à un ordinateur séparé des postes voisins par une cloison garantissant une prise de décision confidentielle et anonyme.** (Villevall 2010)*

Cette rationalité gouvernementale pose les hypothèses de la micro-économie à l'origine d'un problème politique, et tente de faire appliquer ces hypothèses par des mécanismes. Cette équation est insoluble, car elle met en lumière, à supposer que l'identité est quantifiable (un ether = une voix), l'incompatibilité entre mise en œuvre de politiques publiques par le calcul autonome et respect de principes démocratiques que les acteurs cherchaient malgré tout à instaurer. Ce problème n'est pas nouveau (Rouvroy 2011). Il apparaît ici dans la forme d'un calcul auquel de nombreux acteurs, concepteurs et promoteurs mais aussi analystes, confèrent un critère de vérité en raison de l'autonomie de son infrastructure.

Conclusion générale

Les quatre chapitres de cette thèse analysent la blockchain comme une technologie de gouvernance, au sens donné en Introduction générale, à partir d'une enquête du processus de conception d'Ethereum entre 2018 et 2020.

Pour conclure, je commence par caractériser l'imaginaire de l'autonomie projeté dans le processus de conception. Il s'agit de ce que j'ai appelé un imaginaire « statique » en Introduction générale : il désigne un monde à faire advenir, ce qui doit être. L'adjectif « décentralisé », désignant un état plutôt qu'une action, résume la vision d'un « monde sans centres ». Cet imaginaire est traduit en pratique par la quête de ce que je propose de comprendre comme une « souveraineté scripturale ».

Puis, je synthétise les principaux résultats des chapitres. Le trait principal de cette technologie de gouvernance est de « décentraliser ». L'usage du verbe souligne le caractère actif de l'imaginaire d'un « monde sans centres » et la permanence des efforts nécessaires à maintenir un état temporairement « décentralisé ». Cette technologie institue « ce qui doit être » en donnant aux relations numériques la forme particulière de transactions. J'appelle son effet « gouvernance par les transactions », et propose de comprendre l'autonomie qui est prêtée aux espaces dans lesquels elle s'exerce comme le résultat d'un processus impliquant de nombreux protagonistes, dont ceux au cœur de mon enquête.

Enfin, je propose quelques pistes d'enquête et analytiques pour prolonger l'analyse des blockchains comme technologies de gouvernance.

1. Décentralisé : imaginaire de l'autonomie

1.1. Imaginaire d'un monde sans centres

Un mot d'ordre traverse le processus de conception objet de cette thèse : faire advenir des relations émancipées de toute norme extérieure entre entités souveraines. Les relations

Conclusion générale

concernées étaient monétaires, assurantielles, commerciales, financières, contractuelles, entrepreneuriales, associatives, délibératives. Les concepteurs problématisaient la manière de reconnaître ces relations à l'échelle d'un groupe comme d'une société : cette reconnaissance impliquait toujours des entités « intermédiaires », susceptibles d'intervenir en imposant leur norme, par définition incompatibles à la souveraineté individuelle. Aussi bien la loi des États que les pratiques des institutions financières publiques ou privées comme des fournisseurs de services du Web étaient des normes inacceptables.

Cette problématisation des relations en société était ancrée dans la conception de dispositifs informatiques. Elle procédait d'un double déplacement (Latour 1992). Les processus de reconnaissance institutionnelle des relations étaient assimilés à des réseaux informationnels, eux-mêmes vus comme des réseaux informatiques défaillants. Les systèmes des concepteurs étaient au contraire construits pour être autonomes et « anti-fragiles ». Ces qualités découlaient d'une séparation architecturale entre la formation matérielle des relations comme inscriptions et leurs significations, énoncées par les entités mises en relation.

Pas de centre : tel était le principe de ce qui devait être. L'infrastructure ne devait pas avoir de centres physiques, synonymes de défaillance technique ou de contrôle par des entités susceptibles de changer la signification des relations. Son caractère « décentralisé » lui conférait son autonomie, ainsi que celle des espaces transactionnels (Introduction générale). Ces espaces accueillait des relations d'échange et d'association comme transactions, typiquement *via* les « applications décentralisées » (DApps) ou les « organisations autonomes décentralisées » (DAO). Cette autonomie signifiait insensibilité de ces relations aux centres du monde qui donnent habituellement leurs significations aux relations, qu'ils soient administratifs, économiques, financiers, ou juridiques.

Ces espaces étaient pensés comme des hétérotopies (Foucault 2004c), des « contre-emplacements » pour relations numériques. Les transactions devaient y avoir leurs expériences sans intervention directe des centres, les entités mises en relation qui restaient à

Conclusion générale

la frontière. Deux cas illustrent cette séparation. Fizzy (Chapitre 1) : un retard d'avion était traduit en transaction dans l'espace transactionnel, laquelle provoquait une ou plusieurs transactions (mise à jour de contrats d'assurance), lesquelles étaient vues à la frontière comme un signal de remboursement de billets par une société d'assurance et par ses assurés ; Digix (Chapitre 2) : les décisions en jetons de gouvernance étaient des transactions qui en provoquaient d'autres en jetons utilitaires, qui elles-mêmes avaient une incidence sur une entreprise prestataire gérant de l'or physique, hors de l'espace.

1.2. La quête d'une souveraineté scripturale

Cet imaginaire d'un monde sans centres est traduit en pratique dans la quête d'une souveraineté scripturale des relations : donner aux relations formées numériquement une qualité souveraine, c'est-à-dire sans possibilité d'altération par qui que ce soit dans ou en dehors de leurs espaces d'inscription. Cette quête s'appuie sur la vision d'un monde constitué d'entités contractantes sans autres relations entre elles que celles qui sont formulées par ces dispositifs. Elle tente de substituer l'inscription à toute forme d'extériorité nécessaire à la contractualisation (Tadjeddine 2021 : 10).

La gouvernance par les nombres d'Alain Supiot (2013, 2015) permet, par contraste, de préciser l'imaginaire de gouvernance dans la conception des blockchains que j'appelle gouvernance par les transactions.

Premièrement, dans la gouvernance par les nombres, le calcul est imaginé comme le fondement généralisé de la légitimité de toute norme et du droit en particulier, au niveau de l'entreprise, de l'État, de communautés ou dans les relations internationales. Avec les blockchains, le calcul est une opération collective visant à reconnaître collectivement (comme inscription) des actions individuelles. Les blockchains instaurent des espaces protégeant les relations de toute hétéronomie, autonomes si leur « propre norme » est imaginée dans un sens minimal : le protocole comme manière d'exécuter le calcul collectivement. Toutefois, j'ai voulu montrer que cette autonomie ne tenait pas uniquement à la mystique du protocole (Chapitre 1). Au contraire, cette autonomie est instituée ; la

Conclusion générale

section 2.2 de cette Conclusion résume ces résultats. Concernant le droit spécifiquement, les éléments présentés et analysés au Chapitre 2 suggèrent qu'Ethereum était vu comme un dispositif institutionnel aux yeux d'autorités publiques (à propos de la signification d'un instrument financier).

Deuxièmement, les objets de la gouvernance par les transactions sont des relations d'échange et d'association qui doivent être programmées selon un format donné à l'avance. À la différence de la gouvernance par les nombres, elle ne s'applique pas sur chacun dans toutes les dimensions de l'existence. Sur la période d'enquête, les relations gouvernées par les transactions étaient celles des concepteurs, de technophiles, d'investisseurs ou des spéculateurs en cryptoactifs pour l'infrastructure publique, ou alors de grandes sociétés en consortia.

Pour qu'un contrat survienne, il faut au minimum que ces deux contractants, primus et secundus, soient liés par une règle hétéronome. Cette règle qui s'impose également à eux et dont ils ne peuvent disposer, c'est la force de la parole donnée. Pour qu'il y ait un contrat possible, il faut que chacun de ceux qui s'engagent croient à la force de sa parole et à une force qui s'impose à lui. Autrement dit, il n'est pas de contrat sans loi. Cela ne nous dit rien de la nature de cette loi, qui peut aussi bien procéder de la religion, que de la coutume ou d'un code civil ; mais qui dans tous les cas, mets en scène la figure d'un garant de la parole donnée, qu'il s'agisse des dieux, de la communauté, ou de l'État. Et garant qui ne se situe pas sur le même plan que les individus qui contractent. (Supiot 2013)

Troisièmement, l'imaginaire de l'ordinateur inspiré de la cybernétique joue au niveau de l'individu dans la gouvernance par les nombres : l'individu serait assujéti à des objectifs chiffrés, quantifiés, déclinant ceux de l'organisation collective à son niveau. L'indicateur est l'objectif au sens de but et au sens de critère de jugement porté sur le réel. Avec les blockchains, l'imaginaire de l'ordinateur joue (Chapitre 1, Chapitre 4) à un niveau collectif : l'ordinateur est appliqué à la parole donnée, à la reconnaissance collective de relations individuelles. Le nombre résultant d'un calcul a ainsi une réalité confinée dans un espace *ad hoc* mais visible par quiconque en temps réel sur l'écran de n'importe quel ordinateur connecté à Internet. Voir les *smart contracts* comme des « contrats », comme le propose certains juristes, revient à accorder à cet ordinateur la « parole donnée » nécessaire

dans la formation des contrats.

2. Décentraliser : institution d'une gouvernance par les transactions

2.1. Gouvernance par les transactions : quelques traits

La gouvernance par les transactions se distingue d'autres formes de gouvernance par l'infrastructure par son objet : elle vise les relations d'échange et d'association. Les relations gouvernées par les transactions varient en fonction des dispositifs : monétaires avec Bitcoin, elles prennent des significations programmables avec Ethereum. Mais ces dispositifs partagent un trait commun : ils instaurent une rupture épistémique entre entités qui reconnaissent une relation (qui calculent et qui inscrivent une transaction) et entités mises en relation. Il s'agit de la « technologie de pouvoir » (Foucault 2004a) de la gouvernance par les transactions : calculer sans connaître, ce que j'ai appelé la « mystique du protocole » héritée de Bitcoin (Chapitre 1). À condition que la compétition qu'il instaure soit réelle, le protocole neutralise les possibilités d'intervention sur les transactions. Ainsi, cette gouvernance par les transactions s'affranchit d'un rapport entre gouvernants et gouvernés : les relations sont gouvernées par une infrastructure, elle-même garantie par un mécanisme instaurant une compétition en puissance de calcul.

La gouvernance par les transactions est une proposition de gouvernement alternative de l'économie et de la finance numériques. L'infrastructure publique d'Ethereum était imaginée comme espace ouvert de formulation d'un large spectre de relations numériques. Elles prenaient des significations cadrées par leurs concepteurs en fonction des types de jetons, sans que ces cadrages les épuisent (Chapitre 2). En effet, dans leur prolifération, les jetons utilitaires étaient objets de multiples processus de valorisation intriqués. Les jetons utilitaires pouvaient signifier bons d'utilisation d'un service, mais aussi dispositifs

Conclusion générale

d'investissement. Les *smart contracts* étaient un langage de formulation de relations entrepreneuriales, aussi bien utilisés pour définir les relations économiques qu'ils imaginaient (les services eux-mêmes) autant que leurs propres relations dans le processus de conception : levées de fonds en bitcoins ou en ethers, dispositifs d'administration du développement de leur service (par exemple, DigixDAO).

La gouvernance par les transactions s'institue par des plateformes. Ethereum est devenue une « technologie de plateformes », à la suite d'un processus de technologisation de l'infrastructure publique enrôlant des grandes entreprises (Chapitre 3). Ethereum devenait utilisé comme infrastructure de plateformes ayant différents modèles économiques. Les plateformes de type B2C sur l'infrastructure publique avec les jetons projetaient une organisation économique directe entre fournisseurs et producteurs de services ; le modèle de services d'un émergent « Web 3.0 » et d'une « finance décentralisée » autant que les instruments de financement et d'organisation permettant de les faire advenir (Chapitre 2). Selon ce modèle, les concepteurs formulaient les relations pour des utilisateurs tiers. Au contraire dans les utilisations B2B, les concepteurs formulaient les relations pour eux-mêmes, reproduisant des logiques de contrôle sur les relations. L'enjeu n'était pas là de faire reconnaître les relations à l'échelle du Web entier par un réseau tiers inscripteur, mais par des partenaires commerciaux pour mieux contrôler les relations qui les liaient.

La gouvernance par les transactions s'exerce par l'ingénierie de deux opérations : la formation conduisant à inscrire les transactions, et la formulation consistant à définir des significations des transactions (Chapitre 3) qui sont multiples et émergentes avec les jetons, plus situées et spécifiques à l'activité même des concepteurs de plateforme dans le cas des consortia. La formation des transactions définissait un espace transactionnel particulier, séparé des autres par l'infrastructure matérielle. Elle délimitait l'espace de circulation des transactions. Une transaction formée par une DApp de l'infrastructure publique ne pouvait pas, *a priori*, interagir avec les transactions dans des espaces privés de consortium comme Ubin, Komgo, Covantis ou Aura. Toutefois, le cas de The Dauriel Network (Chapitre 2) montre que le langage des *smart contracts* permettait de créer des passerelles entre différents espaces transactionnels (inter-opérables) et par là projeter une économie

Conclusion générale

numérique unifiée par une infrastructure publique et des espaces connectables à une « couche de règlement mondiale » (*global settlement layer*).

La gouvernance par les transactions se diffuse par des pratiques de conception de plateformes qui sont partagées au sein d'un écosystème étendu, quelles que soient les organisations économiques imaginées. Ces pratiques émancipées des formes organisationnelles qu'elles instituent illustrent le déplacement d'un mode de gouvernement des centres, qui vise les données, à une gouvernance des relations par les transactions, qui pense et institue des formes relationnelles. Les relations étaient typées selon des standards informatiques dont la qualité était garantie par une communauté étendue, facilitant leur circulation et leur prise en main par des entrepreneurs de l'écosystème. Cet écosystème regroupait les praticiens ; il était composé d'acteurs travaillant à instituer Ethereum aussi bien sur l'infrastructure publique que dans des infrastructures privées ; les meetups étaient des lieux privilégiés de circulation de pratiques partagées inscrites dans des logiciels de formation et de formulation (Chapitre 2 et 3). Le cas de la conception successive des standards ERC-20, ERC-777 et ERC-1400 témoigne à la fois de la systématisation et de la plasticité de la formulation de relations comme transactions. Ces relations étaient également définies sur mesure, par des sociétés de conseil ou par des sociétés de développement comme ConsenSys. Les relations spécifiques aux grandes entreprises étaient inscrites dans des logiciels constituant une « pile » de produits, par exemple pour garantir confidentialité des échanges ou possibilités de *reporting*.

La gouvernance par les transactions s'intéresse à des relations comme unités échangeables, attachées à des *wallets* et non à des identités du monde définies hors de l'espace, par des centres. Le cas du projet LeVote témoigne du grand écart de conception du lien social entre le cadrage par l'utilisateur générique *wallet* et les citoyens (Chapitre 3). La raison d'être du premier était de réduire des relations à un code dont l'exécution est prévisible et articulée aux autres transactions, alors que les seconds formaient un corps électoral nécessitant identité, administration, ou encore présence physique. Les mécanismes imaginés pour financer les biens publics témoignent de la difficulté à concevoir une action collective basée sur la seule détention d'unités échangeables. Sans identité, l'alternative était la suivante : la

Conclusion générale

ploutocratie, sinon garantir que les individus composant le corps social ne puissent pas s'associer, pour qu'ils agissent absolument isolés.

2.2. Autonomie instituée

L'autonomie de ces espaces transactionnels était sans cesse soumise à l'irruption de centres : décentraliser était une préoccupation et une activité permanente des acteurs participant à les instituer. Le fondement de cette autonomie, l'infrastructure publique d'Ethereum comme de Bitcoin, était confronté à la centralité de fermes de minage qui contrevenait à la compétition matérielle prescrite par la mystique du protocole (Chapitre 4). Elle dépendait également des logiciels « clients » des *miners* : la communauté multipliait les logiciels et les équipes de développement pour éviter les centres logiciels.

L'autonomie de ces espaces était une fonction infrastructurelle qui devait être maintenue par des interventions régulières. Il était communément accepté qu'elle dépende de développeurs proposant des évolutions de protocole. Mais le cas de la controverse TheDAO et l'opposition entre les deux lignes « *Code is Law* » et « *World Computer* » (Chapitre 4) témoigne de manière éclatante des difficultés à penser l'action collective sur un système supposé autonome. Il révèle des conflits que j'ai analysés en termes « rationalité infrastructurelle » à partir de la notion de « rationalité gouvernementale » de Michel Foucault (2004b). La prise en compte de l'écosystème dans la définition de l'autonomie s'imposait ; sans lui, l'infrastructure n'avait plus de raison d'être. C'est encore au nom de l'écosystème que les meneurs d'Ethereum posaient le problème du financement des biens publics. Cette rationalité gouvernementale pose les hypothèses de la micro-économie à l'origine d'un problème politique. Elle met en lumière les tensions entre calcul autonome et démocratie.

L'autonomie de ces espaces supposait que leurs concepteurs évitent les centres dans leur propre organisation. La communauté elle-même se disait décentralisée (Chapitre 4), tout comme l'écosystème dont la figure, le développeur de DApp, était un travailleur autonome (Chapitre 3). Cet impératif s'observait également dans le processus de conception des

Conclusion générale

DApp. La forme idéale d'organisation du travail de conception était la DAO, organisation décentralisée par excellence car décidant du devenir de l'application via l'infrastructure elle-même (Chapitre 2). Il s'observait enfin dans l'élaboration de mécanismes susceptibles de résoudre le problème du financement des « biens publics ». Ces mécanismes étaient imaginés en opposition aux gouvernements centraux de la Fondation Ethereum et de ConsenSys (Chapitre 4).

L'autonomie de ces espaces entrainait en tension avec toute forme d'action concertée, toujours suspecte de la dénaturer au profit d'un sous-ensemble d'acteurs. J'ai proposé une grammaire de l'action collective (Chapitre 4) : décisions comme délibérations devaient passer par l'infrastructure elle-même afin de garantir que seule des expressions de préférences purement individuelles. Les coalitions étaient elles-mêmes des centres dans les actions collectives. La mystique était renversée : son principe d'action collective des *miners*, calculer sans connaître, était appliquée à un groupe décisionnaire et délibérant. Son script (Akrich 1987) était adapté à l'ensemble des porteurs d'ethers : ils étaient, comme les *miners*, des entités agissant selon leurs seuls propres intérêts. Cette hypothèse anthropologique se lisait dans l'anthropologie moutonnaire de Vitalik Buterin. Elle se lisait également dans la figure de Bob le « constructeur de biens publics », individu rationnel agissant de manière isolée. Autrement dit, l'hypothèse permettant de répondre à la problématisation initiale de réseaux défaillants (la compétition entre tous, produite par le protocole, clé de voûte de l'autonomie de l'infrastructure) était un principe actif pour imaginer l'action collective garantissant cette autonomie.

L'autonomie de ces espaces résultait des activités distribuées d'un large ensemble d'acteurs : développeurs, entrepreneurs, investisseurs, militants, administrations et entreprises, cadres de grandes entreprises, passionnés de technologies comme de finance. L'autonomie était sémiotique : les concepteurs étaient suivis par le régulateur français pour laisser aux premiers le soin de définir la signification juridique de leurs créations. Cette compétence était accompagnée par des standards alignés avec des objets régulés : les *security tokens* remplissaient la catégorie juridique d'instrument financier, neutralisant l'incertitude juridique pesant sur la prolifération des jetons utilitaires, pourtant souvent vus

Conclusion générale

comme des dispositifs d'investissement par ceux qui s'en saisissaient. Ce cas témoigne du décalage entre les objets du gouvernement d'un centre (l'État) et la gouvernance par les transactions : alors que le premier s'intéresse aux entités mises en relations avec la catégorie « instrument financier », la seconde cible la relation elle-même, le jeton conçu comme bon d'utilisation d'un service.

L'autonomie de ces espaces était également instituée par les plateformes d'échange de cryptoactifs (*exchanges*) qui garantissaient différentes convertibilités (Chapitre 2). Ils rendaient possibles l'articulation entre utilisateur futur d'une DApp et investissement au présent par les jetons utilitaires. Ils prolongeaient ces espaces transactionnels, rendant commensurables en monnaie (dollar, euro) des cryptoactifs qui étaient conçus pour prendre des significations particulières dans ces espaces, par exemple les jetons utilitaires ou les jetons de gouvernance. Ils garantissaient un cours à des *coins* comme le bitcoin ou l'ether. Ils participaient ainsi à articuler différentes significations de l'ether : paiement de l'exécution des *smart contracts*, financement des startups de DApp par les ICO, financement des biens publics de la communauté, ou encore collatéral dans certaines applications de la finance décentralisée. Leur place stratégique apparaissait dans l'asymétrie des conditions qu'ils imposaient aux entrepreneurs en faisant des ICO des IEO. En réponse à leur « centralité » dans ces espaces, des DApps dites « échanges décentralisés » étaient imaginées ; Kyber Networks (Chapitre 2) était l'une d'elles.

3. Perspectives

J'ai choisi de centrer mon enquête sur le processus de conception des blockchains par Ethereum, suivant une préoccupation et une démarche indiquées en Introduction. Le choix d'une enquête multi-sites visait à multiplier les points de vue sur un processus qui, tout comme l'infrastructure, était distribué. Différents prolongements d'enquête permettraient de poursuivre l'analyse des blockchains comme technologies de gouvernance.

Il serait par exemple intéressant d'enquêter auprès de différents concepteurs de DApps, plusieurs années après le lancement de leur application ou de leur ICO. Ces enquêtes

Conclusion générale

pourraient donner une épaisseur historique à la démarche présentée au Chapitre 2, permettant d'analyser l'évolution des agencements marchands (Callon 2013) imaginés du Web 3.0, les significations des argents qu'il fait circuler et ce qu'ils instituent (De Blic & Lazarus 2021b), ainsi que l'évolution des formes de capitalisation de ces entreprises et de ces objets (Muniesa et al. 2017).

Les consortia et les utilisations « privées » des blockchains sont des objets moins visibles que les cryptoactifs mais qui participent à les diffuser, en finançant leurs concepteurs et en généralisant les pratiques de formation et de formulation des transactions (Chapitre 3). Des études détaillées de ces objets permettraient de mieux comprendre la généralisation de la gouvernance par les transactions et de contribuer à caractériser la spécificité de la forme plateforme (Plantin et al. 2016, 2018). Parmi les points d'entrée et d'une part, il serait possible de suivre des concepteurs dans l'élaboration de consortia aussi bien dans leur ingénierie matérielle et logicielle que dans les couloirs feutrés des grandes entreprises qui imaginent de nouvelles formes pour leurs relations avec ces technologies. D'autre part, il serait intéressant de suivre le parcours de logiciels entre leurs concepteurs comme ConsenSys ou Hyperledger, et leur déploiement sur des projets.

Différentes communautés de développement logiciels, locales ou langagières participaient à la vaste « communauté Ethereum ». J'ai proposé une analyse de la manière dont l'action collective était réfléchie au niveau de cet ensemble à partir d'événements et de problèmes qui ont marqué son histoire (Chapitre 4). Des études de sociologie du numérique centrées sur certaines de ces communautés permettraient de comprendre comment ces acteurs s'organisent en pratique et s'articulent à l'ensemble de la communauté Ethereum. De telles études amélioreraient la compréhension de la dynamique de la communauté et de son rapport à ce qui est commun (Ostrom & Hess 2007). Elles permettraient ainsi de comprendre comment s'organise en pratique l'action collective dans des sous-ensembles de la communauté. Elles renseigneraient également sur les rapports entre la communauté et l'écosystème, c'est-à-dire entre développement open source, maintenance de l'infrastructure publique et développement de logiciels pour des startups, d'une part, et pour des consortia, d'autre part.

Conclusion générale

Il serait par ailleurs important de suivre d'autres regards que ceux des concepteurs ; avant tout, ceux des utilisateurs. En raison de son homogénéité fonctionnelle et de ses communautés mêlant utilisateurs et concepteurs depuis quelques années, les utilisations de la « finance décentralisée » constitueraient un point de départ intéressant pour des études à la rencontre de la sociologie du numérique et des études sociales de la finance et de l'argent. Elles permettraient de cerner les significations que les utilisateurs leur donnent, et ainsi de mieux comprendre la dynamique de la conception de ces applications dans les rencontres d'utilisateurs imaginés par les concepteurs et d'utilisateur en chair et en os (Akrich 1987, 1992).

La gouvernance par les transactions s'étend à des relations entre individus qui n'ont pas « souverainement » décidé de les utiliser, comme au Salvador où Bitcoin est devenue monnaie ayant cours légal. Des études de sociologie économique dans les pays donnant cours légal ou facilitant l'institutionnalisation des cryptoactifs permettrait de documenter les turbulences entre souveraineté scripturale et souveraineté monétaire (Orléan 2016).

Enfin, suivre le regard des autorités de régulation et de surveillance, des gouvernements et des législateurs permettrait de progresser dans l'analyse de l'institutionnalisation des cryptoactifs et des blockchains. Symétriquement, ces études donneraient des prises à une sociologie de l'action publique qui pourrait partir des réglementations portant sur les intermédiaires distribuant les cryptoactifs et les politiques d'accueil sur le territoire (Orange 2022) comme des mobilisations d'utilisateurs demandant des comptes aux autorités publiques (Mauduit 2022).

Bibliographie

- Abbate, Janet. 1999. *Inventing the Internet*. Cambridge, Mass: MIT Press.
- Aglietta, Michel. 2008. « Universalité et transformations de la monnaie : la nature des crises monétaires ». In *La Monnaie dévoilée par ses crises*, éd. Bruno Théret. Paris: Editions de l'EHESS.
- Akrich, Madeleine. 1987. « Comment décrire les objets techniques ? » *Techniques et culture* (9): 49-64.
- . 1989. « La construction d'un système socio-technique ». *Anthropologie et Sociétés* 13(2): 31-54.
- . 1992. « The De-Description of Technical Objects ». In *Shaping Technology/Building Society*, Inside technology, éd. Wiebe E. Bijker, W. Bernard Carlson, et Trevor Pinch. Cambridge, MA: MIT Press, 205-24.
- Akrich, Madeleine, Michel Callon, et Bruno Latour, éd. 2006. *Sociologie de la traduction: Textes fondateurs*. Paris: Presses des Mines.
- Akrich, Madeleine, et Bruno Latour. 1992. « A Summary of a Convenient Vocabulary for the Semiotics of Human and Non-human Assemblies ». In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, éd. Wiebe E. Bijker et John Law. Cambridge, MA: MIT Press.
- Allen, Darcy W. E., Chris Berg, Aaron M. Lane, et Jason Potts. 2018. « Cryptodemocracy and Its Institutional Possibilities ». *The Review of Austrian Economics*. <http://link.springer.com/10.1007/s11138-018-0423-6> (31 mars 2020).
- Allen, Darcy W.E., Chris Berg, et Mikayla Novak. 2018. « Blockchain: An Entangled Political Economy Approach ». *Journal of Public Finance and Public Choice* 33(2): 105-25.
- Atzori, Marcella. 2015. « Blockchain Technology and Decentralized Governance: Is the State Still Necessary? ». https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 (31 mars 2020)
- Bachrach, Peter, et Morton S. Baratz. 1962. « Two Faces of Power ». *American Political Science Review* 56(4): 947-52.

Bibliographie

- Barbrook, Richard, et Andy Cameron. 1996. « The Californian Ideology ». *Science as Culture* 6(1): 44-72.
- Barlow, John Perry. 1996. « A Declaration of the Independence of Cyberspace ». *Electronic Frontier Foundation*.
- Barnes, Barry. 1984. « On Authority and Its Relationship to Power ». *The Sociological Review* 32(1_suppl): 180-95.
- Benghozi, Pierre-Jean. 2006. « Les communautés virtuelles: structuration sociale ou outil de gestion ». *Entreprises et Histoire* Eska(43): 67-81.
- Beniger, James R. 1986. *The Control Revolution. Technological and Economic Origins of the Information Society*. Cambridge, Massachusetts ; London, England: Harvard University Press.
- Benquet, Marlène, et Théo Bourgeron. 2021. *La finance autoritaire - Vers la fin du néolibéralisme*. Paris: Raisons D'agir.
- Berg, Chris. 2017. « What Diplomacy in the Ancient Near East Can Tell Us About Blockchain Technology ». *Ledger* 2: 55-64.
- Berg, Chris, Sinclair Davidson, et Jason Potts. 2018. « Blockchains as Constitutional Orders ». In *James M. Buchanan*, éd. Richard E. Wagner. Cham: Springer International Publishing, 383-97. http://link.springer.com/10.1007/978-3-030-03080-3_18 (31 mars 2020).
- . 2019. « Blockchain Technology as Economic Infrastructure: Revisiting the Electronic Markets Hypothesis ». *Frontiers in Blockchain* 2: 22.
- Beuscart, Jean-Samuel, et Maxime Crépel. 2014. « Les plateformes d'autopublication artistique en ligne : quatre figures de l'engagement des amateurs dans le web 2.0. » In *Les stratégies de la notoriété, Intermédiaires et production de la valeur dans les univers artistiques*, éd. Wenceslas Lizé, Delphine Naudier, et Séverine Sofio, 165-84.
- Beuscart, Jean-Samuel, et Patrice Flichy. 2018. « Plateformes numériques ». *Réseaux* 212(6): 9.
- Bijker, Wiebe E., Thomas Parke Hughes, et Trevor Pinch, éd. 1989. *The Social*

Bibliographie

- Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, Mass: MIT Press.
- Bijker, Wiebe E., et John Law, éd. 1992. *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, Mass.: MIT Press.
- Birch, Kean, et Fabian Muniesa, éd. 2020. *Assetization: Turning Things into Assets in Technoscientific Capitalism*. Cambridge, Massachusetts London, England: The MIT Press.
- Blanc, Jérôme. 2013. « 18. Usages de l'argent et pratiques monétaires: » In *Traité de sociologie économique*, Quadrige, éd. Philippe Steiner et François Vatin. Presses Universitaires de France, 671-710. <https://www.cairn.info/traite-de-sociologie-economique-2013--9782130608318-page-671.htm?ref=doi> (4 avril 2022).
- Blanc, Maurice. 2009. « La transaction sociale : genèse et fécondité heuristique ». *Pensée plurielle* 20(1): 25.
- de Blic, Damien, et Jeanne Lazarus. 2021a. « Conclusion ». In *Sociologie de l'argent*, Repères, Paris: La Découverte, 107-8.
- . 2021b. *Sociologie de l'argent*. Paris: La Découverte.
- Bodó, Balázs, Daniel Gervais, et João Pedro Quintais. 2018. « Blockchain and Smart Contracts: The Missing Link in Copyright Licensing? » *International Journal of Law and Information Technology* 26(4): 311-36.
- Bowker, Geoffrey C., Karen Baker, Florence Millerand, et David Ribes. 2009. « Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment ». In *International Handbook of Internet Research*, éd. Jeremy Hunsinger, Lisbeth Klastrup, et Matthew Allen. Dordrecht: Springer Netherlands, 97-117. http://link.springer.com/10.1007/978-1-4020-9789-8_5 (20 août 2018).
- Bowker, Geoffrey C., et Susan Leigh Star. 1998. « Building Information Infrastructures for Social Worlds — The Role of Classifications and Standards ». In *Community Computing and Support Systems*, éd. Toru Ishida. Berlin, Heidelberg: Springer Berlin Heidelberg, 231-48. http://link.springer.com/10.1007/3-540-49247-X_16 (20 août 2018).
- Broca, Sébastien. 2021. « Communs et capitalisme numérique : histoire d'un antagonisme

Bibliographie

- et de quelques affinités électives ». *Terminal* (130).
<http://journals.openedition.org/terminal/7595> (4 février 2022).
- Brunton, Finn. 2019. *Digital Cash The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton University Press.
- Caliskan, Koray. 2020. « Data Money: The Socio-Technical Infrastructure of Cryptocurrency Blockchains ». *Economy and Society* 49(4): 540-61.
- Çalışkan, Koray, et Michel Callon. 2009. « Economization, Part 1: Shifting Attention from the Economy towards Processes of Economization ». *Economy and Society* 38(3): 369-98.
- . 2010. « Economization, Part 2: A Research Programme for the Study of Markets ». *Economy and Society* 39(1): 1-32.
- Callon, Michel. 1984. « Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay ». *The Sociological Review* 32(1_suppl): 196-233.
- . 2012. « Les incertitudes scientifiques et techniques constituent-elles une source possible de renouvellement de la vie démocratique ? ». *Papiers de Recherche du CSI* (28).
- . 2013. « Qu'est-ce qu'un agencement marchand ? » In *Sociologie des agencements marchands : textes choisis*, éd. Madeleine Akrich, Michel Callon, Bruno Latour. Paris: Presses des Mines.
- , éd. 2013. *Sociologie des agencements marchands : textes choisis*. Sciences sociales. Paris : Presses des Mines.
- . 2015. « Revisiting Marketization: From Interface-Markets to Market-Agencements ». *Consumption Markets & Culture*.
<https://www.tandfonline.com/doi/full/10.1080/10253866.2015.1067002> (6 mars 2023).
- Cardon, Dominique. 2013. « Inside the Mind of PageRank: A Study of Google's Algorithm ». *Réseaux* 1(177).
- . 2015a. *À quoi rêvent les algorithmes*. La république des idées. Seuil.

Bibliographie

- . 2015b. « Surveiller sans punir. La gouvernance de Wikipédia ». In *Wikipédia, objet scientifique non identifié*, Intelligences numériques, éd. Lionel Barbe, Louise Merzeau, et Valérie Schafer. Nanterre: Presses universitaires de Paris Nanterre.
- Cardon, Dominique, et Julien Levrel. 2009. « La vigilance participative. Une interprétation de la gouvernance de Wikipédia ». *Réseaux* 154(2): 51.
- Cardon, Dominique, et Christophe Prieur. 2016. « Comment la conversation a façonné le web ». In: *L'ordinaire d'internet*, Individu et Société, éd. Olivier Martin et Eric Dagira,. Armand Colin, pp. 226–247.
- Cartwright, Nancy. 1999. « Nomological Machines and the Laws They Produce ». In *The Dappled World: A Study of the Boundaries of Science*, Cambridge, UK : New York, NY: Cambridge University Press, 49-74.
- Casilli, Antonio. 2019. *En attendant les robots : enquête sur le travail du clic*. Paris: Seuil.
- Chow-White, Peter, Alberto Lusoli, Vu Thuy Anh Phan, et Sandy Edward Green. 2020. « ‘Blockchain Good, Bitcoin Bad’: The Social Construction of Blockchain in Mainstream and Specialized Media ». *Journal of Digital Social Research* 2(2): 1-27.
- Clarke, Chris, et Lauren Tooker. 2018. « Social Finance Meets Financial Innovation: Contemporary Experiments in Payments, Money and Debt ». *Theory, Culture & Society* 35(3): 3-11.
- Coase, Ronald. 1937. « The Nature of the Firm ». *Economica* 4(16): 386-405.
- Cochoy, Franck. 2004. « La captation des publics entre dispositifs et dispositions, ou le petit chaperon rouge revisité ». In *La captation des publics*, éd. Franck Cochoy. Presses universitaires du Midi, 11-68. <http://books.openedition.org/pumi/14271> (21 janvier 2023).
- Cohen, Julie E. 2019. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York, NY: Oxford University Press.
- Crenson, M. A. 1971. *The Un-Politics of Air Pollution: A Study of Non-Decisionmaking in the Cities*. Baltimore, MD: Johns Hopkins Press.
- Crook, Malcolm, et Tom Crook. 2011. « L'isolement universel ? La globalisation du scrutin

Bibliographie

- secret au XIXe siècle ». *Revue d'histoire du XIXe siècle*, n° 43 (novembre): 41-45.
<https://doi.org/10.4000/rh19.4151>.
- Dahl, Robert A. 1958. « A Critique of the Ruling Elite Model ». *American Political Science Review* 52(2): 463-69.
- . 1974. *Who Governs? Democracy And Power In An American City*. New Haven and London: Yale University Press.
- Daidj, Nabyla. 2011. « Les écosystèmes d'affaires : une nouvelle forme d'organisation en réseau ? » *Management & Avenir* 46(6): 105.
- Davidson, Sinclair, Primavera De Filippi, et Jason Potts. 2016a. « Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology ». *SSRN Electronic Journal*. <https://www.ssrn.com/abstract=2811995> (6 avril 2020).
- . 2016b. « Economics of Blockchain ». *SSRN Electronic Journal*. <https://www.ssrn.com/abstract=2744751> (6 avril 2020).
- . 2018. « Blockchains and the Economic Institutions of Capitalism ». *Journal of Institutional Economics* 14(4): 639-58.
- De Filippi, Primavera, et Samer Hassan. 2016. « Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code ». *First Monday*. <https://firstmonday.org/ojs/index.php/fm/article/view/7113> (29 avril 2021).
- De Filippi, Primavera, et Benjamin Loveluck. 2016. « The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure ». *Internet Policy Review*. <http://policyreview.info/node/427> (25 février 2019).
- De Filippi, Primavera, Morshed Mannan, et Wessel Reijers. 2020. « Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance ». *Technology in Society* 62. <https://linkinghub.elsevier.com/retrieve/pii/S0160791X20303067> (6 février 2021).
- De Filippi, Primavera, et Aaron Wright. 2018. *Blockchain and the Law: The Rule of Code*. Harvard University Press.
- . 2019. « The Rule of Code vs. The Rule of Law ». *Medium* (blog). 4 octobre 2019. <https://hup.medium.com/the-rule-of-code-vs-the-rule-of-law> (6 février 2021).

Bibliographie

- Demazière, Didier, François Horn, et Marc Zune. 2006. « Dynamique de développement des communautés du logiciel libre ». *Terminal* 97(98): 71-84.
- . 2011. « Ethnographie de terrain et relation d'enquête. Observer les « communautés » de logiciels libres ». *Sociologie* 2(2): 165-83.
- Demortain, David. 2019. « Les jeux politiques du calcul: Sociologie de la quantification dans l'action publique ». *Revue d'anthropologie des connaissances* 13(4): 953.
- Denis, Jérôme. 2018. *Le travail invisible des données: Éléments pour une sociologie des infrastructures scripturales*. Paris : Presses des Mines.
- Denis, Jérôme, et David Pontille. 2012. « Travailleurs de l'écrit, matières de l'information ». *Revue d'anthropologie des connaissances* 6, 1(1): 1.
- Dewey, John, et Arthur F. Bentley. 1946. « Interaction and Transaction ». *The Journal of Philosophy* 43(19): 505.
- Dodd, Nigel. 2014. *The Social Life of Money*. Princeton London Oxford: Princeton University Press.
- . 2017. « Utopian Monies. Complementary currencies, Bitcoin, and the social life of money ». In *Money Talks: Explaining How Money Really Works*, éd. Nina Bandelj, Frederik F. Wherry, et Viviana A. Zelizer. Princeton, NJ: Princeton University Press.
- Doganova, Liliana. 2011. « Necessarily Untrue: On the Use of the Discounted Cash Flow Formula in Valuation of Exploratory Projects. », *7th Critical Management Studies Conference (CMS7 2011)*, In Naples, Italie.
- Doganova, Liliana, et Fabian Muniesa. 2015. « Capitalization Devices ». In *Making Things Valuable*, éd. Martin Kornberger, Lise Justesen, Jan Mouritsen, et Anders Koed Madsen. Oxford University Press, 109-25.
<https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780198712282.001.0001/acprof-9780198712282-chapter-6> (16 mars 2022).
- Drummer, Daniel, et Dirk Neumann. 2020. « Is Code Law? Current Legal and Technical Adoption Issues and Remedies for Blockchain-Enabled Smart Contracts ». *Journal of Information Technology* 35(4): 337-60.

Bibliographie

- DuPont, Quinn. 2018. « Experiments in Algorithmic Governance. A History and Ethnography of “The DAO,” a Failed Decentralized Autonomous Organization ». In *Bitcoin and beyond: Cryptocurrencies, Blockchains and Global Governance*, RIPE series in global political economy, éd. Malcolm Campbell-Verduyn. London ; New York: Routledge, Taylor & Francis Group.
- Durkheim, Emile. 1894. *Les Règles de la méthode sociologique*. Petite Bibliothèque Payot. Paris: Payot.
- . 1897. *Le Suicide. Étude de sociologie*. Petite Bibliothèque Payot. Paris: Payot.
- Ebeling, Mary F.E. 2016. *Healthcare and Big Data*. New York: Palgrave Macmillan US.
- Eyal, Ittay, et Emin Gun Sirer. 2013. « Majority Is Not Enough: Bitcoin Mining Is Vulnerable ». arXiv. <http://arxiv.org/abs/1311.0243> (13 avril 2023).
- van Eeten, Michel JG, et Milton Mueller. 2012. « Where Is the Governance in Internet Governance? » *New Media & Society* 15(5): 720-36.
- Eisenstein, Elizabeth L. 1991. *La révolution de l'imprimé Dans l'Europe des premiers temps modernes*. Paris: La Découverte.
- Ellul, Joshua. 2021. « Blockchain Is Dead! Long Live Blockchain! » *The Journal of The British Blockchain Association* 4(1): 1-11.
- Ermoshina, Ksenia, et Francesca Musiani. 2019. « “Standardising by Running Code”: The Signal Protocol and *de Facto* Standardisation in End-to-End Encrypted Messaging ». *Internet Histories* 3(3-4): 343-63.
- Fairclough, Norman. 1989. *Language and Power*. London: Longman.
- Femia, Joseph V. 1981. *Gramsci's Political Thought*. Oxford: Clarendon Press.
- Flichy, Patrice. 2001. *L'imaginaire d'Internet*. Paris: La Découverte.
- Flichy, Patrice. 2017. *Les nouvelles frontières du travail à l'ère numérique*. Paris: Seuil.
- Foucart, Jean. 2013. « Pragmatisme et transaction. La perspective de John Dewey ». *Pensée plurielle* 33-34(2): 73.
- Foucault, Michel. 1972. *Histoire de la folie à l'âge classique*. Paris : Gallimard.

Bibliographie

- . 1975. *Surveiller et punir*. Paris : Gallimard.
- . 1982. « The Subject and Power ». *Critical Inquiry* 8(4): 777-95.
- . 1997. *Il faut défendre la société*. Paris : Seuil.
- . 2004a. *Sécurité, Territoire, Population*. Paris : Seuil.
- . 2004b. *Naissance de la biopolitique*. Paris : Seuil.
- . 2004c. « « Des espaces autres » ». *Empan* 54(2): 12.
- Fréry, Frédéric, Anne Gratacap, et Thierry Isckia. 2012. « Les écosystèmes d'affaires, par-delà la métaphore ». *Revue française de gestion* 38(222): 69-75.
- Friedman, David D. 1973. « The Machinery of Freedom: Guide to a Radical Capitalism ». Open Court Publishing Company.
- Garrigou, Alain. 2012. *Les secrets de l'isoloir*. Le Bord de l'eau.
- Gensollen, Michel. 2004. « Économie non rivale et communautés d'information ». *Réseaux* 124(2): 141.
- Goldenfein, Jake, et Andrea Leiter. 2018. « Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct ». *Law and Critique* 29(2): 141-49.
- Golumbia, David. 2016. *The Politics of Bitcoin. Software as Right-Wing Extremism. Forerunners: Ideas First*. Minneapolis: University of Minnesota Press.
- Goody, Jack. 1979. *La raison graphique*. Paris : Les Editions de Minuit.
- Gramsci, Antonio. 1971. *Selections from the Prison Notebooks*. éd. Quintin Hoare et Geoffrey Nowell Smith. New York : International Publishers.
- Hardin, Garrett. 1968. « The Tragedy of the Commons ». *Science* 162(3859): 1243-48.
- Hart, Oliver, et John Moore. 1990. « Property Rights and the Nature of the Firm ». *Journal of Political Economy* 98(6): 1119-58.
- Hassan, Samer, et Primavera De Filippi. 2017. « The Expansion of Algorithmic Governance: From Code Is Law to Law Is Code ». Institut Veolia.

Bibliographie

- Hayek, Friedrich A. 1945. « The Use of Knowledge in Society ». *The American Economic Review* XXXV(4): 519-30.
- Helmond, Anne. 2015. « The Platformization of the Web: Making Web Data Platform Ready ». *Social Media + Society* 1(2): 205630511560308.
- Hughes, Thomas Parke. 1983a. « L'électrification de l'Amérique : les bâtisseurs de systèmes ». *Culture Technique* 10 : 21-41.
- . 1983b. « Networks of Power: Electrification in Western Society, 1880-1930 ». Baltimore: Johns Hopkins University Press.
- Hunter, Floyd. 1953. *Community Power Structure: A Study of Decision Makers*. Chapel Hill, NC: University of North Carolina Press.
- Hütten, Moritz. 2019. « The Soft Spot of Hard Code: Blockchain Technology, Network Governance and Pitfalls of Technological Utopianism ». *Global Networks* 19(3): 329-48.
- Jabbar, Karim, et Pernille Bjørn. 2019. « Blockchain Assemblages: Whiteboxing Technology and Transforming Infrastructural Imaginaries ». In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, Glasgow, Scotland Uk: ACM Press, 1-13. <http://dl.acm.org/citation.cfm?doid=3290605.3300496> (14 août 2019).
- Jacquet, Édouard. 2015. « Le « prêt payant ». Les paradoxes de l'économie collaborative ». *Réseaux* 190-191(2): 99-120.
- Jasanoff, Sheila, et Sang-Hyun Kim. 2009. « Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea ». *Minerva* 47(2): 119-46.
- Joly, Pierre-Benoît. 2015. « Le régime des promesses technoscientifiques ». In *Pourquoi tant de promesses*, éd. Marc Audétat. Paris: Hermann, 31-48.
- Joly, Pierre-Benoît, Arie Rip, et Michel Callon. 2010. « Re-inventing Innovation ». In *Governance of Innovation. Firms, Clusters and Institutions in a Changing Setting*, éd. Maarten J. Arentsen, Wouter van Rossum, et Albert E. Steenge. Cheltenham, UK ; Northampton, MA: Edward Elgar, 19-32.

Bibliographie

- Käll, Jannice. 2018. « Blockchain Control ». *Law and Critique* 29(2): 133-40.
- Kelty, Christopher M. 2008. *Two Bits. The Cultural Significance of Free Software*. Experimental Futures. Durham and London: Duke University Press.
- Kuhn, Thomas. 1983. *La structure des révolutions scientifiques*. Paris : Flammarion.
- Lafitte, Jacques. 1932. *Réflexions sur la science des machines*. Paris : Vrin.
- Lampert, Leslie, Robert Shostak, et Marshall Pease. 1982. « The Byzantine Generals Problem ». *ACM Transactions on Programming Languages and Systems* 4 (3): 382-401.
- Langley, Paul, et Andrew Leyshon. 2017. « Platform Capitalism: The Intermediation and Capitalization of Digital Economic Circulation ». *Finance and Society* 3(1): 11-31.
- Latour, Bruno. 1984. « The Powers of Association ». *The Sociological Review* 32(1_suppl): 264-80.
- . 1987. *Science in Action: How to Follow Scientists and Engineers through Society*. Cambridge, Massachusetts: Harvard University Press.
- . 1990. « Technology Is Society Made Durable ». *The Sociological Review* 38(1_suppl): 103-31.
- . 1992. « Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts' ». In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, éd. Wiebe E. Bijker et John Law. Cambridge, MA: MIT Press.
- . 1993. « Le “pédofil” de Boa-Vista : montage photo-philosophique ». In *La clef de Berlin. Petites leçons de sociologie des sciences*, La Découverte/Poche, 171-225.
- . 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford ; New York: Oxford University Press.
- . 2007. « La clef de Berlin ». In *Petites leçons de sociologie des sciences*, Poche / Sciences humaines et sociales, La Découverte, 33-46.
- Latour, Bruno, et Steve Woolgar. 1979. *Laboratory Life: The Construction of Scientific Facts*. Sage Publications.

Bibliographie

- Laurent, Brice. 2011. « Democracies on Trial. Assembling Nanotechnology and its Problems ». Mines ParisTech.
- Law, John. 1984a. « Editor's Introduction: Power/Knowledge and the Dissolution of the Sociology of Knowledge ». *The Sociological Review* 32(1_suppl): 1-19.
- . 1984b. « On the Methods of Long-Distance Control: Vessels, Navigation and the Portuguese Route to India ». *The Sociological Review* 32(1_suppl): 234-63.
- . 1986. « On Power and Its Tactics: A View from the Sociology of Science ». *The Sociological Review* 34(1): 1-38.
- . 2009. « Actor Network Theory and Material Semiotics ». In *The New Blackwell Companion to Social Theory*, Blackwell companions to sociology, éd. Turner. Chichester, West Sussex, United Kingdom ; Malden, MA, USA: Wiley-Blackwell.
- Lemieux, Victoria L. 2019. « Blockchain and Public Record Keeping: Of Temples, Prisons, and the (Re)Configuration of Power ». *Frontiers in Blockchain* 2: 5.
- Lessig, Lawrence. 2000. « Code Is Law. On Liberty in Cyberspace ». *Harvard Magazine*. <https://www.harvardmagazine.com/2000/01/code-is-law-html?page=all> (9 décembre 2022).
- Levy, Karen E. C. 2017. « Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law ». *Engaging Science, Technology, and Society* 3: 1-15.
- Li, Zixuan. 2020. *Centrality of Blockchain*. Washington University Open Scholarship Washington University Open Scholarship. https://openscholarship.wustl.edu/cse_research/1180 (10 janvier 2023).
- Lukes, Steven. 2004. *Power: A Radical View*. 2nd ed. Houndmills, Basingstoke, Hampshire : New York: Palgrave Macmillan.
- MacDonald, Trent, Darcy Allen, et Jason Potts. 2016. « Blockchains and the Boundaries of Self-Organized Economies- Predictions for the Future of Banking ». In *Banking beyond Banks & Money*, éd. Paulo Tasca, Tomaso Aste, Lorian Pelizzon, et Nicolas Perony. Springer.
- MacKenzie, Donald. 2019. « Pick a nonce and try a hash ». *London Review of Books* 41(8):

Bibliographie

35-38.

- Malcolm, Jeremy. 2013. « Internet Freedom in a World of States ». https://mail.intgovforum.org/cms/wks2013/workshop_background_paper/64_1367863304.pdf (15 janvier 2021).
- Mallard, Alexandre, Cécile Méadel, et Francesca Musiani. 2014. « The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin ». *Journal of Peer Production*: 11.
- Marcuse, Herbert. 1968. *L'Homme unidimensionnel*. Paris : Les Editions de Minuit.
- Marella, Venkata, Bikesh Upreti, Jani Merikivi, et Virpi Kristiina Tuunainen. 2020. « Understanding the Creation of Trust in Cryptocurrencies: The Case of Bitcoin ». *Electronic Markets* 30(2): 259-71.
- Masutti, Christophe. 2020. *Affaires privées. Aux sources du capitalisme de surveillance*. Caen : C&F éditions.
- Maurel, Lionel. 2014. « Comment “Code Is Law” s’est renversé en “Law Is Code” ». *S.I.Lex*. <https://scinfolex.com/2014/01/24/comment-code-is-law-sest-renverse-en-law-is-code/> (25 février 2021).
- Maurer, Bill. 2015. *How Would You Like to Pay? How Technology Is Changing the Future of Money*. Durham and London: Duke University Press.
- . 2016. « Re-Risking in Realtime. On Possible Futures for Finance after the Blockchain ». *Behemoth* 9(2). <https://freidok.uni-freiburg.de/data/11525> (5 mars 2019).
- . 2017. « Blockchains Are a Diamond’s Best Friend. Zelizer for the Bitcoin Moment ». In *Money Talks: Explaining How Money Really Works*, éd. Nina Bandelj, Frederik F. Wherry, et Viviana A. Zelizer. Princeton, NJ : Princeton University Press.
- Maurer, Bill, Taylor C. Nelms, et Lana Swartz. 2013. « “When Perhaps the Real Problem Is Money Itself!”: The Practical Materiality of Bitcoin ». *Social Semiotics* 23(2): 261-77.
- May, Timothy C. 1992. « The Crypto Anarchist Manifesto », 22 novembre 1992.

Bibliographie

- Mellet, Kevin, et Thomas Beauvisage. 2020. « Cookie Monsters. Anatomy of a Digital Market Infrastructure ». *Consumption Markets & Culture* 23(2): 110-29.
- Metcalfe, Robert. 2020. « The Ethernet Diagram ». *ieee802.org*. https://www.ieee802.org/3/ethernet_diag.html (15 septembre 2022).
- Mills, C. Wright. 1956. *The Power Elite*. Oxford University Press.
- Minsky, Marvin L. 1965. « Matter, Mind and Models ». *Proceedings of the IFIP Congress*: 45-49.
- Mirowski, Philip. 2002. *Machine Dreams: Economics Becomes a Cyborg Science*. Cambridge ; New York: Cambridge University Press.
- . 2017. « « What is science critique? Lessig, Latour » ». In *Handbook of the Political Economy of Science*, édité par David Tyfield, Rebecca Lave, Samuel Randalls, et Charles Thorpe. Londres et New York : Routledge, 429-50.
- Moore, James F. 1993. « Predators and Prey: A New Ecology of Competition ». *Harvard Business Review*.
- Morrison, Robbie, Natasha C. H. L. Mazey, et Stephen C. Wingreen. 2020. « The DAO Controversy: The Case for a New Species of Corporate Governance? » *Frontiers in Blockchain* 3: 25.
- Muniesa, Fabian. 2011. « A Flank Movement in the Understanding of Valuation ». *The Sociological Review* 59(2_suppl): 24-38.
- . 2015. « Actor-Network Theory ». In *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier, 80-84. <https://linkinghub.elsevier.com/retrieve/pii/B9780080970868850011> (18 mars 2021).
- . 2019. « Société du comportement, information de la sociologie ». *Zilsel* (5): 196-205.
- . 2021. « Finance: Cultural or Political? » *Journal of Cultural Economy*: 1-4.
- Muniesa, Fabian, Yuval Millo, et Michel Callon. 2007. « An Introduction to Market Devices ». *The Sociological Review* 55(2_suppl): 1-12.

Bibliographie

- Muniesa, Fabian, Liliana Doganova, Horacio Ortiz, Florence Paterson, Alaric Bourgoïn, Véra Ehrenstein, Pierre-André Juven, David Pontille, Basak Saraç-Lesavre, et Guillaume Yon, 2017. *Capitalization: a cultural guide*. Sciences sociales, Paris : Presses des Mines.
- Musiani, Francesca. 2013. « Network Architecture as Internet Governance ». *Internet Policy Review* 2(4). <https://policyreview.info/node/208> (15 octobre 2022).
- . 2018. « L'invisible qui façonne. Études d'infrastructure et gouvernance d'Internet ». *Tracés* (35): 161-76.
- . 2022. « La gouvernance d'Internet, brève histoire d'un espace à controverses ». *Terminal* (132-133). <http://journals.openedition.org/terminal/8398> (7 octobre 2022).
- Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, et Nanette S. Levinson, éd. 2016. *The Turn to Infrastructure in Internet Governance*. New York: Palgrave Macmillan US. <http://link.springer.com/10.1057/9781137483591> (17 avril 2021).
- Musiani, Francesca, Alexandre Mallard, et Cécile Méadel. 2018. « Governing What Wasn't Meant to Be Governed. A Controversy-Based Approach to the Study of Bitcoin Governance ». In *Bitcoin and beyond: Cryptocurrencies, Blockchains and Global Governance*, RIPE series in global political economy, éd. Malcolm Campbell-Verduyn. Abingdon, Oxon ; New York, NY: Routledge.
- Nelms, Taylor C., Bill Maurer, Lana Swartz, et Scott Mainwaring. 2018. « Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy ». *Theory, Culture & Society* 35(3): 13-33.
- Orléan, André. 2016. « 1. La sociologie économique de la monnaie »: In *Théories françaises de la monnaie*, Presses Universitaires de France, 33-65. <https:// Cairn.info/theories-francaises-de-la-monnaie-2016--9782130731474-page-33.htm?ref=doi> (18 mars 2021).
- Orlowski, Jeff, réal. 2020. *The Social Dilemma*. Netflix.
- Ortiz, Horacio. 2014. « The Limits of Financial Imagination: Free Investors, Efficient Markets, and Crisis: The Limits of Financial Imagination ». *American Anthropologist* 116(1): 38-50.

Bibliographie

- Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press.
- Ostrom, Elinor, et Charlotte Hess. 2007. *Understanding Knowledge as a Commons: From Theory to Practice*. Cambridge, Massachusetts, London, England : MIT Press.
- Perdana, Arif, W. Eric Lee, et Alastair Robb. 2021. « From Enfant Terrible to Problem-Solver? Tracing the Competing Discourse to Explain Blockchain-Related Technological Diffusion ». *Telematics and Informatics* 63: 101662.
- Pickering, Andrew. 2010. *The Cybernetic Brain: Sketches of Another Future*. Chicago: Univ. of Chicago Press.
- Pike, C, et A Capobianco. 2020. *Antitrust and the trust machine*. <http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf> (23 mai 2021).
- Pistor, Katharina. 2019. *The Code of Capital*. Princeton & Oxford: Princeton University Press.
- Plantin, Jean-Christophe, Carl Lagoze, Paul N Edwards, et Christian Sandvig. 2016. « Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook ». *New Media & Society* 20(1): 293-310.
- Plantin, Jean-Christophe, et Aswin Punathambekar. 2018. « Digital Media Infrastructures: Pipes, Platforms, and Politics ». *Media, Culture & Society* 41(2): 163-74.
- Pontille, David. 2016. *Signer ensemble. Contribution et évaluation en sciences*. Paris : Economica.
- Power, Michael. 2019. « Infrastructures of Traceability ». In *Research in the Sociology of Organizations*, éd. Martin Kornberger et al. Emerald Publishing Limited, 115-30. <https://www.emerald.com/insight/content/doi/10.1108/S0733-558X20190000062007/full/html> (7 février 2021).
- Przeworski, Adam. 1985. *Capitalism and Social Democracy*. Editions de la Maison des Sciences de l'Homme. Paris: Cambridge University Press.
- Quéré, Louis. 1989. « Les boîtes noires de Bruno Latour ou le lien social dans la machine ». *Réseaux* 7(36): 95-117.

Bibliographie

- Raskin, Max. 2017. « The Law And Legality Of Smart Contracts ». https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166 (13 février 2021).
- Reijers, Wessel, et Mark Coeckelbergh. 2018. « The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies ». *Philosophy & Technology* 31(1): 103-30.
- Rios-Bordes, Alexandre. 2018. *Les savoirs de l'ombre*. Paris : éditions EHESS.
- Rochet, Jean-Charles, et Jean Tirole. 2003. « Platform Competition in Two-Sided Markets ». *Journal of the European Economic Association* 1(4): 990-1029.
- Rosenblat, Alex, et Luke Stark. 2016. « Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers ». *International Journal of Communication* 10: 3758-94.
- Rossi, Julien, Francesca Musiani, et Lucien Castex. 2022. « La gouvernance d'Internet, entre infrastructures et espaces socio-politiques: apports de la recherche: Introduction par les coordinateurs du dossier ». *Terminal* (132-133). <http://journals.openedition.org/terminal/8210> (7 octobre 2022).
- Rouvroy, Antoinette. 2011. « Technology, virtuality and utopia: governmentality in an age of autonomic computing ». In *Law, human agency and autonomic computing : the philosophy of law meets the philosophy of technology*, éd. M Hildebrt et A Rouvroy. London: Routledge, 119-40.
- Rouvroy, Antoinette, et Thomas Berns. 2013. « Gouvernamentalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation ? » *Réseaux* 177(1): 163.
- Samuelson, Paul A. 1954. « The Pure Theory of Public Expenditure ». *The Review of Economics and Statistics* 36(4): 387.
- Shier, Charlie et al. 2017. « Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack ». *SSRN Electronic Journal*. <https://www.ssrn.com/abstract=3014782> (15 octobre 2021).
- Simondon, Gilbert. 1958. *Du mode d'existence des objets techniques*. Paris: Éditions Aubier-Montaigne.

Bibliographie

- Smith, Adam. 1776. *La richesse des nations*. London : W. Strahan and T. Cadell.
- Star, Susan Leigh. 1999. « The Ethnography of Infrastructure ». *American Behavioral Scientist* 43(3): 377-91.
- Steiner, Pierre. 2010. « Interaction et transaction: quelques enjeux pragmatistes pour une conception relationnelle de l'organisme ». *chromatikon* 6: 203-13.
- Supiot, Alain. 2013. *Cours: Du gouvernement par les lois à la gouvernance par les nombres*. Collège de France.
- . 2015. « La Gouvernance par les nombres ». Paris : Seuil.
- Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy*. First edition. Beijing : Sebastopol, CA: O'Reilly.
- Swartz, Lana. 2015. « Blockchain Dreams: Imagining Techno-Economic Alternatives After Bitcoin ». https://llaannaa.com/papers/Swartz_Blockchain_Dreams.pdf (12 février 2021).
- Tadjeddine, Yamina. 2021. « Souveraineté monétaire et financiarisation ». *Revue française de finances publiques* (155).
- Tapscott, Don, et Alex Tapscott. 2016. *Blockchain Revolution How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin Publishing Group.
- Toledano, Joëlle, et Lionel Janin. 2018. « Les enjeux des blockchains ». France Stratégie.
- Treiblmaier, Horst. 2019. « Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies ». *Frontiers in Blockchain* 2: 3.
- Turing, Alan M. 1936. « On Computable Numbers, With An Application To The Entscheidungsproblem ». *Proceedings of the London Mathematical Society* s2-42(1): 230-65.
- Varenne, Franck. 2016. « Histoire de la modélisation : quelques jalons ». In *Actes du colloque Modélisation succès et limites*, Paris, 9-36.
- Vidan, Gili, et Vili Lehdonvirta. 2019. « Mine the Gap: Bitcoin and the Maintenance of Trustlessness ». *New Media & Society* 21(1): 42-59.

Bibliographie

- Villeval, Marie Claire. 2010. « Quand le marché ne suffit plus : biens publics et coopération conditionnelle »: *Idées économiques et sociales* 161(3): 6-14.
- Volckart, Oliver, et Antje Mangels. 1999. « Are the Roots of the Modern Lex Mercatoria Really Medieval? » *Southern Economic Journal* 65(3): 427.
- Wagner, Pierre. 2005. « Wittgenstein et les machines de Turing ». *Revue de métaphysique et de morale* 2(46): 181-96.
- Werbach, Kevin, et Nicolas Cornell. 2017. « Contracts Ex-Machina ». *Duke Law Journal* 67: 70.
- Wiener, Norbert. 1948. *Cybernetics: or Control and Communication in the Animal and the Machine*. second edition. Cambridge, MA: The MIT Press.
- Williamson, Oliver. 1979. « Transaction cost economics: the governance of contractual relations ». *Journal of Law and Economics* 2(22): 233-61.
- Winner, Langdon. 1980. « Do Artifacts Have Politics? » *Daedalus* 109(1). <http://www.jstor.org/stable/20024652> (21 mars 2019).
- . 1997. « Cyberlibertarian Myths and the Prospects for Community ». *ACM SIGCAS Computers and Society* 27(3): 14-19.
- Wright, Aaron, et Primavera De Filippi. 2015. « Decentralized Blockchain Technology and the Rise of Lex Cryptographia ». *SSRN Electronic Journal*. <https://www.ssrn.com/abstract=2580664> (5 mars 2019).
- Zavolokina, Liudmila, Mateusz Dolata, et Gerhard Schwabe. 2016. « The FinTech Phenomenon: Antecedents of Financial Innovation Perceived by the Popular Press ». *Financial Innovation* 2(1): 16.
- Zelizer, Viviana A. Rotman. 1994. *The Social Meaning of Money*. New York: BasicBooks.
- Zook, Matthew A., et Joe Blankenship. 2018. « New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance ». *Geoforum* 96: 248-55.
- Zook, Matthew, et Michael H. Grote. 2020. « Initial Coin Offerings: Linking Technology and Financialization ». *Environment and Planning A: Economy and Space* 52(8):

Bibliographie

1560-82.

Sources

- Accenture. 2017. « Blockchain. Reengineering The Media Value Chain ». <https://www.accenture.com/acnmedia/PDF-132/Accenture-Blockchain-Media-Report.pdf>.
- ADAN, et KPMG. 2022. « Synthèse du rapport “Structuration du secteur et adoption par le grand public” ». <https://assets.kpmg.com/content/dam/kpmg/fr/pdf/2022/02/fr-executive-summary-la-crypto-en-france.pdf>.
- Adarme, Nicole. 2021. « Introducing MetaMask Institutional ». *ConsenSys Blog* (blog). 7 avril 2021. <https://consensys.net/blog/metamask/metamask-institutional/introducing-metamask-institutional/>.
- AFP. 2010. « Assange dénonce Visa, Mastercard et PayPal qui ont bloqué les virements ». *La Depeche*, 14 décembre 2010. <https://www.ladepeche.fr/article/2010/12/14/970008-wikileaks-assange-denonce-visa-mastercard-paypal-ont-bloque-virements.html>.
- Ames, Mark. 2015. « Google Is Helping to Fund the Group That’s Trying to Kill Obamacare in the Supreme Court ». *Pando Daily* (blog).
- AMF. 2018. « L’AMF publie la synthèse des réponses apportées à sa consultation publique sur les initial coin offerings (ICO) ». *Site internet de l’AMF* (blog). 22 février 2018. <https://www.amf-france.org/fr/actualites-publications/communiqués/communiqués-de-lamf/lamf-publie-la-synthèse-des-réponses-apportées-sa-consultation-publique-sur-les-initial-coin>.
- . 2019. « Vers un nouveau régime pour les crypto-actifs en France ». 15 avril 2019. <https://www.amf-france.org/fr/actualites-publications/actualites/vers-un-nouveau-regime-pour-les-crypto-actifs-en-france>.
- Apantes, Karine. 2018. « Et J.R. Willett créa l’ICO ». *Journal du Coin* (blog). 26 août 2018. <https://journalducoin.com/defi/jr-willett-createur-ico-portrait/>.
- Atmani, Mehdi. 2014. « Stephan Tual: «Ethereum, c’est le Web sans les serveurs» ». *Le Temps*, 24 octobre 2014. <https://www.letemps.ch/no-section/stephan-tual-ethereum-cest-web-serveurs>.

Sources

- AXA. 2017. « AXA se lance sur la Blockchain avec fizzy ». 13 septembre 2017. <https://www.axa.com/fr/magazine/axa-se-lance-sur-la-blockchain-avec-...1>.
- Bains, Pavel. 2018. « Bluzelle A Decentralized Database For The Future. Whitepaper V1.4 ». <https://whitepaperdatabase.com/bluzelle-blz-whitepaper/>.
- Balanc3. 2017. « Balanc3 Showcases Financial Statements for Gnosis, Aragon and Digix ». *ConsenSys Media* (blog). 6 octobre 2017. <https://media.consensys.net/balanc3-unveils-financial-statements-for-gnosis-aragon-and-digix-e57888add4ee>.
- . 2018. « First Live Demo of a Digital Asset Accounting Platform ». *ConsenSys Media* (blog). 8 mai 2018. <https://medium.com/consensys-media/first-live-demo-of-a-digital-asset-accounting-platform-fb8e2d152592>.
- Barlow, John Perry. 1996. « A Declaration of the Independence of Cyberspace ». *Electronic Frontier Foundation* (blog). 8 février 1996.
- Bercy Infos. 2022. « Crypto-monnaies, crypto-actifs... Comment s’y retrouver ? » Ministère de l’économie et des finances français. *Épargne et investissements mobiliers* (blog). 20 avril 2022. <https://www.economie.gouv.fr/particuliers/cryptomonnaies-cryptoactifs>.
- btc.com. 2022. « Pool Distribution ». btc.com. 5 février 2022. https://btc.com/stats/pool?pool_mode=day.
- Butcher, Mike. 2021. « ConsenSys Raises \$65M from JP Morgan, Mastercard, UBS to Build Infrastructure for DeFi ». *Techcrunch*, avril. <https://techcrunch.com/2021/04/13/consensys-raises-65m-from-jp-morgan-mastercard-ubs-to-build-infrastructure-for-defi/>.
- Buterin, Vitalik. 2012. « WordPress Accepts Bitcoin ». 2012.
- . 2013. « Ethereum Whitepaper ». 2013. <https://ethereum.org/en/whitepaper>.
- . 2014a. « So where did the name Ethereum come from? » *Ethereum Community Forum*. https://wayback.archive-it.org/16516/20210628224915/https://forum.ethereum.org/discussion/comment/3389#Comment_3389.
- . 2014b. « Ethereum: A Next-Generation Smart Contract and Decentralized

Sources

- Application Platform », https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf.
- . 2014c. « Launching the Ether Sale ». *Ethereum Foundation's blog* (blog). 22 juillet 2014. <https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/>.
- . 2017a. « The Meaning Of Decentralization ». *Medium* (blog). 6 février 2017. <https://medium.com/@VitalikButerin/the-meaning-of-decentralization>.
- . 2017b. « Notes on Blockchain Governance ». *Vitalik Buterin's website* (blog). 17 décembre 2017. <https://vitalik.ca/general/2017/12/17/voting.html>.
- . 2018. « Governance, Part 2: Plutocracy Is Still Bad ». *Vitalik Buterin's website* (blog). 28 mars 2018. <https://vitalik.ca/general/2018/03/28/plutocracy.html>.
- . 2019a. « On Collusion ». *Vitalik Buterin's website* (blog). 3 avril 2019. <https://vitalik.ca/general/2019/04/03/collusion.html>.
- . 2019b. « Developer incentivization: in-protocol contract author fee rebates ». *https://ethresear.ch* (blog). 22 septembre 2019. <https://ethresear.ch/t/developer-incentivization-in-protocol-contract-author-fee-rebates/6179>.
- . 2021. « Moving beyond coin voting governance ». *Vitalik Buterin's website* (blog). 16 août 2021. <https://vitalik.ca/general/2021/08/16/voting3.html>.
- Canton, Ben. 2022. « Les dons encombrants de FTX mettent les politiques US dans l'embarras ». *Le Journal du Coin*, 14 décembre 2022. <https://journalducoin.com/exchanges/dons-encombrants-ftx-politiques-us-embarras/>.
- Carmichael, Joe. 2016. « Meet Ethereum, the “World Computer” That May Power the Future ». *Inverse* (blog). 30 mars 2016. <https://www.inverse.com/article/13436-meet-ethereum-the-world-com>.
- CFTC. 2019. « IN CASE YOU MISSED IT: Chairman Tarbert Comments on Cryptocurrency Regulation at Yahoo! Finance All Markets Summit ». *cftc.gov* (blog). 10 octobre 2019. <https://www.cftc.gov/PressRoom/PressReleases/8051-19>.
- Clement, Alexandre. 2019. « fizzy by AXA: Ethereum Smart Contract in details ». *Medium*

Sources

- (blog). 24 mai 2019. <https://medium.com/@humanGamepad/fizzy-by-axa-ethereum-smart-contract-in-details-40e140a9c1c0>.
- ConsenSys. 2019a. « The Dauriel Network: Nouvelle solution Ethereum pour les Security Token ». Meetup.com. *ConsenSys Paris Ethereum & Blockchain Meetup* (blog). 2019. <https://www.meetup.com/fr-FR/ConsenSysParis/events/257477115/>.
- . 2019b. « Get to Know the ConsenSys Mesh ». *Medium* (blog). 1 mai 2019. <https://medium.com/@ConsenSys/get-to-know-the-47-projects-that-make-up-the-consensys-mesh-478b7d3028c1>.
- . 2019c. « ConsenSys Monthly Report — May 2019 ». *ConsenSys Media* (blog). 3 juin 2019. <https://media.consenSys.net/consensys-monthly-report-may-2019-9b8e449dc01f>.
- . 2019d. « Infura Launches Infura+ for Improved Ethereum Infrastructure Support ». *ConsenSys Blog* (blog). 17 juillet 2019. <https://consensys.net/blog/press-release/press-release-infura-a-consensys-company-launches-infura-for-improved-ethereum-infrastructure-support/>.
- . 2019e. « Infura Launches New Infura+ Subscription Service ». *ConsenSys Media* (blog). 18 juillet 2019. <https://media.consenSys.net/infura-launches-new-infura-subscription-service-bdf9e6855b44>.
- . 2019f. « One Million Ethereum Developers: Five ConsenSys Announcements from Devcon 5 ». 10 octobre 2019. <https://media.consenSys.net/one-million-ethereum-developers-five-consensys-announcements-from-devcon-5-28520ce63d73>.
- . 2020. « ConsenSys Acquires Truffle Suite ». *ConsenSys* (blog). 17 novembre 2020. <https://consensys.net/blog/press-release/consensys-acquires-truffle-suite/>.
- . 2021a. « ConsenSys Raises \$65 Million to Accelerate Convergence Of Traditional And Decentralized Finance ». 13 avril 2021. <https://consensys.net/blog/press-release/consensys-raises-65-million-to-accelerate-convergence-of-traditional-and-decentralized-finance/>.
- . 2021b. « MetaMask Surpasses 21 Million MAUs as ConsenSys Raises \$200 Million to Make Web3 Universally Easy to Use, Access, and Build On ». *ConsenSys Blog* (blog). 17 novembre 2021. <https://consensys.net/blog/press->

Sources

[release/metamask-surpasses-21-million-maus-as-consensys-raises-200-million-to-make-web3-universally-easy-to-use-access-and-build-on/](#).

Dawson, Rob, et Meredith Baxter. 2019. « Announcing Hyperledger Besu ». *Hyperledger* (blog). 29 août 2019. <https://www.hyperledger.org/blog/2019/08/29/announcing-hyperledger-besu>.

De La Roche, Zoé. 2020. « ConsensSys est désormais propriétaire de Metamask ». *Cointribune*, 4 septembre 2020. <https://www.cointribune.com/consenssys-est-desormais-propretaire-de-metamask/>.

Deloitte, et Monetary Authority of Singapore. 2016. « The future is here. Project Ubin: SGD on Distributed Ledger ». <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin--SGD-on-Distributed-Ledger.pdf>.

Digix Writer. 2016a. « DigixDAO — Governance / Reward claiming Process ». *Medium* (blog). 23 avril 2016. <https://medium.com/@Digix/digixdao-governance-reward-claiming-process-583d06c93956>.

———. 2016b. « Digix does not recognise DGD classic. DGD will stay on the proFork chain. » *Medium* (blog). 27 juillet 2016. https://www.reddit.com/r/digix/comments/4uvebf/we_do_not_recognise_dgd_classic_dgd_will_stay_on/.

———. 2017. « ANN: Digix closes 1.25mio USD seed investment round with Global Brain and Fenbushi Capital ». *Medium* (blog). 29 novembre 2017. <https://medium.com/@Digix/ann-digix-closes-1-25mio-usd-seed-investment-round-with-global-brain-and-fenbushi-capital-85d3d5bc2cfc>.

———. 2018. « DigixDAO Governance Model — Update #4 ». *Medium* (blog). 5 juin 2018. <https://medium.com/@Digix/digixdao-governance-model-update-4-2f92798242bd>.

Electric Capital. 2019. « Electric Capital Developer Report (H2 2018) ». *Medium* (blog). 7 mars 2019. <https://medium.com/electric-capital/dev-report-476df4ff1fd2>.

Ethereum France. 2020. « EthCC : Ethereum Community Conference ». Ethereum France. 2020. <https://www.ethereum-france.com/ethcc-ethereum-community-conference/>.

Sources

- ethereum.org. 2022. « Smart Contract Libraries ». ethereum.org. 10 janvier 2022. <https://ethereum.org/en/developers/docs/smart-contracts/libraries/>.
- Eudes, Yves. 2014. « L'ether, la future monnaie qui vaut déjà des millions ». *Le Monde* (blog). 6 octobre 2014. https://www.lemonde.fr/pixels/article/2014/10/07/l-ether-la-future-monnaie-qui-vaut-deja-des-millions_4501940_4408996.html.
- Eufemio, AC, KC Chng, et S Djie. 2016. « Digix's Whitepaper: The Gold Standard in CryptoAssets. Version 1.03 ». <http://digix.io/whitepaper>.
- Field, Matan. 2015. « Backfeed ». Présenté à Devcon 1, novembre. <https://archive.devcon.org/archive/watch/1/backfeed/?tab=YouTube>.
- Finlay, Dan. 2020. « Evolving our License for the Next Wave of MetaMask Users ». *Medium* (blog). 21 août 2020. <https://medium.com/metamask/evolving-our-license-for-the-next-wave-of-metamask-users-81b0b494c09a>.
- Gartner. 2015. « Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor ». <https://www.gartner.com/en/newsroom/press-releases/2015-08-18-gartners-2015-hype-cycle-for-emerging-technologies-identifies-the-computing-innovations-that-organizations-should-monitor>.
- . 2016. « Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage ». <https://www.gartner.com/en/newsroom/press-releases/2016-08-16-gartners-2016-hype-cycle-for-emerging-technologies-identifies-three-key-trends-that-organizations-must-track-to-gain-competitive-advantage>.
- . 2017. « Top Trends in the Gartner Hype Cycle for Emerging Technologies 2017 ». <https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017>.
- . 2018. « 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018 ». <https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018>.
- Havilland, Paul de. 2019. « The Ethereum Token Ecosystem Is Thriving ». *CryptoBriefing* (blog). 13 novembre 2019. <https://cryptobriefing.com/ethereum-token-ecosystem-thriving/>.

Sources

- Hollander, Luit. 2020. « History of Ethereum Hard Forks ». *Medium* (blog). 4 mai 2020. <https://medium.com/mycrypto/the-history-of-ethereum-hard-forks-6a6dae76d56f>.
- Hughes, Eric. 1993. « A Cypherpunk's Manifesto ». *activism.net* (blog). 9 mars 1993. <https://www.activism.net/cypherpunk/manifesto.html>.
- Idle, Elaine. 2016. « Stick a Fork in Ethereum ». *Elaine's Idle Mind* (blog). 18 juillet 2016. <https://elaineou.com/2016/07/18/stick-a-fork-in-ethereum/>.
- Infura. 2019. « Infura has officially been acquired by ConsenSys ». *Infura Blog* (blog). 4 octobre 2019. <https://blog.infura.io/post/infura-has-officially-been-acquired-by-consensys-e6ac5d27afa>.
- . 2023. « Infura Transactions The easiest way to transact on Web3 ». 2023. <https://www.infura.io/product/ethereum/transactions-itx>.
- Irrera, Anna. 2017a. « JPMorgan, Microsoft, Intel and others form new blockchain alliance ». *Reuters*, 27 février 2017. <https://www.reuters.com/article/us-ethereum-enterprises-consortium-idUSKBN1662K7>.
- . 2017b. « JPMorgan Chase & Co leaves blockchain consortium R3 ». *Reuters*, 27 avril 2017. <https://www.reuters.com/article/us-jpmorgan-r3-idUSKBN17T2T4>.
- . 2020. « Exclusive: JPMorgan in Talks to Merge Blockchain Unit Quorum with Startup ConsenSys - Sources ». *Reuters*, 11 février 2020. <https://www.reuters.com/article/us-jp-morgan-blockchain-exclusive/exclusive-jpmorgan-in-talks-to-merge-blockchain-unit-quorum-with-startup-consensys-sources-idUSKBN2051AW>.
- KPMG France. 2021. « Blockchain Partner rejoint KPMG France ». 15 mars 2021. <https://home.kpmg/fr/fr/home/media/press-releases/2021/03/blockchain-partner-rejoint-kpmg.html>.
- Kirsner, Scott. 1998. « The Legend of Bob Metcalfe ». *Wired*: 22.
- Laloux, Frédéric. 2014. *Reinventing Organizations. A . À Guide to Creating Organizations Inspired by the Next Stage of Human Consciousness*. Nelson Parker.
- . 2016. *Reinventing Organizations. An Illustrated Invitation to Join the Conversation on Next-Stage Organizations*. Nelson Parker.

Sources

- Le Vote Officiel. 2018. « Le Vote par Orange ». <https://vimeo.com/240969442>.
- Liao, Shannon. 2018. « John McAfee reveals he charges \$105,000 per promotional cryptocurrency tweet ». *The Verge* (blog). 2 avril 2018. <https://www.theverge.com/2018/4/2/17189880/john-mcafee-bitcoin-cryptocurrency-twitter-ico/>.
- Maffock, Junie. 2020. « JPMorgan pourrait mener une levée de fonds de \$50M pour ConsenSys », 14 août 2020. <https://cryptoast.fr/jpmorgan-pourrait-mener-une-leeve-de-fonds-de-50m-pour-consensys/>.
- Mauduit, Laurent. 2022. « Cryptomonnaies : une plainte contre Binance éclabousse les autorités françaises ». *Mediapart*, 19 décembre 2022. <https://www.mediapart.fr/journal/economie-et-social/191222/cryptomonnaies-une-plainte-contre-binance-eclabousse-les-autorites-francaises>.
- McGlynn, Daniel, réal. 2019. *Crypto Bites : A chat with Ethereum Founder Vitalik Buterin*. <https://www.abra.com/blog/crypto-bites-a-chat-with-ethereum-founder-vitalik-buterin/>.
- Mesh. 2023. « What is ConsenSys MESH? » *mesh.xyz* (blog). 6 janvier 2023. <https://www.mesh.xyz/insights/consensys-mesh>.
- Metamask. 2021. « At the moment, some falsehoods about MetaMask are circulating widely, and we want to set a few things straight »: *Twitter* (blog). 21 août 2021. <https://twitter.com/MetaMask/status/1428904438719139853>.
- Miller, Philippe. 2022. « Tradingducoin.com: 10 Millions D'euros Bloqués Chez FTX ». *Warning Trading* (blog). 17 novembre 2022. <https://www.warning-trading.com/enquetes-et-decryptages/tradingducoin-ftx/>.
- Monaghan, Angela. 2017. « Bitcoin is a fraud that will blow up, says JP Morgan boss ». *The Guardian*, 13 septembre 2017. <https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers>.
- Murarka, Neeraj. 2017. « Difference between Bluzelle and IPFS/Filecoin: Data vs Files ». *Medium* (blog). 17 octobre 2017. <https://blog.bluzelle.com/how-is-bluzelle-different-from-ipfs-filecoin-storj-sia-and-ethereums-swarm-1d1d792658f8>.

Sources

- Nakamoto, Satoshi. 2008. « Bitcoin: A Peer-to-Peer Electronic Cash System ». <https://bitcoin.org/bitcoin.pdf>.
- Nilson Report. 2022. « Global Network Cards — Purchase Transactions ». *Nilson Report* (blog). août 2022. https://nilsonreport.com/research_featured_chart.php.
- Orange, Martine. 2022. « La France cède aux sirènes de la cryptomonnaie et accueille le sulfureux Binance à bras ouverts ». *Mediapart*, 10 juin 2022. <https://www.mediapart.fr/journal/economie/100622/la-france-cede-aux-sirenes-de-la-cryptomonnaie-et-accueille-le-sulfureux-binance-bras-ouverts>.
- Pazaitis, Alex, et Primavera De Fili. s. d. « The Illustrative Case of Backfeed », 31.
- PegaSys. 2019. « [On-Demand] PegaSys Plus: Ensure Your Blockchain Solution is Production Ready ». *ConsenSys Pages* (blog). 2019. https://pages.consensys.net/pegasys_plus_launch.
- phyro. 2018. « The DAO is History... or is it? » *Medium* (blog). 14 mai 2018. <https://medium.com/coinmonks/the-dao-is-history-or-is-it-47a6f457338a>.
- Quittner, Josh. 2020. « More Layoffs at ConsenSys ». *Decrypt*, 20 avril 2020. <https://decrypt.co/26131/more-layoffs-at-consensys>.
- Sanders, R. 2018. « Crypto's Social Media Scammers (and How to Fight Back) ». *Medium* (blog). 2018. <https://medium.com/cipherblade/cryptos-social-media-scammers-and-how-to-fight-back-1abede525997>.
- Satoshi Nakamoto Institute. 2021. « Literature ». *Satoshi Nakamoto Institute* (blog). 2021. <https://nakamotoinstitute.org/literature/>.
- SG Innovate. 2017. « SGInnovate Facts Sheet – 7 Aug 2017 ». <https://www.sginnovate.com/sites/default/files/SGInnovate%20Factsheet%20-%207%20Aug%202017.pdf>.
- Stateofthedapps. 2021. « Explorer les applications décentralisées ». 2021. www.stateofthedapps.com.
- Stilmant, André. 2019. « Protocole ». *Bitcoin.fr* (blog). 6 avril 2019. <https://bitcoin.fr/protocole/>.

Sources

- Takkal Bataille, Adli, et Jacques Favier. *Bitcoin La monnaie acéphale*. Paris : CNRS Editions.
- The Bounties Network. 2019. « Smart Contracts in Solidity to serve as a Standard for Bounties for EVM dApps ». *Github* (blog). 2019. <https://github.com/Bounties-Network/StandardBounties>.
- The Economist. 2015. « The trust machine ». *The Economist*, 31 octobre 2015. <https://www.economist.com/leaders/2015/10/31/the-trust-machine>.
- Tomescu, Alin, et Srinivasa Devadas. 2016. « Nakamoto Blockchains How proof-of-work consensus and Bitcoin really work ». juin 27.
- Ulieru, Michaela. 2016. « Blockchain: what it is, how it really can change the world ». *World Economic Forum* (blog). 23 juin 2016. <https://www.weforum.org/agenda/2016/06/the-blockchain/>.
- Victor, Jon. 2019. « ConsenSys Seeks \$200 Million From Investors After Bumpy Year ». *The Information*, 15 avril 2019. <https://www.theinformation.com/articles/consensus-seeks-200-million-from-investors-after-bumpy-year>.
- Villeroy de Galhau, François. 2017. « Déclaration : “Le bitcoin n’est en rien une monnaie, ou même une crypto monnaie.” » In . Pékin. <https://www.banque-france.fr/intervention/declaration-le-bitcoin-nest-en-rien-une-monnaie-ou-meme-une-crypto-monnaie>.
- Ward, Edward. 2018. « DigixDAO ». [https://messari.github.io/research/profiles/DigixDAO\(DGD\).pdf](https://messari.github.io/research/profiles/DigixDAO(DGD).pdf).
- Wardzala, Clément. 2020a. « ConsenSys acquiert Quorum, la plateforme blockchain de JPMorgan ». *Cryptoast*, 6 août 2020. <https://cryptoast.fr/consensus-acquiert-quorum-plateforme-blockchain-jpmorgan/>.
- . 2020b. « Metamask met à jour sa licence pour saisir les opportunités commerciales ». *Cryptoast*, 24 août 2020. <https://cryptoast.fr/metamask-met-a-jour-licence-opportunités-commerciales/>.
- Wikipedia. 2023. « London bullion market ». *Wikipedia*. Consulté le 15 mars 2023. https://en.wikipedia.org/wiki/London_bullion_market.

Sources

Wood, Gavin. 2014. « Ethereum: A Secure Decentralised Generalised Transaction Ledger ». <https://ethereum.github.io/yellowpaper/paper.pdf>.

Zamfir, Vlad. 2017. « Against on-chain governance ». *Medium* (blog). 1 décembre 2017. https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca.

Annexes

Annexe 1 – Épisodes de terrain hors ligne

Le tableau suivant résume mes différents épisodes d'enquête sur la période retenue pour ce manuscrit : de février 2018 à mars 2020. Tous les épisodes listés n'ont pas été directement mobilisés dans le manuscrit ; je les mentionne, car ils ont joué dans l'écriture, au moins indirectement.

| # | Date | Intitulé | Type | Durée indicative |
|----|------------|--|------------------|------------------|
| 1 | 2018/02 | Attores / Indorse (Singapour) | Entretien | 1 heure |
| 2 | 2018/02 | Averspace (Singapour) | Entretien | 1 heure |
| 3 | 2018/02 | Bluzelle (Singapour) | Entretien | 1 heure |
| 4 | 2018/02 | ConsenSys (Singapour) | Entretien | 1 heure |
| 5 | 2018/02 | Digix (Singapour) | Entretien | 1 heure |
| 6 | 2018/02 | Energy Market Authority (Singapour) | Entretien | 1 heure |
| 7 | 2018/02 | IBM (Singapour) | Entretien | 1 heure |
| 8 | 2018/02 | Kyber Networks (Singapour) | Entretien | 1 heure |
| 9 | 2018/02 | KYCK! (Singapour) | Entretien | 1 heure |
| 10 | 2018/02 | Lala World (Singapour) | Entretien | 1 heure |
| 11 | 2018/02 | Popety (Singapour) | Entretien | 1 heure |
| 12 | 2018/02 | R3 (Singapour) | Entretien | 1 heure |
| 13 | 2018/02 | SG Innovate (Singapour) | Entretien | 1 heure |
| 14 | 2018/02 | SGX (Singapour) | Entretien | 1 heure |
| 15 | 2018/02 | SP Group (Singapour) | Entretien | 1 heure |
| 16 | 2018/02 | TenX (Singapour) | Entretien | 1 heure |
| 17 | 2018/02 | VeChain (Singapour) | Entretien | 1 heure |
| 18 | 2018/02/19 | Impressions passants sur un graph Bitcoin | Micro-entretiens | 1 heure |
| 19 | 2018/03/26 | Responsable Blockchain Conseil (anonymisé) | Entretien | 30 minutes |
| 20 | 2018/04/05 | Jacques Favier (Bitcoin) | Entretien | 1 heure |
| 21 | 2018/04/09 | « Repas du Coin » (Bitcoin) à Paris | Observation | 3 heures |
| 22 | 2018/04/19 | Conférence Craig Wright (Bitcoin) | Entretien | 1,5 heures |
| 23 | 2018/05/24 | Salon VivaTech | Observation | 2,5 journées |
| 24 | 2018/05/30 | « Repas du Coin » (Bitcoin) à Bordeaux | Observation | 1 journée |
| 25 | 2018/06/05 | IBM Blockchain Summit | Observation | 1 journée |
| 26 | 2018/06/05 | Meetup Ethereum Regulation | Observation | 2 heures |
| 27 | 2018/06/21 | Club Finance : Actualités (anonymisé) | Observation | 3 heures |
| 28 | 2018/06/21 | Meetup Ethereum At Scale | Observation | 2 heures |
| 29 | 2018/07/06 | Présentation Stratégie Blockchain Orange | Observation | 1 heure |
| 30 | 2018/09/19 | France Stratégie Régulation Crypto-Actifs | Observation | 2 heures |
| 31 | 2018/10/09 | Meetup Ethereum 2.0 | Observation | 2 heures |

Annexes

| | | | | |
|----|------------|--|-------------|------------|
| 32 | 2018/10/17 | LeVote : Geoffrey | Entretien | 30 minutes |
| 33 | 2018/10/23 | Présentation Livre « Bitcoin Métamorphoses » | Observation | 1,5 heures |
| 34 | 2018/11/13 | Salon « Bercy Innov » (ministère) | Observation | 2 heures |
| 35 | 2018/11/14 | LeVote : Geoffrey | Entretien | 1 heure |
| 36 | 2018/11/15 | Meetup Future of Work | Observation | 2 heures |
| 37 | 2018/11/21 | ConsenSys Claire et Amélie | Entretien | 1 heure |
| 38 | 2018/11/21 | Mission Conseil, Service Public (anonymisé) | Entretien | 1 heure |
| 39 | 2018/11/23 | Armand (NXT) | Entretien | 1,5 heures |
| 40 | 2018/11/28 | Salon Blockchain Paris | Observation | 2 heures |
| 41 | 2018/12/04 | Réunion stratégique LeVote | Observation | 2 heures |
| 42 | 2018/12/07 | Mission Conseil en Service Public (anonymisé) | Entretien | 2 heures |
| 43 | 2018/12/13 | Club Finance : Actualités (anonymisé) | Observation | 3 heures |
| 44 | 2018/12/13 | Meetup ConsenSys Numérisation Actifs | Observation | 3 heures |
| 45 | 2018/12/19 | AG Asseth | Observation | 2 heures |
| 46 | 2018/12/19 | LeVote Entretien Fabrice | Entretien | 1 heure |
| 47 | 2018/12/19 | LeVote Entretien Salah | Entretien | 1 heure |
| 48 | 2018/12/20 | LeVote Présentation Point Interne Orange | Observation | 1 heure |
| 49 | 2019/01/04 | LeVote Entretien Denis | Entretien | 1,5 heures |
| 50 | 2019/01/31 | Meetup ConsenSys The Dauriel Network | Observation | 2 heures |
| 51 | 2019/02/05 | Club Finance : régulation cryptoactifs (anonymisé) | Observation | 2 heures |
| 52 | 2019/02/27 | Meetup ConsenSys Pantheon | Observation | 2 heures |
| 53 | 2019/03/06 | Meetup ConsenSys The Future of Web 3.0 | Observation | 2 heures |
| 54 | 2019/04/02 | Film Protocole (Bitcoin) | Observation | 4 heures |
| 55 | 2019/04/16 | Meetup ConsenSys Cercle & Co | Observation | 3 heures |
| 56 | 2019/05/16 | Meetup ConsenSys Entrepreneuria | Observation | 3 heures |
| 57 | 2019/05/16 | Salon VivaTech | Observation | 2 jours |
| 58 | 2019/05/23 | Meetup ConsenSys Decentralized Identity | Observation | 2 heures |
| 59 | 2019/06/06 | Meetup ConsenSys Tech Workshop | Observation | 2 heures |
| 60 | 2019/06/25 | Meetup ConsenSys Cloud & BC | Observation | 2 heures |
| 61 | 2019/07/09 | Logan (NXT) | Entretien | 1 heure |
| 62 | 2019/07/17 | Meetup ConsenSys pierre papier | Observation | 2 heures |
| 63 | 2019/07/22 | Logan (NXT) | Entretien | 30 minutes |
| 64 | 2019/08/08 | AGE Asseth | Observation | 3 heures |
| 65 | 2019/09/10 | Meetup Asseth Kleros | Observation | 2 heures |
| 66 | 2019/09/11 | EU Blockchain Observatory ConsenSys | Observation | 2 heures |
| 67 | 2019/09/12 | Meetup ConsenSys Dev Toolbox | Observation | 2 heures |
| 68 | 2019/09/23 | Arnaud | Entretien | 1,5 heures |
| 69 | 2019/11/07 | Club Finance : Blockchain (anonymisé) | Observation | 3 heures |
| 70 | 2019/11/20 | Meetup DeFi 2 | Observation | 2 heures |
| 71 | 2019/12/05 | AG Ethereum France + Debrief DevCon | Observation | 2 heures |
| 72 | 2019/12/12 | Meetup DeFi 3 | Observation | 2 heures |
| 73 | 2019/12/18 | Meetup DAO | Observation | 2 heures |
| 74 | 2020/01/09 | P2P Festival | Observation | 2 heures |

Annexes

| | | | | |
|----|------------|--------------------------------|-------------|-------------|
| 75 | 2020/01/10 | P2P Festival | Observation | 3 heures |
| 76 | 2020/01/11 | P2P Festival | Observation | 1 journée |
| 77 | 2020/01/12 | P2P Festival | Observation | 0,5 journée |
| 78 | 2020/01/15 | Meetup ConsenSys StableCoins | Observation | 2 heures |
| 79 | 2020/01/16 | Meetup DeFi4 | Observation | 2 heures |
| 80 | 2020/02/13 | Meetup DeFi5 | Observation | 2 heures |
| 81 | 2020/02/24 | Meetup Introduction à la DeFi | Observation | 2 heures |
| 82 | 2020/03/02 | Blockchain Week – Atka Web3 | Observation | 2 heures |
| 83 | 2020/03/02 | Blockchain Week – Joseph Lubin | Observation | 2 heures |
| 84 | 2020/03/02 | Blockchain Week – Kleros | Observation | 2 heures |
| 85 | 2020/03/03 | EthCC Day 1 | Observation | 1 journée |
| 86 | 2020/03/04 | EthCC Day 2 | Observation | 1 journée |
| 87 | 2020/03/05 | Blockchain Week – DAO Fest | Observation | 2 heures |
| 88 | 2020/03/05 | EthCC Day 3 | Observation | 1 journée |
| 89 | 2020/08/03 | Arnaud | Entretien | 1 heure |
| 90 | 2021/11/25 | Jean | Entretien | 1 heure |

Annexe 2 – Meetups

Ce tableau propose des détails sur un sous-ensemble d'épisodes d'enquête listés en Annexe 1 : les meetups (co)organisés par ConsenSys France entre juin 2018 et mars 2020.

| # 219 | Date | Titre de l'événement ²²⁰ | Lieu ²²¹ | Format | Orateurs ²²² |
|----------|-----------|--|----------------------------|---------------|--|
| 1 | juin 2018 | Government Blockchain Association event (*) | L'Antenne (75011) | Table-ronde | <ul style="list-style-type: none"> • Government Blockchain Association • Ledger • Association française des marchés financiers (AMAFI) • CoinHouse • Consultant en droit • Kramer Levin Avocats • European Securities and Markets Authority |
| 2 | juin 2018 | La Scalabilité d'Ethereum, aujourd'hui et demain (**) | Finance Innovation (75002) | Conf. | <ul style="list-style-type: none"> • Asseth |
| 3 | oct 2018 | ConsenSys Ask Me Anything - Ethereum 2.0: évolution ou révolution? | L'Antenne (75011) | Conf. | <ul style="list-style-type: none"> • PegaSys |
| 4 | nov 2018 | Future of Work : What about yours? | ConsenSys France (75001) | Table-ronde | <ul style="list-style-type: none"> • ConsenSys • Talent.io • Comet • Bounties Network |
| 5 | dec 2018 | Conférence : Blockchain & Numérisation des | Le Tripot Régnier (75015) | Tables-rondes | <ul style="list-style-type: none"> • ConsenSys (Direction France) • Economiste |

219 Les numéros soulignés correspondent à des événements dont l'annonce a été diffusée par mail, annoncés sur Internet mais qui n'étaient pas publiés sur la plateforme meetup.

220 Les titres sont donnés tels qu'ils apparaissaient sur le groupe Meetup de ConsenSys (<https://www.meetup.com/fr-FR/ConsenSysParis/events/past/>) ou sur la page de l'événement quand l'information était reçue par courriel directement. Les événements marqués par (*) organisé par la « Government Blockchain Association », (**) organisé par l'association Asseth, (+) en partenariat avec l'Institut Louis Bachelier, (++) co-organisé avec Paris EUROPLACE.

221 Sauf précision contraire entre parenthèses, ces événements avaient lieu en soirée.

222 Listés par ordre de nomination sur la page de présentation de l'événement ou par ordre de prise de parole.

Annexes

| | | | | | |
|----|------------|---|--------------------------|--------|---|
| | | actifs financiers (+) | | | <ul style="list-style-type: none"> • Direction Générale du Trésor • European Securities and Markets Authority • ConsenSys / ChainTech • Crypto Valley Association • Bredin Prat / ChainTech • Autorité des Marchés Financiers • ConsenSys (Relations Institutions) • Gide 255 • Société Générale • Asseth |
| 6 | jan 2019 | The Dauriel Network: Nouvelle solution Ethereum pour les Security Token | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • ConsenSys (Direction France) • ConsenSys (Product Lead) • ConsenSys (Product Manager) |
| 7 | fev 2019 | Taking Ethereum to production: Panthéon 1.0 Intro | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • PegaSys (Cofondateur) • PegaSys (Product Manager) |
| 8 | mars 2019 | The Future of Web 3.0 & Demo of new HTC Exodus Phone | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • HTC • Opera Crypto • ConsenSys (Direction France) |
| 9 | avril 2019 | Blockchains & Crypto : un état des lieux par la Communauté française | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • Asseth • Le Cercle du Coin • ChainTech • CryptoFR |
| 10 | mai 2019 | Entreprendre dans la Blockchain: Quelles clés pour réussir | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • CoinHouse • ChainTech / Blockchain Partners • ChainTech / ORWEL Avocats • Asseth • ConsenSys (Product Lead) |
| 11 | mai 2019 | L'identité Décentralisée: Quid des enjeux et des opportunités | ConsenSys France (matin) | Conf.s | <ul style="list-style-type: none"> • ConsenSys (Direction France) • ConsenSys (Government Strategy Lead) |
| | | | | Table- | <ul style="list-style-type: none"> • ConsenSys (Cryptographe) |

Annexes

| | | | | | |
|----|------------|---|-------------------------------------|---------------|---|
| | | | | ronde | <ul style="list-style-type: none"> • Bredin Prat Avocats • ConsenSys (Government Strategy Lead) |
| 12 | juin 2019 | {Tech Workshop} How to implement an ERC 1400 | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • ConsenSys (Product Lead) • ConsenSys (Product Manager) |
| 13 | juin 2019 | Build a blockchain architecture from A to Z: Tool Box and Experience Feedback | ConsenSys France | Table-ronde | <ul style="list-style-type: none"> • Amazon Web Service • Kaleido • ConsenSys |
| 14 | juill 2019 | {Blockchain Series} Quand la Blockchain rencontre le marché de la pierre papier (***) | ConsenSys France (matin) | Conf.s | <ul style="list-style-type: none"> • ConsenSys (Real Estate Lead) • Mata Capital |
| 15 | sep 2019 | How the EU is approaching the Financial Services transformation through Blockchain technology | ConsenSys France (matin) | Tables-rondes | <ul style="list-style-type: none"> • Gide 255 • Société Générale • ConsenSys • International Swaps and Derivatives Association • European Central Bank • Monerium • Kramer Levin • Groupe Casino • Central Bank of Lithuania |
| | | | | 'Battles' | <ul style="list-style-type: none"> • Fragmos Chain • Coinhouse • ConsenSys • Association française des marchés financiers (AMAFI) • Autorité des Marchés Financiers (AMF) |
| 16 | sep 2019 | Meetup "How to build a successful Blockchain product" | ConsenSys France | Conf.s | <ul style="list-style-type: none"> • Komgo • PegaSys • ConsenSys (Software Developer) • ConsenSys (Product Owner) |
| 17 | sep 2019 | Stablecoin Conference: Which ambitions for Europe? | La Fabrique Evéne-mentielle (75010) | Conf.s | <ul style="list-style-type: none"> • Banque de France - 1er Gouverneur Adjoint • Député |
| | | | | Tables-rondes | <ul style="list-style-type: none"> • ConsenSys (Direction France) • Paris EUROPLACE |

Annexes

| | | | | | |
|----|--------------|--|--------------------------------------|-----------------|---|
| | | | | | <ul style="list-style-type: none"> • TOBAM • ConsenSys (ex AMAFI) • Gide 255 • Banque de France • Maker DAO • Casino Group • Monerium • ConsenSys (Strategic Sales) |
| 18 | mars 2020 | Joe Lubin in Paris - The Ethereum Momentum: On the road to Product- Market Fit | Maison de la Mutualité (75005) | Interview | <ul style="list-style-type: none"> • ConsenSys (CEO et fondateur) • ConsenSys (Direction France) |
| | | | | Table- ronde | <ul style="list-style-type: none"> • LVMH • Covantis • Mata Capital |

Annexe 3 – Ethereum par un bord

Cette Annexe 3 est un document de travail que je propose comme un glossaire situé. Il raconte une prise de contact avec Ethereum par un de ses bords, mon navigateur Web, en détaillant le cours d'action dans lequel une transaction est validée. Je l'ai rédigé en 2018 comme une auto-ethnographie dans laquelle je discute avec un lecteur fictif, anticipant ses surprises qui, souvent, étaient également les miennes.

Faisant face au foisonnement de termes techniques apparaissant sur l'interface du *wallet* en ligne MyEtherWallet comme les *nodes* (nœuds), *blocks* (blocs), ou *hash*, j'y ai consigné ma compréhension de relations entre différentes entités peuplant l'infrastructure. Je l'ai enrichie de recherches sur les nœuds et sur un autre système de *wallet*, Metamask.

Avant de rédiger ce document, j'avais uniquement expérimenté l'usage des cryptoactifs *via* les plateformes d'échanges (*exchanges*), en l'occurrence Binance et Coinbase (pour des montants de quelques dizaines d'euros). Mais ces plateformes masquaient le fonctionnement du réseau auquel je souhaitais accéder. L'interface retenue permettait de mieux comprendre ce qu'il se passait.

Les pages qui suivent restituent ce document tel quel.

Qu'est-ce qu'Ethereum ? Le lecteur curieux aura peut-être interrogé son moteur de recherche préféré avec le mot-clé « ethereum ». La diversité des réponses est frappante. Parmi ces pages web, le lecteur pourra trouver des pages représentant des cours d'actifs (financiers), des forums de spécialistes ou de passionnés, des pages encyclopédiques, ou encore des sites présentant une forme « officielle »²²³. Ces derniers décrivent Ethereum comme un « ordinateur mondial »²²⁴, ou une « plateforme » qui permet de construire des

223 comme <http://www.ethereum.org> ou <http://www.ethereum-france.com>

224 <https://www.ethereum-france.com/quest-ce-que-lethereum/>, consulté le 2 octobre 2018

Annexes

« applications inarrêtables »²²⁵. Ethereum y est décrit comme un « réseau », et associé à différents termes peu parlants pour le lecteur non averti (parmi lesquels « blockchain »). De telles pages ont au moins deux points communs. D'une part, elles mobilisent un vocabulaire appartenant au champ lexical de l'informatique, que ce soit du développement web ou de l'architecture de systèmes et réseaux. D'autre part, toutes « parlent » d'Ethereum sans jamais le « montrer ». À la différence de services web habituels, Ethereum ne se réduit pas à un site web à partir duquel un utilisateur potentiel pourrait explorer une offre de services.

Appréhender Ethereum en pratique, c'est-à-dire sans se limiter à une analyse discursive, implique de chercher à « toucher » ou « voir » Ethereum. Dit pragmatiquement : comment accéder à Ethereum ? Comment interagir avec cet « ordinateur monde » ? Sur quel site web se rendre pour le découvrir ? Cette dernière question est à l'évidence cadrée par l'habitude d'interagir dans un mode client / serveur : le client (ici, le lecteur curieux qui interagit par le truchement de son navigateur web favori) cherche à se connecter à un serveur (ordinateur distant qui, à la demande d'un client, transmet par le réseau Internet des données qui sont présentées par le navigateur web du client) *via* le protocole http dont le rôle est de faire communiquer un client et un serveur sur le World Wide Web²²⁶. Cette habitude est insatisfaisante pour « accéder » à Ethereum : l' « ordinateur mondial » annoncé semble caché, en tous cas inaccessible par les pratiques habituelles du web. Le lecteur non seulement curieux mais aussi obstiné pourrait adapter sa recherche, par exemple « comment accéder à ethereum ». Les cinq premières réponses de Google à cette requête ont les titres suivants : « Créer et gérer votre compte d'ether (ETH) »²²⁷, « Comment miner de l'ether (ETH) – Windows »²²⁸, « portefeuille »²²⁹, « Tuto : Comment utiliser MyEtherWallet ? »²³⁰, « MyEtherWallet : Comment créer votre portefeuille Ethereum »²³¹. Dans tous ces résultats

225 <https://www.ethereum.org/>, consulté le 2 octobre 2018

226 Le World Wide Web (WWW) est une des applications d'Internet, parmi lesquelles les messageries électroniques, les messageries instantanées, ou le partage de fichier de pair-à-pair. Chacune de ses applications fonctionne avec un ensemble de protocoles informatiques ; http est le protocole du WWW.

227 <https://www.ethereum-france.com/creer-et-gerer-son-portefeuille-dether-en-2-minutes-avec-myetherwallet-com/>, consulté le 2 octobre 2018.

228 <https://www.ethereum-france.com/comment-miner-de-lether-eth-windows/>

229 <https://www.ethereum-france.com/tag/portefeuille/>

230 <https://cryptoast.fr/tutoriel-myetherwallet/>

231 <https://cryptogains.fr/1566-creez-portefeuille-ethereum-myetherwallet>

Annexes

figurent systématiquement les notions de « portefeuille » (ou en version anglaise « *wallet* ») ou d' « *ether* » qui apparaît comme une unité de « compte ». MyEtherWallet apparaît comme un outil capable de créer des « portefeuilles Ethereum ».

Les lignes qui suivent décrivent Ethereum en suivant mon propre parcours d'utilisateur tirant le fil esquissé aux paragraphes précédents. Par l'expérimentation de MyEtherWallet (MEW pour les prochaines occurrences), je décris les objets qui émergent dans mon interaction avec Ethereum médiée par MEW (1.). La description de ces objets permet d'appréhender des cours d'action entre un utilisateur et Ethereum, sans toutefois pouvoir « toucher » ou « voir » Ethereum autrement que par des médiateurs (objets décrits en 1., et sites web agissant comme interfaces) comme MEW, décrit par ses concepteurs comme un dispositif d' « interaction » avec Ethereum²³². La description des liens entretenus entre MEW et Ethereum est intéressante et permettra d'aborder l'architecture d'Ethereum par l'arrivée de nouveaux acteurs, les « nœuds » d'Ethereum (2.). Ces premières approches d'Ethereum mettent en évidence le rôle particulier des intermédiaires entre Ethereum et ses utilisateurs (3.).

1. L'utilisateur : un portefeuille responsable

Un utilisateur d'Ethereum est un portefeuille, ou *wallet*²³³. Dans cette section, je détaille mon parcours d'utilisateur qui découvre MEW pour créer un *wallet* en décrivant les différentes interfaces que je rencontre. De nombreux objets apparaissent au cours de ce parcours, souvent à connotation technique. Cette description les laisse émerger pour les appréhender tels qu'ils émergent dans le cours d'action (*via* MEW). Cette approche de l'interaction entre un utilisateur et Ethereum se veut « située » ; les objets qui apparaissent dans cette interaction particulière sont *de facto* formatés par MEW.

232 <https://www.myetherwallet.com/>

233 Les termes désignant des objets propres à Ethereum sont conservés dans leur version d'origine, en langue anglaise.

1.a. Accéder à MEW : l'utilisateur « responsable » de sa « sécurité »

La connexion au site web de MEW fait apparaître une fenêtre pop-up qui est reproduite sur la Figure 31. L'utilisateur y observe de nombreux avertissements, soulignés à grand renfort d'émoticônes et de variations typographiques. Il apprend non seulement qu'il s'expose à un risque de vol de ses fonds s'il s'aventurait sur un site de *phishing*²³⁴ ou s'il perdait sa *private key*, mais aussi qu'une telle situation serait irréversible ; l'utilisateur est lui seul « responsable » de sa « sécurité ». L'utilisateur est prévenu : ce nouvel objet, la *private key*, est d'emblée présentée comme un intermédiaire crucial entre l'utilisateur et ses fonds, susceptibles d'être volés en cas d'imprudence.

Qu'est-ce que MEW ? Cette première fenêtre (Figure 31) apporte des premiers éléments de réponse. Le service est qualifié d' « interface côté-client ». En langage de programmation web, cette expression²³⁵ désigne la vue d'un site web tel qu'il s'affiche dans le navigateur web, par opposition au site web « côté-serveur »²³⁶. MEW est décrit comme un site web destiné aux utilisateurs d'un service qu'il « interface » *via* un navigateur web. La visée de ce service est décrite sur la même fenêtre : l'utilisateur peut « interagir directement avec la *blockchain* » tout en restant en total « contrôle » de ses « *keys* » et de ses « *funds* ». MEW apparaît donc comme un intermédiaire entre d'une part un utilisateur équipé de *keys* et de *funds*, et d'autre part la *blockchain*.

234 L'hameçonnage, *phishing* ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte nationale d'identité, date de naissance, etc. En effet, le plus souvent, une copie exacte d'un site internet est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel où elle pensait se connecter. La victime va ainsi saisir ses codes personnels qui seront récupérés par celui qui a créé le faux site, il aura ainsi accès aux données personnelles de la victime et pourra dérober tout ce que la victime possède sur ledit site web. L'attaque peut aussi être réalisée par courrier électronique ou autres moyens électroniques.

235 Dont un synonyme est « *front-end* ».

236 Dite aussi « *back-end* ».

Annexes

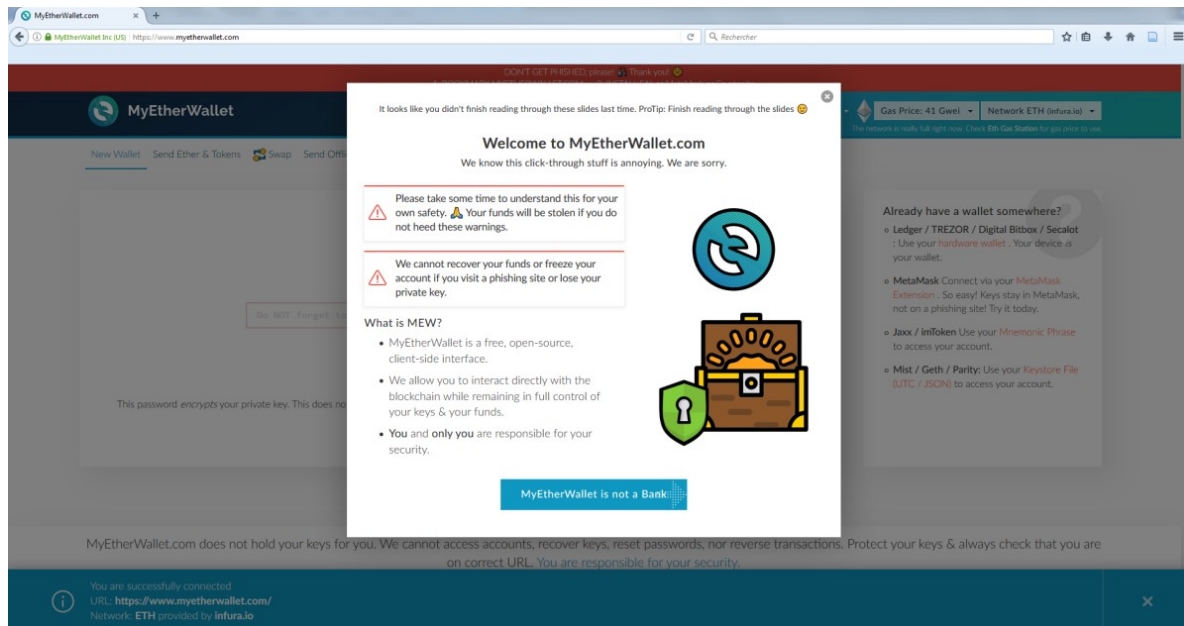


Figure 31 : Page d'accueil du site MyEtherWallet.com

Ce premier contact avec MEW fait émerger différents objets : *private key*, *keys*, *funds*, *blockchain*. Les trois premiers apparaissent comme médiateurs, la *blockchain* comme un correspondant de l'utilisateur. L'espace dans lequel s'engage l'utilisateur pour correspondre avec la *blockchain* est décrit comme dangereux : chacun est « responsable » de ses affaires.

1.b. Créer un « wallet » : s'équiper des « keys » pour gérer ses « Ethers » et ses « Tokens »

La page d'accueil de MEW, visible une fois la fenêtre présentée sur la Figure 31 fermée, invite l'utilisateur à créer un nouveau « *wallet* » en entrant un « *password* » (Figure A²³⁷). Une fois le *password* entré, le site invite à télécharger et sauvegarder un « *keystore* » (Figure B et contenu du *keystore* reproduit en Figure C). La *private key* apparaît alors à l'écran sous forme d'une suite de caractères alphanumériques (Figure D). Sur cette même page, MEW propose d'imprimer un « *paper wallet* » et de sauvegarder son « *address* ». Le *paper wallet* est une image (Figure 32) sur laquelle sont inscrites l'*address* ainsi que la *private key*, chacune présentée textuellement (la *private key* figurant sur le *paper wallet* est

237 Les nombreuses figures numérotées par des lettres sont renvoyées à la fin de cette Annexe pour ne pas alourdir le texte.

Annexes

bien identique à celle qui était affichée à l'écran, Figure D) et sous forme de QR Codes.



Figure 32 : Paper wallet

En choisissant de sauvegarder son *address* (« *Save your address* » sur la Figure D), l'utilisateur est invité à choisir entre différents formats proposés sous forme de liste (Figure E) précédée du texte suivant :

Your Address can also be known as you Account # or your Public Key. It is what you share with people so they can send you Ether or Tokens. (www.myetherwallet.com, consulté le 17/10/2018)

Cette phrase est intéressante à deux titres. D'une part, elle propose une première définition de l'*address* : ce qu'un utilisateur U partage avec d'autres utilisateurs pour que ces derniers puissent envoyer des *Ethers* ou des *Tokens* à U. D'autre part, l'*address* est un numéro de compte (« *account number* ») dont un synonyme est « *public key* ». Ce numéro de compte est « public » comme le terme *public key* le suggère : sa vocation est d'être communiqué aux utilisateurs susceptibles d'envoyer des *Ethers* ou des *Tokens* à l'utilisateur qui détient le *wallet* identifié par cette *address*.

Différents objets apparaissent dans le processus de création d'un *wallet* : *paper wallet*, *Ether*, *Tokens*, *password*, *keystore*. Le *paper wallet* est une représentation du *wallet* qui ne représente que l'*address* et la *private key*. Ce nouvel objet permet ainsi de préciser l'objet *wallet* : l'*address* et la *private key* définissent le *wallet*, qui est destiné à contenir des *Ethers* ou des *Tokens*. Ces derniers constituent les *funds* qui faisaient l'objet des avertissements observés en 1.a. et menacés par la perte ou le vol de la *private key*.

1.c. Interagir avec d'autres : générer une « transaction » et l'envoyer dans le « network »

Equippé de son *wallet*, l'utilisateur peut désormais chercher à envoyer des *Ethers* ou des *Tokens*. La page « *Send Ether ou Tokens* » demande à l'utilisateur de s'identifier en renseignant les informations sur son *wallet*. Étant donné les opérations préalablement conduites dans le cadre de ce parcours, l'utilisateur dispose de deux options : utiliser sa *private key* ou charger le fichier *keystore*. Ces deux options sont équivalentes pour la suite, mais l'utilisation du *keystore* permet de préciser cet objet. Après avoir chargé le fichier *keystore* sur MEW, l'utilisateur doit renseigner son *password*. Cette opération montre que le couple *private key / address* est équivalent au couple *keystore / password* pour s'identifier. Quelle que soit la solution retenue pour s'identifier (*private key* ou *keystore*), l'ambition de l'utilisateur est mise à l'épreuve par ce qui apparaît être une règle comptable de MEW : il n'est pas possible d'envoyer d'*Ether* ou de *Tokens* sans en disposer dans son *wallet* au préalable (Figure F). Pour le dire rapidement, MEW ne fait pas crédit.

Pour les besoins de l'exposé, un compte tiers a envoyé des *Ethers* dans le *wallet* créé au paragraphe 1.b. En actualisant la page décrite au paragraphe précédent ou en s'identifiant à nouveau *via* le menu « *Send Ether ou Tokens* » à l'aide de sa *private key* ou du *keystore*, on observe en effet que le *wallet* dispose d'un montant de 0.39821736 *Ether* (Figure G). Qui a envoyé ces *Ethers* sur le *wallet* de l'utilisateur, et quand ? La rubrique « *Transaction history* » de cette même page permet de répondre à ces questions. MEW redirige l'utilisateur vers le site d'EtherScan²³⁸ (Figure H) qui fait figurer le montant disponible sur ce *wallet* ainsi que l'historique des *transactions* qui l'ont alimenté (« *IN* » en vert sur la page). Cette vue est intéressante à différents titres. Premièrement et en réponse aux questions posées ci-dessus, l'utilisateur observe que ses 0.39821736 *Ether* proviennent du *wallet* identifié par l'*address* 0x4129D7521264Ce326c03D610E165fc9276649Da1 et que cette *transaction* date de 4 minutes dans le passé. Deuxièmement, l'utilisateur peut visualiser l'intégralité des *transactions* effectuées par le *wallet* émetteur uniquement à partir de son *address* (Figure I) ; aucune identification particulière n'est demandée, quiconque

238 <http://etherscan.io>

Annexes

renseignant l'*address* d'un *wallet* peut visualiser l'historique des *transactions* sur depuis la création de ce *wallet*. Troisièmement, il apparaît que les *transactions* sont numérotées par des *TxHash* et qu'à chacune est associé un *block*.

Pour effectuer sa première *transaction* en *Ether*, l'utilisateur souhaite rendre les 0.39821736 *Ether* disponibles sur son *wallet* à celle ou à celui qui utilise le *wallet* 0x4129D7521264Ce326c03D610E165fc9276649Da1. L'utilisateur renseigne l'*address* du destinataire, le montant envoyé en *Ether*, ainsi que la « Gas Limit »^{239,240} (Figure J). Une fois confirmée, cette première étape produit deux séries de caractères hexadécimaux (Figure K) : la *transaction* est « générée », désormais prête à être « envoyée ». Une fenêtre propose un récapitulatif de l'ensemble des informations qui composent la *transaction* avant la confirmation de son « envoi » (Figure L). Certaines informations composant cette *transaction* sont attendues, notamment : *address* émettrice des *Ethers* (l'utilisateur), *address* du destinataire des *Ethers*, montant d'*Ether* envoyé, solde du *wallet* en *Ether*, et différentes informations relatives au coût de la *transaction* (*gas*). D'autres informations complètent la *transaction* à confirmer : *nonce*²⁴¹ et *network*, ici « infura.io ». Une fois l'envoi de la confirmation confirmé par l'utilisateur, la *transaction* est augmentée d'un *TxHash*²⁴², visible sur la Figure M. Le *TxHash* donne accès à un suivi de la *transaction* : d'abord « *pending* » (Figure N1 via EtherScan ou Figure N2 via MEW), et quelques secondes plus tard le statut passe à « *confirmed* » (Figure O1 via EtherScan ou Figure O2 via MEW).

Différents objets apparaissent dans le processus d'envoi d'*Ether* : *transaction*, *TxHash*, *block*, *gas*, *network*. Une *transaction* est signée par l'utilisateur du *wallet* émetteur des *Ethers* au moyen de sa *private key* puis émise dans le *network*. Cette opération lui attribue un *TxHash*.

239 Une fenêtre contextuelle sur MEW à propos du « Gas Limit » affiche : « *Gas limit is the amount of gas to send with your TX. TX fee = gas price * gas limit & is paid to miners for including your TX in a block. Increasing this number will not get your TX mined faster. Sending ETH = 21 000. Sending Tokens = ~200 000* ». Le *gas* correspond à un coût de *transaction*.

240 Dans cet exemple pratique, nous conservons la valeur de « Gas Limit » par défaut.

241 Corresponds au nombre de *transactions* déjà envoyées depuis ce *wallet*.

242 En l'occurrence : 0x72397f9397b79beb2a3d7e4798b6adcc9900de6d85fce902fd0d610c2c08939c.

2. Ethereum : un « réseau » dans lequel on entre par des « nodes »

La description des différentes opérations conduites par un utilisateur utilisant les services de MEW décrites en 1. (accès à MEW, création d'un *wallet*, envoi d'une *transaction*) font émerger différents objets. Les fonctions de plusieurs d'entre eux sont compréhensibles dans le script. C'est le cas de l'*address* et de la *private key* qui constituent le *wallet*. L'*address* est communiquée publiquement pour recevoir des *Ethers* ou des *Tokens* ; sa connaissance permet à quiconque de lire l'intégralité des *transactions* passées sur ce *wallet*, c'est-à-dire les *transactions* entre ce *wallet* et les autres *wallets*, chacune identifiée par un *TxHash*. La *private key* permet de générer une *transaction* et de l'envoyer dans le *network*. D'autres objets au contraire – comme *network*, *blockchain*, *gas*, *block* – sont fonctionnellement moins lisibles bien qu'ils aient tous en commun de participer au traitement des *transactions* une fois « envoyées » par l'utilisateur. Ces transactions sont « générées » par l'utilisateur : le *network* reçoit les *transactions* ; la *blockchain* interagit avec l'utilisateur via MEW ; le *gas* représente un coût de *transaction* prélevé sur le *wallet* de l'utilisateur ; le *block* est une caractéristique propre à *transaction*.

Dans les paragraphes qui suivent, je poursuis l'investigation de ces objets en m'intéressant à ce qui rassemble les objets les moins compris de l'enquête à ce stade : le traitement des *transactions* « envoyées » dans le *network*. Que se passe-t-il pour une transaction « envoyée » ? Qu'est-ce que ce *network* ? Quels objets fait-il circuler ? Pour répondre à ces questions, je m'intéresse à la relation entre MEW et la *blockchain* : en quoi consiste l'« interaction » entre l'utilisateur et la *blockchain* via MEW ? Quand est-ce que MEW interagit avec l'utilisateur, avec la *blockchain* ?

2.a « Network » et « gas price » : paramétrer les transactions

Les notions de *network* et de *gas price* apparaissent dès la page d'accueil de MEW, où l'utilisateur a l'opportunité de changer des paramètres laissés par défaut au paragraphe au

Annexes

paragraphe 1. (« Network ETH (infura.io) » et « 41 GWEI »²⁴³ respectivement, visibles sur toutes les figures représentant l'interface web de MEW en Annexes). Un menu déroulant permet de changer « Network ETH (infura.io) » ; une barre horizontale propose une corrélation directe entre le « Gas Price » et la vitesse d'exécution d'une *transaction* (Figure 33). À partir de la lecture de ces deux paramètres, je décris dans les lignes qui suivent les objets construits à partir de la signature d'une *transaction*, et comment ces objets circulent.

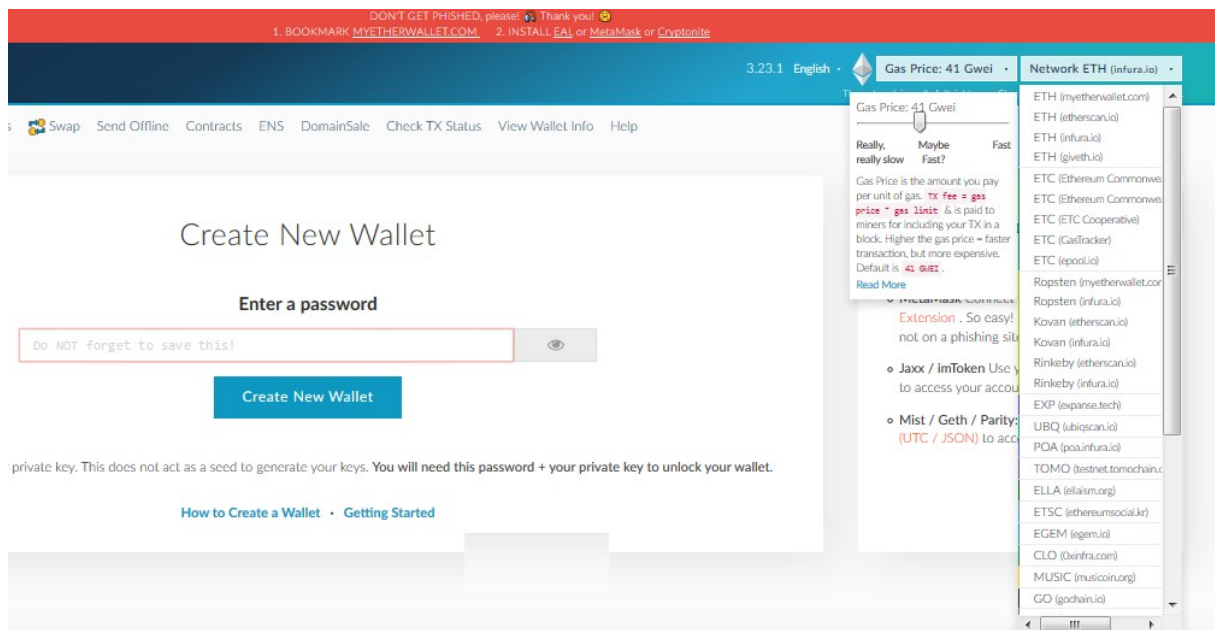


Figure 33 : Paramétrage du gas price et du network

Changer « Network ETH (infura.io) » par « ETH (etherscan.io) » fait apparaître un message sur la page du site web, reproduit sur la Figure 34.



Figure 34 : Confirmation de changement de network

²⁴³ 1 GWEI = 10^{-9} Ethers = 0,000000001 Ether

Annexes

Le *network* « ETH », c'est-à-dire Ethereum, est désormais « fourni » par « etherscan.io » (et plus par « infura.io », choix par défaut conservé tel quel au paragraphe 1.). Ce changement révèle l'existence de nouveaux acteurs qui « fournissent » le *network* aux utilisateurs. Il permet également de constater que différents *networks* sont proposés par MEW : ils sont différenciés par des couleurs sur le côté gauche de leurs noms.

Le texte suivant (extrait de la Figure 33) indique que le coût (*fee*) d'une *transaction* est proportionnel au « Gas Price » et que ce coût est « payé aux mineurs » pour le travail d'inclusion dans un *block* :

*Gas Price is the amount you pay per unit of gas. TX fee = gas price * gas limit & is paid to miners for including your TX in a block. Higher the gas price = faster the transaction, but more expensive. Default is 41 GWEI.*

Une *transaction* entre donc dans un *network*, qui est « fourni » par des acteurs comme « etherscan.io » ou « infura.io », pour être incluse dans un *block* par des *miners*. Cette opération est d'autant plus rapide que le *gas price* paramétré par l'utilisateur est élevé. Le texte ci-dessus explicite que le coût de la *transaction* est versé aux *miners* et que le montant de ce coût influe directement sur la vitesse d'inclusion de la *transaction* dans un *block*.

Qui sont ces « fournisseurs » d'Ethereum ? Pourquoi les transactions sont-elles traitées en fonction du *gas price* calibré par l'utilisateur, et pas toutes traitées de manière identique ? Qui sont ces *miners* qui prélèvent un coût pour inclure une *transaction* dans un *block* ? Pourquoi les *transactions* sont-elles incluses dans des *blocks* ? Ces questions font émerger plus généralement la question de la trajectoire des *transactions* depuis leur « génération » par l'utilisateur (1.b.) jusqu'à leur « confirmation » (1.c.). Cette trajectoire semble inscrite dans un dispositif dont les objets et les acteurs ont été effleurés dans ce document – parmi lesquels *miners*, *blocks*, *gas*.

2.b. Trajectoire des « transactions »

MEW propose une description de ce que j'ai appelé la trajectoire des *transactions* dans le paragraphe précédent. La Figure 35, obtenue sur le site web de MEW (bouton « Read

more » sur la Figure 33) représente cette trajectoire. La trajectoire suivie par une *transaction* suit deux séries de traitements. La première série de traitements est sous la « responsabilité » (*sic*) de MEW (étapes 1, 2 et 3 en haut de la Figure 35). La deuxième série de traitements est « simplement la manière dont la *blockchain* fonctionne » (*re-sic*) (étapes 4, 5 et 6 en bas de la Figure 35).

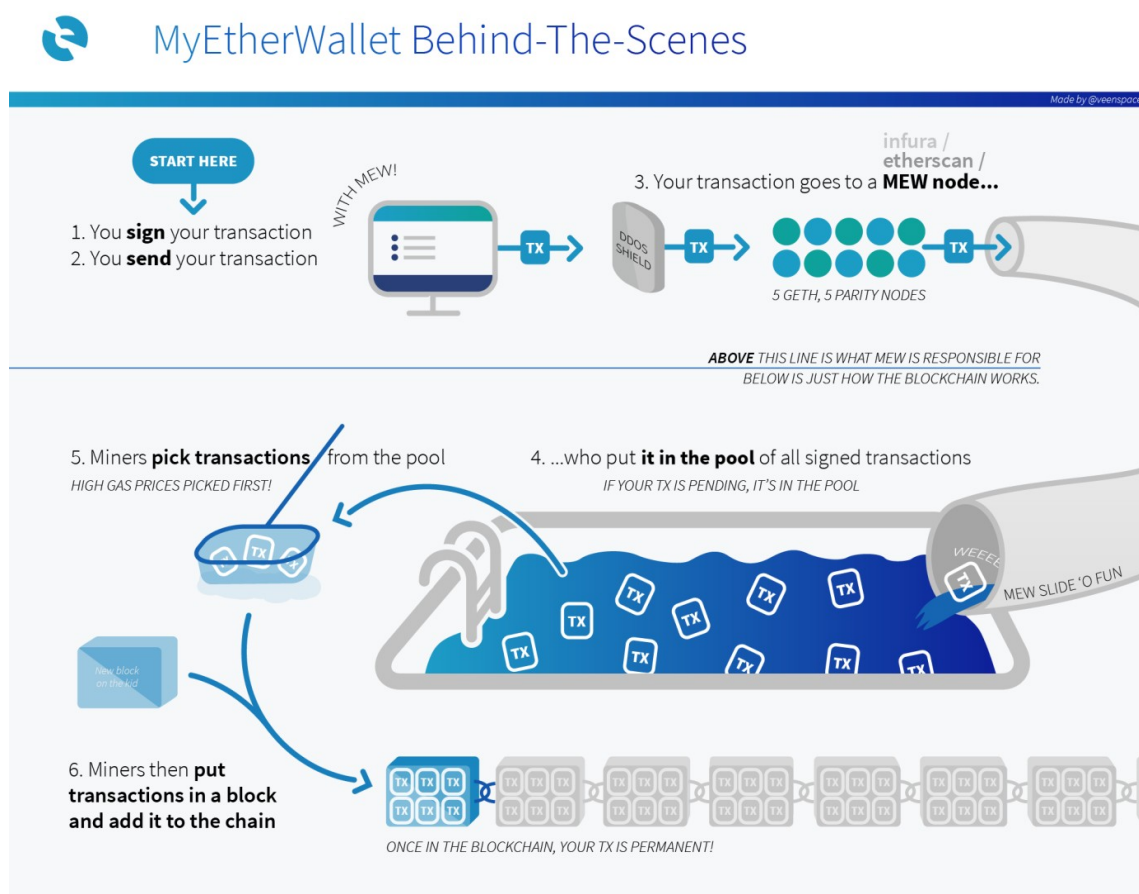


Figure 35 : Représentation de la trajectoire des transactions par MEW

La première série de traitements formate la *transaction* en la signant et en l’envoyant (étapes 1 et 2, correspondant aux opérations décrites en 1.c.) vers un *node* de MEW comme « infura » ou « etherscan » (étape 3). Ces *nodes*, ou « fournisseurs » du *network* comme nous les avons décrits plus haut, dirigent les *transactions* vers une « fosse » (*pool*) qui

Annexes

collecte les transactions signées. Les *nodes* agissent comme un point d'entrée vers la seconde série de traitements où les *transactions* sont successivement « choisies » (*picked*) par les *miners* pour être mises dans un *block* et ajoutées à la *chain*, c'est-à-dire « dans la *blockchain* ». À partir de leur entrée par un *node*, les transactions suivent une série de traitements indépendants de MEW qui les rendent successivement « *pending* » (étape 4) puis « *permanent* » (étape 6). Ces termes font écho aux situations rencontrées lors de l'envoi d'une *transaction* (1.c.) : MEW et EtherScan rendaient visibles en temps réel le statut de la *transaction* (« *pending* » en N1 ou N2, « *confirmed* » en O1 et O2).

Pourtant, le rôle de MEW semble s'arrêter à l'étape 3 de la Figure 35. Comment expliquer que le statut d'une *transaction*, c'est-à-dire sa position dans la trajectoire, puissent être suivis sur MEW ou sur EtherScan dans les dernières étapes (4, 5 et 6) ? Observer le statut *pending* nécessite de savoir si une *transaction* se trouve dans la « fosse » ; observer le statut *confirmed* nécessite de savoir si une *transaction* a été ajoutée dans un *block* lui-même ajouté à la *blockchain*.

Si la trajectoire d'une *transaction* est linéaire comme l'indique la Figure 35, il existe une forme de rétroaction de l'information permettant de faire remonter le statut de la *transaction* depuis la « fosse » ou la *blockchain* (fin de la trajectoire) jusqu'à MEW ou EtherScan (début de la trajectoire). MEW et etherscan ont en effet tous deux une forme de visibilité sur toute la trajectoire. Où sont dirigés les « yeux » de ces deux services pour fournir cette information à l'utilisateur ? Où sont la « fosse » et la *blockchain* qu'ils « regardent » ?

2.c. « Nodes » omniscients : valideurs ou « miners »

MEW apparaît à la fois comme un service front-end, ou d'interfaçage web, qui permet de suivre la trajectoire d'une *transaction* à partir de son *TxHash* (1.c.), et comme un service back-end qui « envoie » les transactions signées vers les *miners* et la *blockchain* à partir d'un *node* (2.b.). La notion de *node* n'est pas définie sur MEW ; elle fait partie du jargon de la technologie blockchain. Pour répondre aux questions posées en 2.b. il me faut introduire

Annexes

des éléments descriptifs absents de MEW. Un *node* prend la forme physique d'un serveur qui stocke l'intégralité des *blocks* qui ont été validés par les *miners* (c'est-à-dire la *blockchain*). Un *node* reçoit des *transactions* signées mais pas encore ajoutées à un *block* (ensemble de *transactions* désigné par « pool » par MEW). Un *node* est connecté par Internet aux autres *nodes* du *network* Ethereum de manière à ce que la *blockchain* qu'il stocke à un instant donné soit la même que celle stockée sur tout autre *node* au même instant. Un *node* qui a reçu une *transaction* signée peut ainsi déterminer à tout moment si cette *transaction* a obtenu le statut « *confirmed* » en observant l'état de la *blockchain* (qu'il stocke) ; dans le cas contraire, le *node* déduit que la transaction est « *pending* ».

Les *nodes* ont donc un double rôle : ils dirigent les transactions et conservent, en temps réel, l'ensemble du registre de *transactions* qui ont été confirmées sur le *network*. Comment s'opère cette confirmation ? Les paragraphes précédents ont mis en évidence la présence de *miners*. Les *miners* sont des *nodes* particuliers. Parmi les *transactions* qu'ils reçoivent d'autres *nodes*, les *miners* choisissent des *transactions* qui sont signées (étape 5 de la Figure 35) en vue d'en faire un *block*. Selon la documentation fournie par MEW, le choix d'une *transaction* est guidé par la rémunération qui lui est associée (2.a.) : plus elle est élevée, plus les *miners* sont incités à traiter cette *transaction* en priorité. Cette rémunération correspond exactement au « coût » de *transaction* (*gas*) rencontré en 2.a. Ce coût, payé par l'utilisateur qui signe une *transaction*, est versé au *miner* en tant que rémunération pour inclure la *transaction* dans un *block*. L'utilisateur n'échappe pas au paiement de ce coût : sans elle, une transaction ne pourrait pas être signée, et ne serait donc pas ajoutée dans un *block*. Or, seule l'inclusion dans un *block* performe une *transaction*, c'est-à-dire traduit les informations que l'utilisateur a signées en un transfert de fonds observables sur la *blockchain* : c'est en faisant passer le statut de « *pending* » à « *confirmed* » que les fonds sont transférés. L'utilisateur doit par conséquent veiller à ne pas proposer une rémunération trop faible, faute de quoi les *miners* pourraient éternellement ignorer cette *transaction* au profit d'autres *transactions* plus rémunératrices²⁴⁴. Une telle *transaction* resterait au stade

²⁴⁴ Les *transactions* les moins rémunératrices sont susceptibles d'être ignorées au profit de transactions plus rémunératrices. Cet arbitrage, à la main de chaque *miner*, peut s'exercer selon des temporalités variables. À court terme, un *miner* pourra décider d'ignorer une *transaction* jugée peu rémunératrice en la gardant tant que d'autres *transactions* sont plus rémunératrices. À plus long terme, un *miner* pourra décider de

Annexes

de projet : signée par son émetteur, son statut resterait « *pending* » sans jamais connaître le statut « *confirmed* ».

Pourquoi les *miners* sont-ils rémunérés pour inclure des *transactions* dans un *block* (étape 6 de la Figure 35) ? L'opération de « minage » d'un *block* est coûteuse pour un *miner*. La rémunération vient rétribuer le *miner* pour effectuer la confirmation de *transactions* dans un *block*. Cette opération suit un ensemble de règles fixées par le *network* Ethereum. Un *miner* commence par sélectionner des *transactions* signées en veillant à ce que la quantité de lignes de codes correspondantes à ces *transactions* ne dépasse pas la limite autorisée, qui se mesure en *gas*. La somme du montant en *gas* de chaque *transaction* ne doit pas excéder le montant maximal de *gas* autorisé pour un *block*²⁴⁵. Ainsi, le *network* fixe la quantité de lignes de code à exécuter mais pas la rémunération de chaque *miner* qui, elle, dépend des *transactions* qu'il choisit d'exécuter (individuellement paramétrée par les émetteurs de transactions, cf. 2.a.). Le *miner* est alors confronté à une opération singulière : il doit résoudre un problème algorithmique complexe. À . À partir de l'identifiant du dernier *block* validé sur le *network* (appelé *hash*) et des *transactions* sélectionnées à inclure dans le *block*, le *miner* cherche à construire un identifiant pour ce nouveau *block*, son *hash*, qui doit satisfaire différentes conditions. Le *hash* doit être produit par un algorithme appelé *Ethash*²⁴⁶, qui est coûteux à exécuter : la découverte d'un *hash* qui corresponde aux règles du *network* demande de nombreux calculs informatiques. La découverte de la bonne solution est aléatoire : *Ethash* exécute en boucle la même série d'opérations qui contient des paramètres aléatoires jusqu'à ce qu'une solution correcte soit trouvée. Le premier *miner* qui trouve une solution convenable la diffuse au reste du réseau (*broadcast*), le *block* est

supprimer une *transaction* de sa liste de transactions en attente (« pool » ou « fosse ») jugée peu rémunératrice pour libérer de l'espace disque pour d'autres transactions potentiellement plus rémunératrices.

245 Le *gas* permet de créer une relation d'équivalence entre l'effort d'exécution de toutes transactions. Dans cette section, nous n'avons rencontré que des transactions élémentaires : le transfert d'Ethers d'un *wallet* à un autre. D'autres *transactions* existent, notamment dans les *smart contracts*, qui seront discutés en section 2. La fabrication du montant de *gas* associé à un *block* n'est pas être discutée ici.

246 Cet algorithme est d'abord exécuté à partir des données d'entrées propres au *block* en cours de construction : le *hash* du *block* précédent, les *transactions* dans le *block* en cours de construction, et un extrait des *blocks* de la *blockchain*. Ce résultat intermédiaire est ensuite comparé à une valeur fixée à l'avance : si le *hash* obtenu est numériquement inférieur à cette valeur, le *hash* est considéré comme valide, sinon le calcul recommence depuis le début jusqu'à ce qu'un *hash* inférieur à la valeur fixée à l'avance soit trouvé.

Annexes

alors ajouté à la *blockchain* par chaque *node* (à son « exemplaire » de la *blockchain*, sur son serveur). Lorsque la majorité des *miners* ont ajouté ce *block*, le *block* et les *transactions* qu'il contient deviennent valides. Après la découverte d'un *block* valide, les *miners* recommencent le travail (depuis le début) à partir de nouvelles données d'entrée. Le *hash* du *block* fraîchement construit devient une donnée d'entrée du nouveau *block* en cours de construction, d'où la notion de « chaîne » de « blocs ».

Le caractère « aléatoire » de l'algorithme *Ethash*, au cœur du processus de construction des *blocks*, permet de répartir les chances de découvertes d'un *block* en fonction de la « puissance de calcul » des *miners*, c'est-à-dire des capacités algorithmiques investies dans leurs serveurs (processeurs notamment). Plus un *miner* dispose de « puissance de calcul » dans le *network*, plus il aura de chance de découvrir un *block* valable en premier et d'obtenir la rémunération liée à ce *block*. Pourquoi la construction d'un *block*, opérée par un *miner*, est-elle coûteuse ? Que se passerait-il si les *miners* suivant ce même processus de vérification / inscription d'un *block* dans la *blockchain* sans avoir à calculer un problème mathématique complexe ? Ce processus permet – en théorie au moins – de répartir la rémunération en fonction de la puissance investie, mais aussi de séquencer la validation des *transactions*. Le temps de validation entre deux *blocks* est d'approximativement 15 secondes (approximativement car gouverné par un processus aléatoire) : sans difficulté dans la recherche d'un *block*, différentes *transactions* pourraient se trouver de nombreuses fois dans différents *blocks* validés en même temps.

Ce type de mécanisme dit « de consensus » par « preuve de travail » permet surtout de se prémunir d'attaques contre des *miners* mal intentionnés en limitant le nombre de propositions de *blocks*. Pour qu'une transaction frauduleuse soit validée (par exemple, envoyer 1000 *Ethers* depuis un *wallet* qui n'en contient pas) il faudrait qu'une majorité de *miner* valident cette transaction. Ceci n'est possible que si au moins la moitié des *miners* valident cette transaction²⁴⁷. Or, dans un mode de « consensus » par « preuve de travail », le poids de chaque *miner* est mesuré en « puissance de calcul » plutôt que par leur identité sur Internet. Ainsi, pour qu'une transaction frauduleuse soit validée, il faudrait qu'au moins la

247 Une telle situation est appelée « attaque à 51 % »

moitié de la puissance de calcul du *network* soit coalisée pour valider des *transactions* selon un procédé contraire aux règles du *network*. Ethereum (comme Bitcoin) considère qu'une telle situation est très peu probable, en tous cas beaucoup moins que si le poids des utilisateurs était mesuré par leur identité sur Internet (leur adresse IP). Dans ce dernier scénario, il serait en effet aisé pour un utilisateur « mal » intentionné de créer des adresses IP fictives pour valider des transactions contraires aux règles du *network*. Des alternatives au mécanisme de consensus par preuve de travail sont un objet important de recherche en algorithmique et en ce qui concerne les architectures de réseaux distribués. J'évoquerai un autre mécanisme dit par « preuve d'enjeu » en II.3²⁴⁸.

3. Les formes des nodes, pivots entre l'utilisateur et la blockchain

MEW propose un service pour signer des transactions (1.) et pour envoyer les transactions dans le *network* pour qu'elles soient validées (2.). Ainsi, MEW a un rôle de pivot à deux titres : en permettant à l'utilisateur de signer ses *transactions* (c'est-à-dire en les formatant) et en assurant la communication avec le *network* par sa position de *node*. Dans quelle mesure ces deux opérations sont-elles liées ? Peut-on se passer de MEW, comment accéder à Ethereum sans son intermédiation ? Qui sont les autres *nodes* d'Ethereum ?

3.a. Être node soi-même

Quiconque peut décider d'agir comme un *node* d'Ethereum. Différents logiciels permettent d'installer sur sa machine, comme *Geth*. Agir en tant que *node* permet de signer des transactions et de les envoyer dans le *network* sans intermédiaire comme MEW. Un *node* pourra également explorer la *blockchain*, c'est-à-dire connaître l'intégralité des transactions d'une quelconque *address*. Toutes ces caractéristiques sont communes à celles décrites pour MEW ou EtherScan mais selon une architecture informatique fondamentalement différente. En disposant d'un *node*, l'utilisateur ne dispose pas d'autre interface que le terminal de sa machine dans lequel il communique avec la *blockchain* en lignes de commandes interprétées par un logiciel spécifique (comme *Geth*)

²⁴⁸ Cette partie du document de travail n'a pas été ajoutée à ce manuscrit.

Annexes

En construisant un *node* Ethereum, l'utilisateur a également l'opportunité de « miner » de l'*Ether*, c'est-à-dire de participer à la construction de *blocks* en échange d'*Ethers*. Cette activité est controversée à différents titres²⁴⁹. Premièrement, la volatilité du cours de l'*Ether* vis-à-vis des devises légales (comme l'euro ou le dollar), dans lesquelles sont facturés les coûts d'électricité nécessaires à l'activité de minage, est perçue comme un risque. Deuxièmement, la rentabilité d'un utilisateur donnée est fonction de paramètres propres à Ethereum, qui varient dans le temps, qui se mesurent à l'aide d'indicateurs. Parmi ces indicateurs figure la difficulté de minage (*mining difficulty*). Plus les *miners* participant à la construction de *blocks* sont nombreux, plus la difficulté de résolution des problèmes algorithmiques complexes (*cf.* 2.c.) est élevée afin de conserver une vitesse de validation des transactions (en moyenne) la même sur Ethereum. La difficulté de minage ne dépendant pas de l'activité de l'utilisateur mais de la quantité d'offre de minage, elle représente elle aussi un risque. Troisièmement, la vitesse à laquelle un *miner* résout les problèmes mathématiques, appelée *hash rate* (en construisant un *block*, un *miner* produit un *hash*, *cf.* 2.c.), dépend du matériel dont dispose le *miner*. Certains constructeurs de puces électroniques se sont spécialisés dans la construction de puces spécialisées dans le minage permettant à un *miner* d'optimiser son *hash rate* pour une même quantité d'électricité dépensée. Ces puces sont appelées ASIC pour « *Application-specific integrated circuit* » et construites spécifiquement pour une blockchain donnée ; certaines puces sont donc spécialement construites pour Ethereum²⁵⁰. Elles sont très prisées par les investisseurs constituant des « fermes » de minage c'est-à-dire des salles de serveurs entièrement dédiées au minage. Ce type d'investissements, favorisant une difficulté de minage importante, est dénoncé par les défenseurs d'une « décentralisation » du minage. Ces investissements favoriseraient la concentration du pouvoir de minage à proportion de la concentration du *hash rate*. Cette concentration est condamnée à deux titres : d'abord, car elle empêche ceux qui n'investissent pas dans du matériel haut de gamme à pouvoir participer à la maintenance de l'infrastructure, mais surtout elle menace l'intégrité de l'infrastructure²⁵¹.

249 Différents éléments du paragraphe sont inspirés de <http://etherumin.com/how-much-can-you-make-mining-ethereum-beginners-guide/>.

250 Différents modèles sont développés pour chaque *network*, adaptées aux problèmes mathématiques de chacune. Les modèles Bitcoin sont par exemple différents des modèles Ethereum.

251 Le « poids » des *miners* dépend de leur puissance de calcul. Ainsi, si quelques *miners* disposant d'au

Cette critique est parfois embarquée dans le design de certaines *blockchains* dont les mécanismes de consensus empêchent l'optimisation par du matériel du type ASIC.

3.b. Ce qu'il se passe en ligne, ce qu'il se passe hors ligne

Construire un *node* Ethereum ou se connecter à MEW sont des moyens pour effectuer les opérations décrites en 1. Les liens avec la *blockchain* sont-ils les mêmes ? MEW agit comme un *node* auquel l'utilisateur se connecte *via* un site Internet. Ce faisant, l'utilisateur évite d'installer un logiciel comme *Geth*, procédure qui implique de maintenir en temps réel l'intégralité de la *blockchain* (entre 100 et 120 GB en octobre 2018), et interagit avec la *blockchain* *via* une interface graphique. En revanche, l'utilisateur confie ses informations, dont ses *keys*, à un site web distant qui signe les transactions. La signature d'une *transaction*, mais aussi la création d'un *wallet*, peuvent se faire hors ligne. MEW propose d'ailleurs de signer une *transaction* hors ligne (bouton « Send Offline » sur le site web de MEW). Si la création d'un *wallet* ou la signature d'une *transaction* s'effectuent sans lien avec la *blockchain*, comment ces opérations sont-elles synchronisées avec le reste du *network* ? La création d'un *wallet* ne l'est pas : les *addresses* sont générées aléatoirement et les chances de générer une *address* déjà existante sont quasi-nulles²⁵². La signature est, elle aussi, à la main de l'utilisateur (*cf.* 2.b.).

Les *nodes* représentent les frontières entre les utilisateurs et le *network*. Un utilisateur qui dispose d'un *node* Ethereum peut non seulement signer ses *transactions* mais aussi les envoyer dans le *network*. Les services tels que MEW ou EtherScan sont des interfaces qui proposent des services d'appoint aux utilisateurs ne disposant pas de *node*.

D'autres solutions existent pour communiquer avec Ethereum. L'une d'elle consiste à stocker les informations de son *wallet* (*address* et *private key*) dans son navigateur web à

moins 51 % de la puissance de calcul se mettent d'accord pour valider des *transactions*, ces dernières seraient valides qu'elles soient conformes ou non à l'historique des transactions sur la *blockchain*. De fait, ces transactions contraires aux règles du réseau deviendraient « *confirmed* » (réussite d'une « attaque à 51 % »).

252 Le nombre d'*address* possible sur Ethereum est de 2^{160} soit environ 10 fois plus que de molécules d'eau sur Terre.
https://www.reddit.com/r/ethereum/comments/5em2mk/chance_of_creating_an_existing_inuse_key/

Annexes

l'aide d'un « add-on ». C'est par exemple ce que propose Metamask²⁵³ dont les premières lignes de présentation sur le site web de Metamask sont :

MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereum dApps right in your browser without running a full Ethereum node.

MetaMask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions.

You can install the MetaMask add-on in Chrome, Firefox, Opera, and the new Brave browser. If you're a developer, you can start developing with MetaMask today.

Our mission is to make Ethereum as easy to use for as many people as possible.

Metamask est décrit comme un « pont », un moyen d'éviter de maintenir un *node* Ethereum, entreprise dont la mission est de « rendre Ethereum aussi simple que possible à utiliser pour le plus grand nombre possible ». Alors que MEW met en garde contre les risques de sécurité inhérent à l'utilisation d'Ethereum (cf. 1.a.), Metamask met au contraire en avant la sécurité assurée par son service. MEW comme Metamask ont en commun d'interfacer l'utilisateur avec le *network* Ethereum, de le rendre invisible.

3.c. De la diversité des points d'entrées d'Ethereum. Des nodes « techniques » aux positions « économiques » : individus, startups et plateformes d'échanges

Par quel canal un utilisateur de Metamask communique ses *transactions* au *network* ? Metamask n'est pas un *node*, mais un logiciel installé dans le navigateur de l'utilisateur (add-on). Metamask communique pourtant bien avec un *node* via Internet pour envoyer les *transactions* dans le *network*. Ce *node*, ou plutôt cet ensemble de *nodes*, est administré par une société appelée Infura²⁵⁴. Cette société est décrite comme un « *infrastructure provider* »

253 <https://metamask.io/>

254 <https://ethereum.stackexchange.com/questions/13362/to-which-remote-ethereum-nodes-does-metamask-plugin-send-signed-transactions-an>

Annexes

auquel peuvent s'adosser différents services comme MEW²⁵⁵ mais aussi des startups, comme la Singapourienne Digix. Développé au départ pour les projets de ConsenSys, pépinière de projets Ethereum, Infura a ouvert ses services à l' « écosystème [Ethereum] en entier »²⁵⁶.

Tout individu peut devenir un *node* Ethereum (3.a.) et ainsi fournir un service pour lequel il est rémunéré (2.c.) ; des entreprises, comme Infura, proposent d'établir la connexion au *network* pour des entreprises qui préfèrent déléguer la gestion de l'accès à Ethereum plutôt que de construire et de maintenir un *node* elles-mêmes. D'autres acteurs proposent des services de change entre devises légales et crypto-monnaies (dont l'*Ether*), de cotation de crypto-monnaies et de *tokens*²⁵⁷, ainsi que d'échanges de crypto-monnaies et de *tokens* : les plateformes d'échange. Parmi les plateformes les plus populaires figurent Coinbase (US), Kraken (US), Bitfinex (HK) ou Binance (Chine continentale jusqu'en septembre 2017, puis Japon en prévision de l'interdiction des plateformes d'échanges de Chine, puis Taïwan à partir de mars 2018).

Du point de vue de l'utilisateur, ces plateformes apparaissent comme des applications web « classiques » : l'utilisateur s'identifie *via* son adresse email sur le site ou l'application mobile de la plateforme. Le schéma d'authentification n'est pas basé sur un système d'*address / private key*. Ces informations sont pourtant nécessaires pour signer une *transaction* avant de l'envoyer dans le *network* (voir 1.) : où sont l'*address* et la *private key* d'un utilisateur sur ces plateformes ? Les plateformes d'échanges ont leurs propres *wallets* (*address / private key*) en *Ether* (et autres crypto-monnaies et *Tokens*) que l'utilisateur peut visualiser s'il souhaite transférer ses fonds vers une *address* personnelle²⁵⁸. Ainsi, ces plateformes fonctionnent comme des « banques » de cryptoactifs : leurs comptabilités sont

255 <https://blog.infura.io/infura-and-myetherwallet-5d98b71b8e40>

256 <https://infura.io/about>

257 « *token* » désigne (souvent, à préciser) un actif numérique adossé à une crypto-monnaie qui est, elle, inscrite dans une *blockchain*. L'*Ether* peut être considéré comme une crypto-monnaie. Les *tokens* émis dans le cadre d'ICO (Initial Coins Offerings) sont qualifiés de *tokens*.

258 Ceci peut être observé sur un site permettant de suivre les transactions effectuées sur la *blockchain* comme MEW ou etherscan (voir *supra* 1.c.). La figure I permet de visualiser que ces *wallets* propriétés des plateformes d'échanges sont connus de services comme MEW ou etherscan qui remplacent leurs *address* (en 0x...) par un nom (Binance_1 par exemple).

Annexes

« internes » à leurs structures légales et invisibles publiquement, en particulier invisibles sur la *blockchain*. De cette invisibilité découlent des risques de piratage : le vol des *private key* des *wallets*, propriétés de ces plateformes, conduit à la perte immédiate des fonds pour la plateforme (mais aussi pour les utilisateurs qui ne disposent d'aucun moyen de recours légal). La plateforme Mt. Gox a par exemple vu s'envoler 744 408 bitcoins en février 2014, valorisés à environ 4,6 milliards de dollars US à fin octobre 2018. Ce risque de vol alimente les critiques sur les crypto-monnaies en général qualifiées de faiblement sécurisées [à préciser largement].

Ces plateformes permettent d'obtenir des crypto-monnaies ou des *tokens* à partir de devises comme l'euro ou le dollar. L'utilisateur peut envoyer des fonds en devises sur son compte par virement bancaire à partir du RIB de la plateforme. Ce type de services permet aux plateformes d'occuper une place quasi incontournable pour quiconque souhaite se « lancer » dans la manipulation de crypto-monnaies²⁵⁹. Parmi les autres rares solutions figure l'achat de crypto-monnaies à un guichet, en boutique. C'est ce que propose Coinhouse Store, anciennement « Maison du Bitcoin », dans le 2^e arrondissement de Paris. Les plateformes d'échanges, sur Internet ou en boutique comme Coinhouse Store, prennent aussi une position de place de marché : quiconque peut y suivre, en temps réel, la cotation des crypto-monnaies et *tokens* que la place permet d'échanger. Une plateforme agit à la fois comme courtier (intermédiaire entre acheteur et vendeur, aussi bien en tant qu'interface graphique que sur la *blockchain* en organisant les inscriptions comptables d'achat / vente) et comme commissaire-priseur (fixation des paramètres spot d'achat ou de vente en fonction de l'offre et de la demande dans une crypto-monnaie / *token*, visibles en termes de prix et de volumes d'échange).

259 Par souci de clarté dans la partie a, j'ai évité d'introduire les plateformes et ai alimenté le *wallet* à partir d'un autre *wallet*. Cet autre *wallet* avait, lui, été alimenté à partir d'un compte créé sur une plateforme d'échange (Binance).

Annexes

Figures de l'Annexe 3

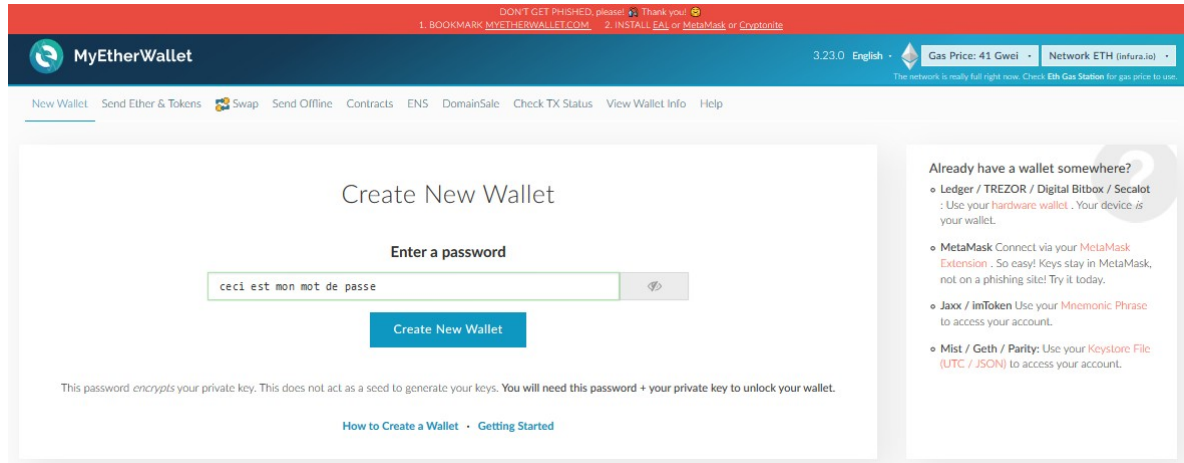


Figure A : Page d'accueil de MyEtherWallet.com avec le mot de passe « ceci est mon mot de passe » saisi

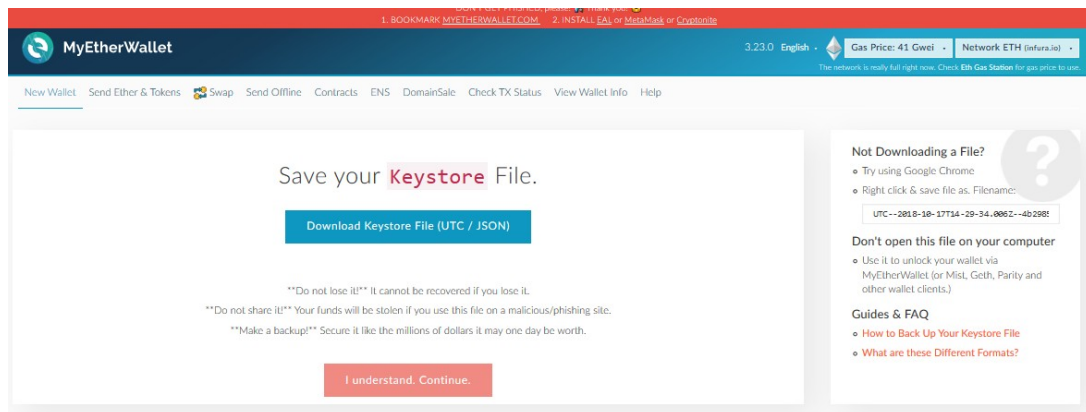


Figure B : Parcours de création d'un wallet – sauvegarde du keystore

```
{"version":3,"id":"93d5032c-01b0-41dc-968e-9caee09b453b","address":"4b2985b10cb3d727577fac07a508228fdec7f97d","Crypto":{"ciphertext":"b053e836632feda908a8e08994f10fb3374ff83df503016d19651d99afa1d6a0","cipherparams":{"iv":"64c0d8c9711fbd7b289fb146002a3587"},"cipher":"aes-128-ctr","kdf":"scrypt","kdfparams":{"dklen":32,"salt":"b3df37154ed48795c7b3dfb0e6d7c8c237247eab3ab548c489e5a45c6b1f7f18"},"n":8192,"r":8,"p":1},"mac":"3c3c8bef2a04b45cf41df7ee41158c2b5716b916e879b3b1d1eeefddf747a2d6"}}
```

Figure C : Exemple de contenu d'un fichier keystore lisible après téléchargement par l'utilisateur

Annexes

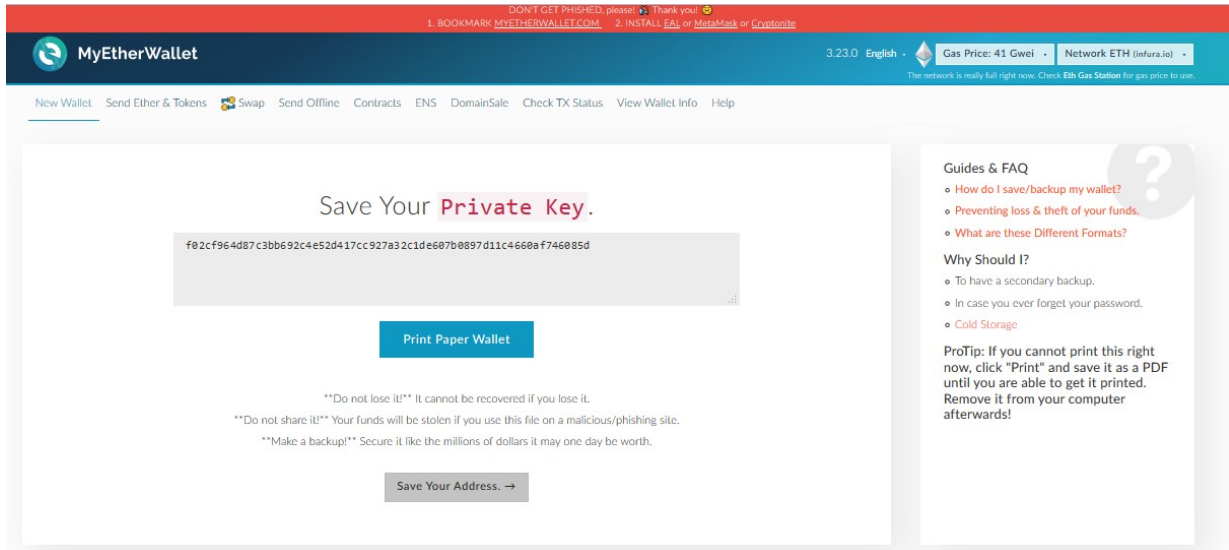


Figure D : Troisième fenêtre dans le parcours de création d'un portefeuille

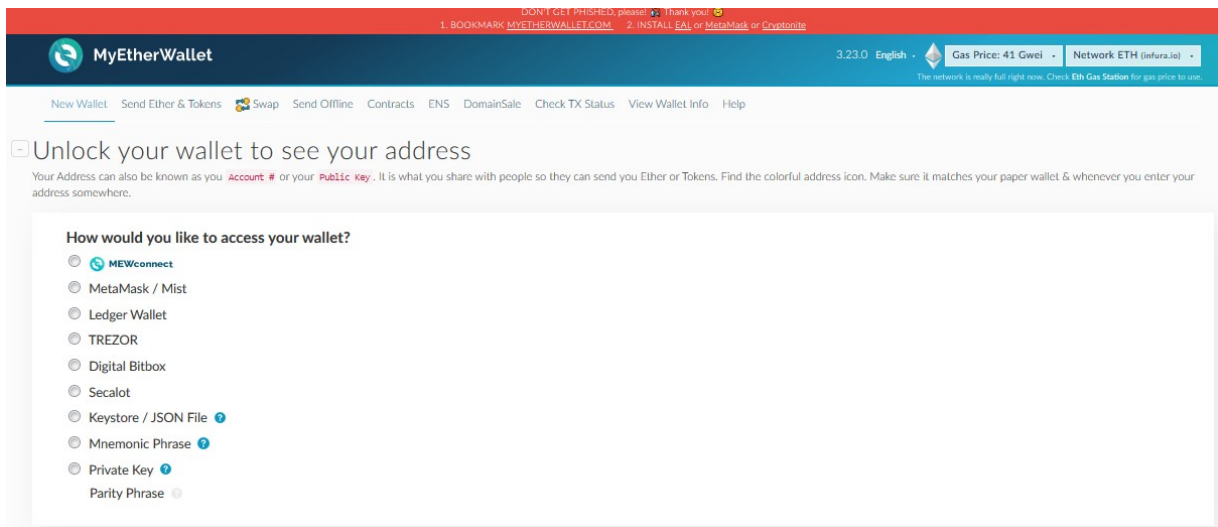


Figure E : Parcours de création d'un wallet – sauvegarde de l'address

Annexes

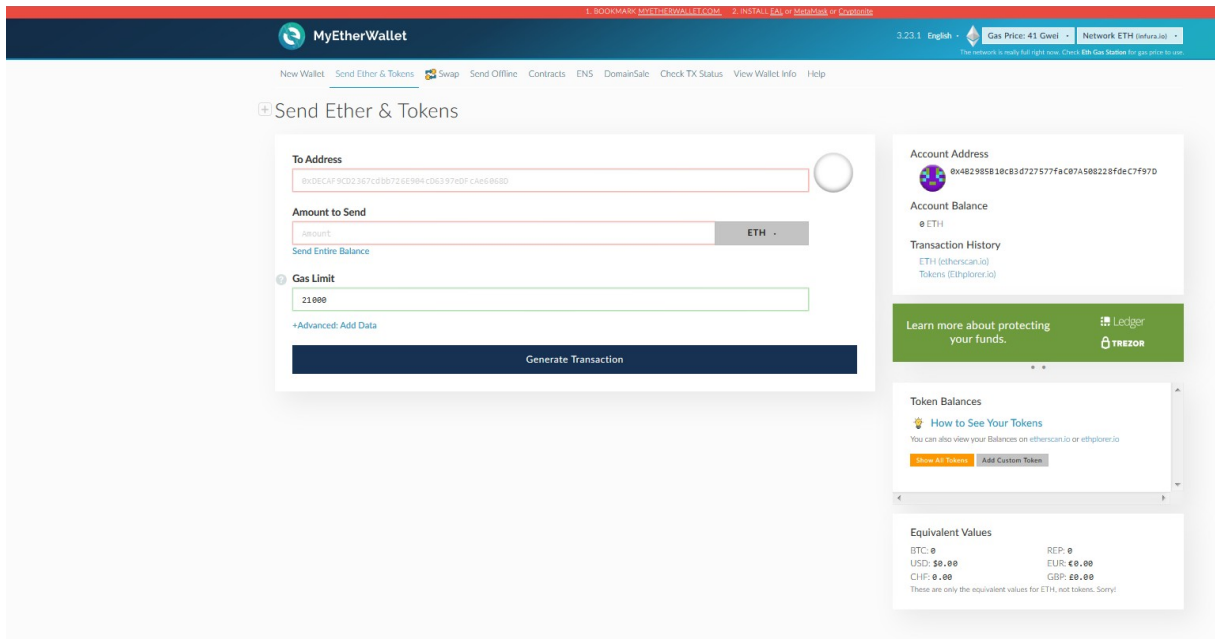


Figure F : Parcours d'envoi de fonds / Aucun fonds sur le wallet

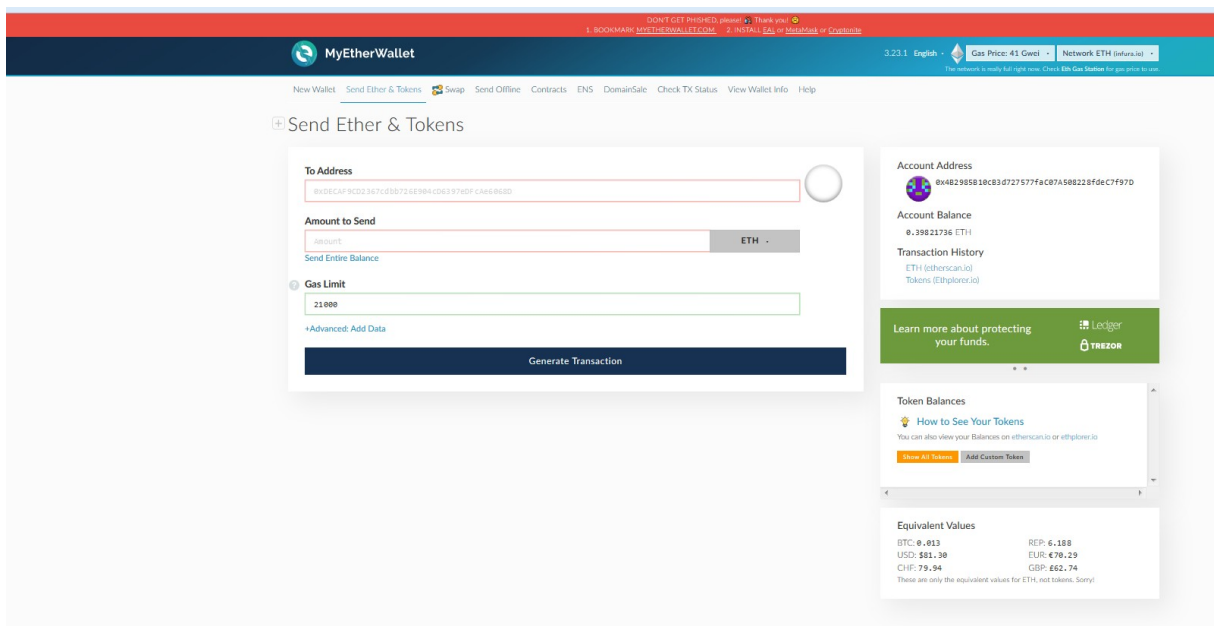


Figure G : Parcours d'envoi des fonds

Annexes

Etherscan - The Ethereum Block Explorer

Search by Address / Txhash / Block / Token / Ens Language

HOME BLOCKCHAIN TOKENS RESOURCES MORE

Address: 0x4B2985B10cB3d727577faC07A508228fdeC7f97D

Overview

Balance: 0 Ether

Ether Value: \$0

Transactions: 1 txn

Misc: Address Watch:

Transactions

| TxHash | Block | Age | From | To | Value | [TxFee] |
|---------------------|---------|------------|---------------------|---------------------|------------------|----------|
| 0x99505c1140260a... | 6561833 | 4 mins ago | 0x4129d7521264ce... | 0x4b2985b10cb3d7... | 0.39821736 Ether | 0.000861 |

[Download CSV Export]

Figure H : Parcours d'envoi des fonds / Historique des transactions

Etherscan - The Ethereum Block Explorer

Search by Address / Txhash / Block / Token / Ens Language

HOME BLOCKCHAIN TOKENS RESOURCES MORE

Address: 0x4129D7521264Ce326c03D610E165fc9276649Da1

Sponsored: **Crypto.com** - Crypto Invest: Democratizing Quant Trading - designed to perform in any market - start an automated portfolio with \$20 min.

Overview

Balance: 0.39907836 Ether

Ether Value: \$81.48 (@ \$204.17/ETH)

Transactions: 2 txns

Misc: Address Watch:

Transactions

| TxHash | Block | Age | From | To | Value | [TxFee] |
|---------------------|---------|-------------|---------------------|---------------------|------------------|----------|
| 0x99505c1140260a... | 6561833 | 6 mins ago | 0x4129d7521264ce... | 0x4b2985b10cb3d7... | 0.39821736 Ether | 0.000861 |
| 0x5a0ed4b2085c3... | 6561808 | 12 mins ago | Binance_1 | 0x4129d7521264ce... | 0.39907836 Ether | 0.00063 |

[Download CSV Export]

Figure I : Parcours d'envoi de fonds / Visualisation du wallet émetteur

Annexes

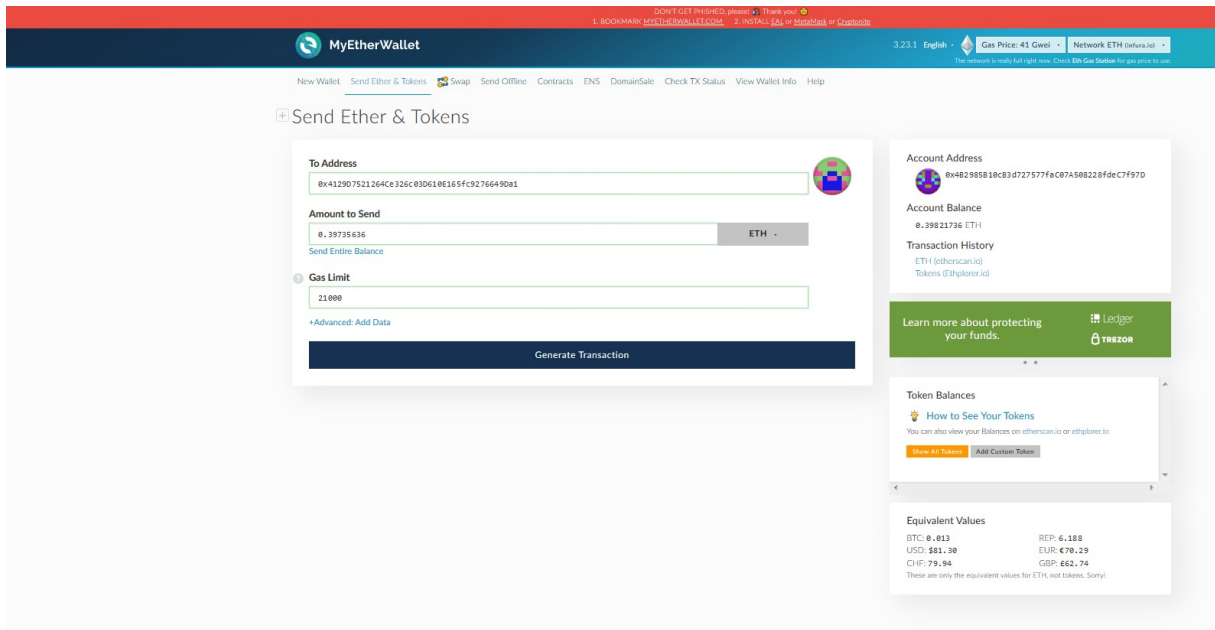


Figure J : Parcours d'envoi de fonds / Génération de la transaction

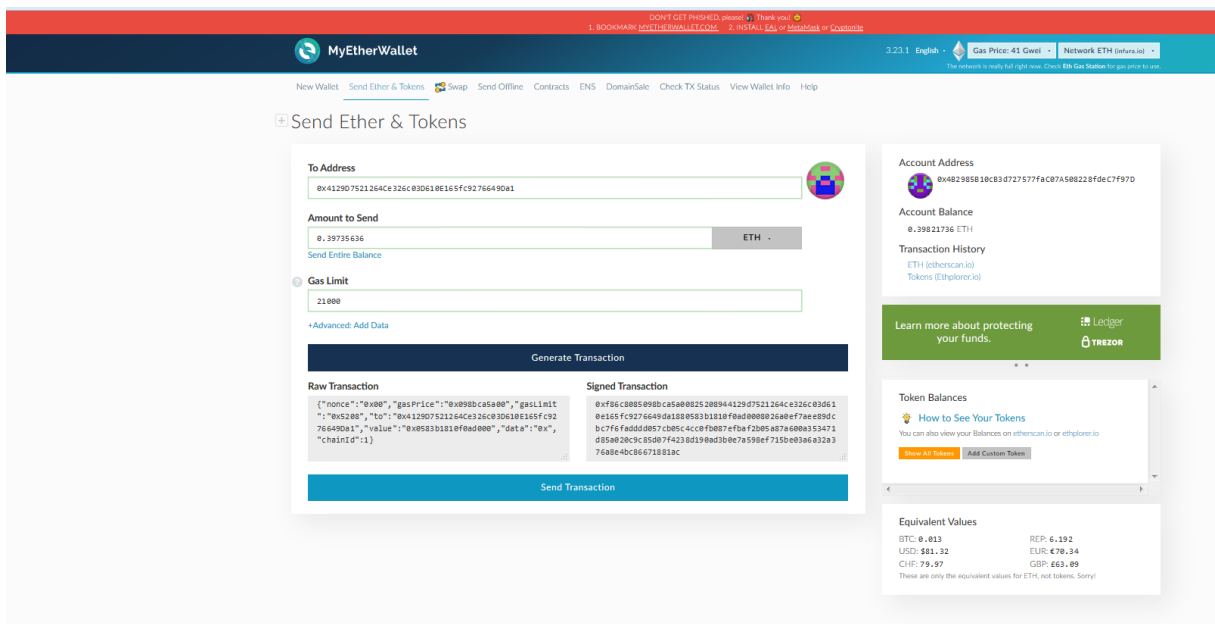


Figure K : Parcours d'envoi de fonds / Envoi de la transaction

Annexes

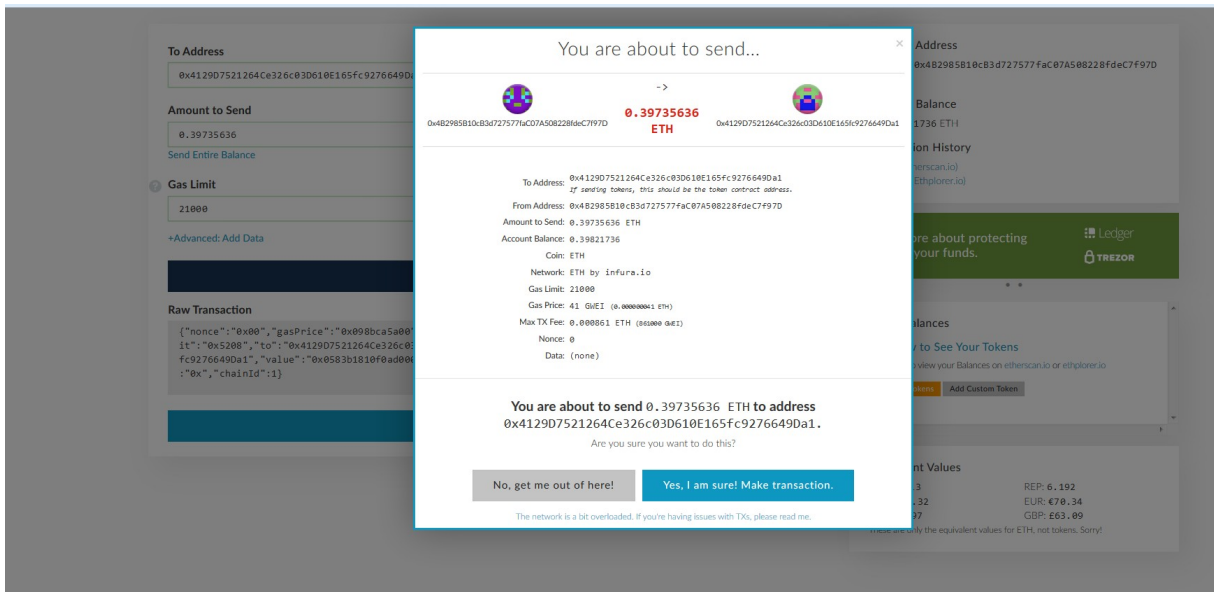


Figure L : Parcours d'envoi de fonds / Demande de confirmation d'envoi de la transaction

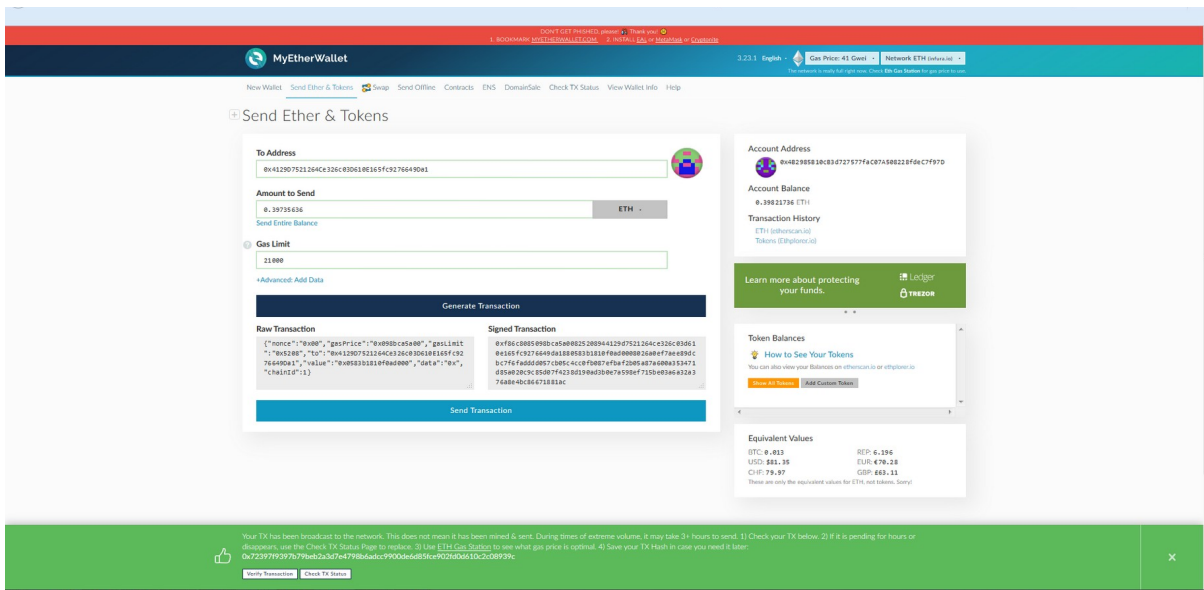


Figure M : Parcours d'envoi de fonds / Confirmation d'envoi au réseau

Annexes

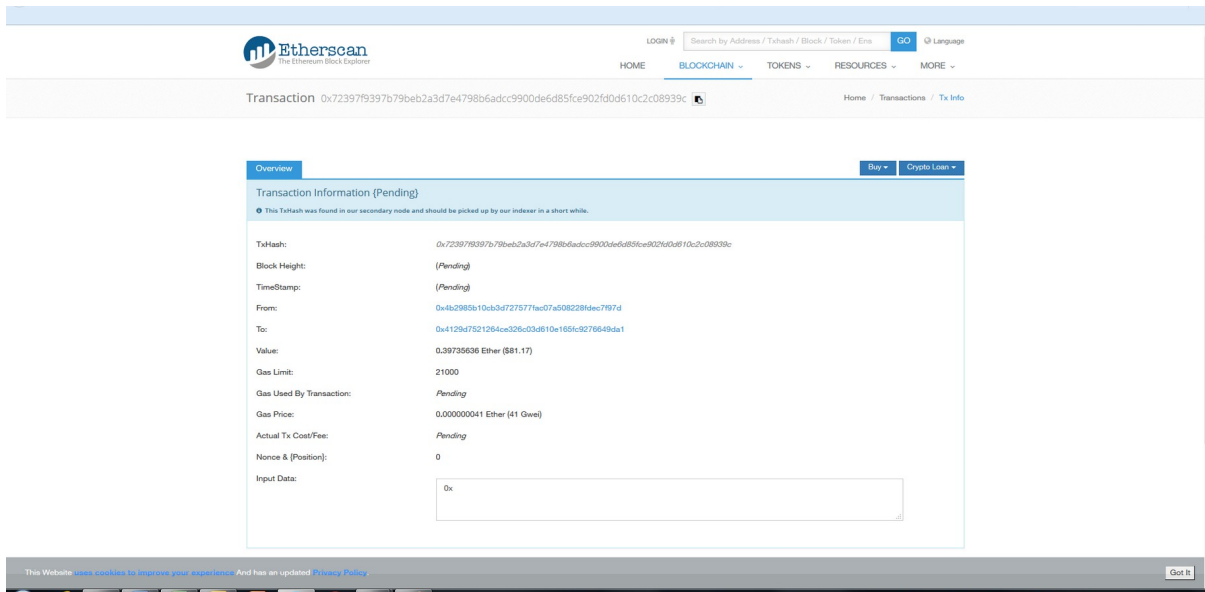


Figure N1 : Parcours d'envoi de fonds / Transaction en attente via etherscan.io

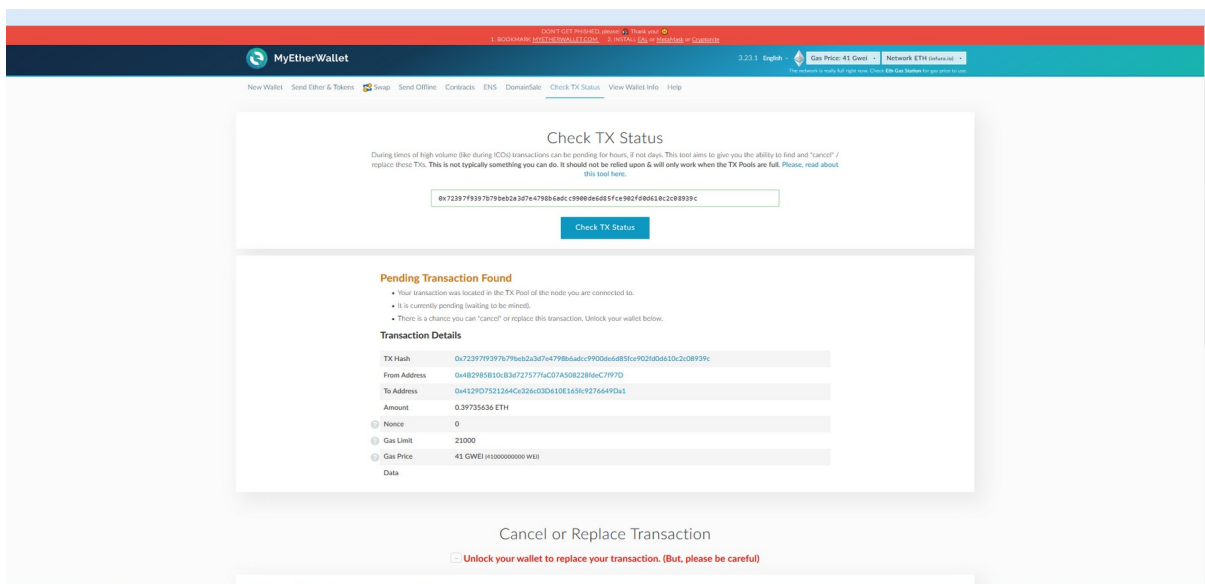


Figure N2 : Parcours d'envoi de fonds / Transaction en attente via MEW

Annexes

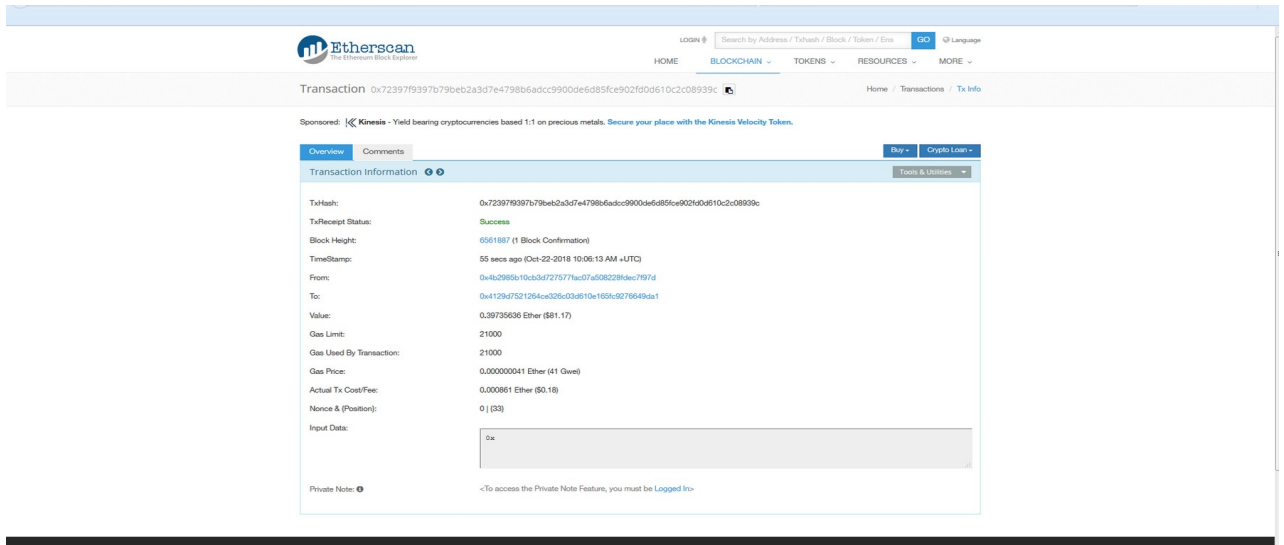


Figure O1 : Parcours d’envoi de fonds / Transaction confirmée via etherscan.io

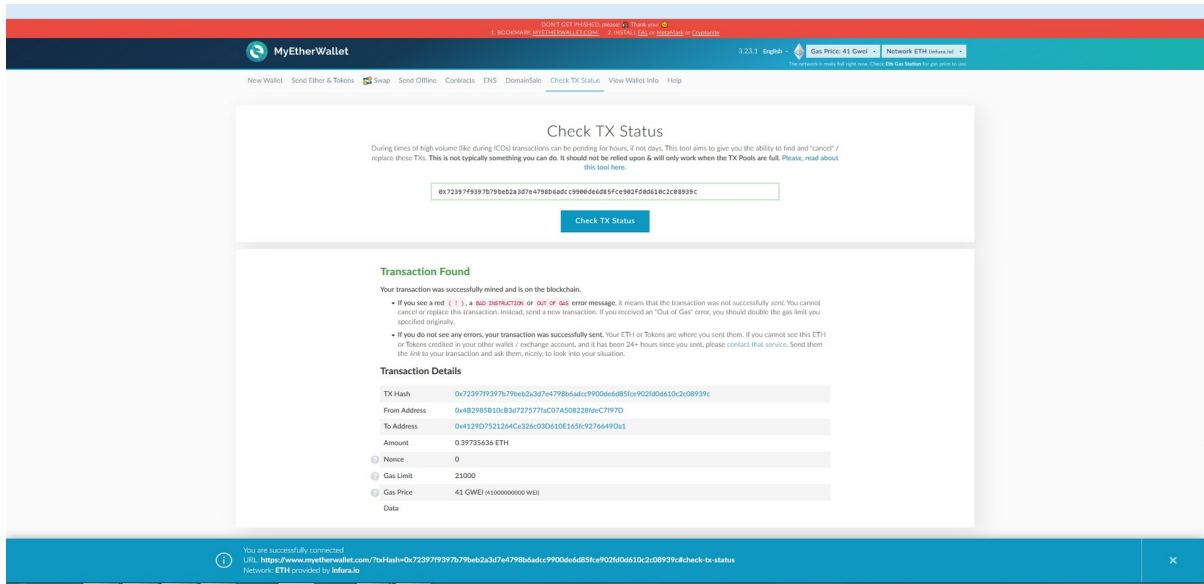


Figure O2 : Parcours d’envoi de fonds / Transaction confirmée via MEW

RÉSUMÉ

Les concepteurs des blockchains inventent des manières d'entrer en relation par des infrastructures numériques. Elles sont développées aussi bien au sein d'institutions publiques et privées que par des communautés de cryptomonnaies qui cherchent à éviter ces institutions. Cette thèse vise à saisir les dimensions politiques de ce processus d'innovation en rendant compte de l'activité de développeurs, d'ingénieurs, d'entrepreneurs, d'investisseurs, de cadres d'entreprises et de militants. Elle s'appuie sur une enquête ethnographique multi-située du processus de conception d'Ethereum entre 2018 et 2020 en France, à Singapour et en ligne. Cette thèse se situe au croisement des études sociales des sciences et des techniques (STS), de la sociologie du numérique et des études sociales de l'économie.

Les concepteurs ont une vision : un monde dépourvu de centres administratifs, économiques, juridiques et techniques ; un monde où chacun formule souverainement ses relations. Ils le font advenir en développant des protocoles réseaux, des logiciels et des modèles d'affaires qui donnent aux relations une forme particulière : la transaction. La thèse analyse cette ingénierie comme une manière originale de gouverner les relations. Cette gouvernance par les transactions suppose deux opérations (inscription et programmation) par des dispositifs conçus, financés et diffusés au travers de réseaux associatifs et entrepreneuriaux étendus. Symétriquement, certains concepteurs cherchent à gouverner l'activité de conception elle-même par les transactions.

MOTS CLÉS

architecture, argent, blockchain, cryptomonnaie, décentralisation, finance, gouvernance, infrastructure, Internet, numérique, plateforme, protocole, transaction, Science & Technology Studies (STS), valorisation, Web

ABSTRACT

Blockchain designers invent new ways of relating through digital infrastructures. They are developed both within public and private institutions and by cryptocurrency communities that seek to avoid these institutions. This thesis aims to capture the political dimensions of this innovation process by reporting on the activity of developers, engineers, entrepreneurs, investors, corporate executives and activists. It is based on a multi-sited ethnographic investigation of the Ethereum design process between 2018 and 2020 in France, Singapore and online. This thesis is situated at the intersection of Science & Technology Studies (STS), digital sociology, and social studies of the economy.

The designers have a vision: a world devoid of administrative, economic, legal or technical center; a world in which each person sovereignly formulates his or her relations. They make it happen by developing network protocols, software and business models that give relationships a particular form: the transaction. The thesis analyzes this engineering as an original way of governing relationships. This governance by transactions is conceived by two operations on transactions (registration and programming) integrated in devices that are financed and diffused through extended associative and entrepreneurial networks. Symmetrically, some designers seek to govern the design activity itself through transactions.

KEYWORDS

architecture, blockchain, cryptocurrency, decentralization, digital, finance, governance, infrastructure, internet, money, platform, protocol, sovereignty, transaction, Science & Technology Studies (STS), valuation, Web