

Ecole doctorale de l'EHESS

Centre d'Étude des Mouvements Sociaux (CEMS)

Doctorat

Discipline : Économie et Sciences sociales

**ROLLAND MAËL**

**Au-delà des codes : infrastructure et gouvernance  
discrète et polycentrique des cryptomonnaies  
Bitcoin et Ethereum dévoilées par leurs crises**

**Thèse dirigée par:** Ève Chiapello

**Date de soutenance : le 13 décembre 2024**

- |      |   |   |
|------|---|---|
| Jury | 1 | Francesca Musiani, CNRS (Rapportrice)                               |
|      | 2 | Jérôme Blanc, Science Po Lyon (Rapporteur)                          |
|      | 3 | Jézabel Couppey-Soubeyran, Paris 1 Panthéon Sorbonne (Examinateuse) |
|      | 4 | Éric Monnet, Ehess et Paris School of Economics (Examinateur)       |
|      | 5 | Alexandre Mallard, Mines Paris (Examinateur)                        |

*À Hanna, Nils et Mina*

## REMERCIEMENTS

Cette thèse est l'aboutissement d'un long parcours d'apprentissage du métier de chercheur. Comme toute production scientifique (ou qui aspire à l'être), elle est le résultat d'un travail collectif. Pourtant, les contributions et soutiens essentiels qui ont jalonné ce parcours resteront dans l'ombre, car c'est en mon seul nom que cette thèse est déposée, enregistrée et sera (je l'espère) citée. Ces quelques pages de remerciements sont dédiées à les honorer.

Ma reconnaissance infinie va à Ève Chiapello, ma directrice de thèse. Sa présence et son attention pour mes travaux et pour moi-même, son professionnalisme, sa sagacité, mais aussi son affection et son soutien indéfectibles, pendant six ans et ce, dans chacune des épreuves de mon parcours, ont été essentiels à la direction prise et à l'achèvement de cette thèse. Je ne la remercierai jamais assez.

Je tiens à exprimer ma gratitude à Francesca Musiani, Jézabel Couppey-Soubeyran et Jérôme Blanc d'avoir accepté de faire partie du jury de cette thèse et pour leurs travaux qui l'ont nourrie. Je remercie Alexandre Mallard et Éric Monnet pour avoir de surcroît accompagné ce travail pendant quatre ans au sein du comité de thèse. Leurs remarques et critiques ont été cruciales dans l'avancement, l'approfondissement et l'achèvement de ce travail.

Je témoigne aussi toute ma reconnaissance à l'EHESS, à mon laboratoire le Centre d'Études des Mouvements Sociaux (CEMS) et au personnel administratif et technique qui m'a accompagné toutes ces années. Je remercie en particulier Zouhour Ben Salah, Guillaume Braunstein, Joëlle Caugnon, pour leurs travaux d'accompagnement quotidien.

Je remercie chaleureusement mes collègues et ami.e.s docteur.e.s et doctorant.e.s, Mehdi Arfaoui, Vincenzo Buffa, Hélène Croguenne-Le Saout, Antoine Leymarie, Juliette Marin, Ilias Naji, Damien Piron, Lukas Posselt, Camille Rivière, Océane Ronal, Virginia Santilli, Antonin Thyrard, dont les relectures, critiques et réflexions constructives ont contribué à ce manuscrit.

Mes remerciements vont ensuite aux membres du Cercle du Coin, tout particulièrement Jacques Favier, Benoît Huguet, Adli Takkal Bataille, Adrian Sauzade ainsi qu'à Laurence Allard et toutes celles et ceux avec qui j'ai eu le plaisir d'échanger et de débattre. Pour les échanges fructueux, les étudiant.e.s et intervenant.e.s du cours « *Espace(s) monétaire(s), monnaies parallèles, crypto-monnaies et crises institutionnelles* », donné de 2016 à 2019 à l'EHESS, comme les étudiant.e.s et

les chargé.e.s de travaux dirigés de l'ESILV et l'ESGI. Tous les coiners qui m'ont fait confiance et ont accepté de me parler, ce travail leur doit beaucoup.

Je remercie chaleureusement les professeurs, chercheur.e.s et étudiant.e.s qui ont accompagné et inspiré mon parcours académique, de l'université de Chambéry en passant par Paris X Nanterre, l'ENS et l'EHESS. Je ne peux que trop remercier Jacques Sapir et les membres de feu le Centre d'Études des Moyens d'Industrialisation (CEMI-Ehess) d'avoir accompagné mes premières recherches sur la monnaie et les CM, ainsi que de m'avoir offert de les présenter en Russie.

Je tiens à saluer le travail de correction de Xavier Van Welden et Isabelle San Juan et leur exprime toute ma reconnaissance.

Enfin, j'exprime ma profonde gratitude à mes proches et à ma famille, qui ont accompagné cette thèse, avec ses défis et sa précarité. Une immense reconnaissance va à Hanna, qui m'a épaulé avec patience durant ces années. Son soutien affectif, matériel et ses encouragements constants ont rendu possible ce travail. Merci à mes enfants, Nils et Mina, qui ont dû composer avec un papa en fin de thèse. Et enfin, je remercie mes parents et amis, pour leur soutien indéfectible et leurs encouragements. Ils et elles ont tous et toutes contribué, d'une manière ou d'une autre, à l'achèvement de cette thèse.

## RÉSUMÉ ET MOTS CLÉS

**Titre : Au-delà des codes : infrastructure et gouvernance discrète et polycentrique des cryptomonnaies Bitcoin et Ethereum dévoilées par leurs crises.**

**Résumé :** Cette thèse étudie les cryptomonnaies (CM) Bitcoin et Ethereum et leur gouvernance, en interrogeant les prétentions libérales-technicistes qui les présentent comme des monnaies acéphales, décentralisées, autonomes, neutres et apolitiques du fait de leur nature technique.

Ces prétentions reposent sur un « technologisme » dissociant technique et société, un premier écueil à dépasser, dominant dans la littérature axée sur les caractéristiques techniques des CM. Le second écueil est le « sociologisme » inverse, réduisant toute nature socio-politique à leur origine libertarienne. Au-delà, les CM sont des infrastructures composites et négociées où technique et monde social s'influencent mutuellement dans un va-et-vient politique.

Notre approche croise l'institutionnalisme monétaire, l'ethnographie économique et la sociologie des sciences et techniques, et repose sur des matériaux quantitatifs et qualitatifs tirés d'une enquête multiniveau (en ligne et hors ligne) alliant analyses documentaires, immersions participantes, observations participantes et entretiens. La gouvernance des CM est examinée au travers de deux crises : Bitcoin CVE 2018 et le *Hard Fork* d'Ethereum suite à « The DAO ».

La conception de Bitcoin et Ethereum, notamment le consensus PoW et l'émission monétaire des UCN, résulte de négociation hybride idéelle et matérielle. Un protocole ne devient CM qu'en tant qu'infrastructure, *confronté* à des usages, à d'autres arrangements pour s'y connecter, à une maintenance et des évolutions qui en renégocient formes, contenus et normativité. Réductible ni aux desseins de Nakamoto, ni à ses frontières protocolaires, Bitcoin est « sans couture » à l'aune d'un développement *carnavalesque* en trois phases (preuve de concept, péché et maturation). La comparaison avec Ethereum met en lumière sa propre normativité ainsi que celle de Bitcoin, dont elle vise à s'émanciper. Dans la controverse sur le statut monétaire des CM, nous affirmons que celles-ci sont des monnaies. Nous rejetons les perspectives monétaires orthodoxes – en termes d'exclusivité et d'homogénéité – les reléguant au statut d'actifs financiers, depuis un institutionnalisme monétaire intéressé aux usages. Empiriquement, les CM donnent lieu à des usages en compte et en paiement et sont des monnaies communautaires. Leur singularité monétaire réside dans une logique fiduciaire à *consensus distribué* : leur valeur et pouvoir d'achat sont garantis par des institutions et des acteurs sociaux dans le cadre d'une gouvernance polycentrique. Le phénomène de crise permet d'identifier deux types de crises de CM - les *crises de vulnérabilité* et les *crises d'évolution* – et une gouvernance de crise à deux volets : de *huis clos*, routinière à consensus local, ou *publique*, conflictuelle et à consensus global. La première est encadrée par des spécialistes (Core Devs) tandis que, en cas de dissensus, la seconde mobilise largement les parties prenantes pour rechercher une légitimité communautaire à travers des débats et des mesures de consensus. Dans tous les cas, la gouvernance polycentrique permet la formation d'un consensus tout en garantissant traçabilité, vérification et participation aux décisions. Finalement, nous démontrons que le consensus social (espace de la discréption) prime toujours face aux codes irrespectueux de l'esprit communautaire (espace de la règle).

**Mots clés :** Cryptomonnaie, Bitcoin, Ethereum, Gouvernance polycentrique, Ethnographie, Institutionnalisme Monétaire, Sociologies des Sciences et Technologies, Crises, Monnaie.

## ABSTRACT AND KEYWORDS

### **Title : Beyond the Codes: Discreet and Polycentric Infrastructure and Governance of Bitcoin and Ethereum CMs Unveiled by Their Crises**

**Summary :** This thesis studies the Bitcoin and Ethereum CMs and their governance, questioning the liberal-technicist claims that portray them as acephalous, decentralized, autonomous, neutral and apolitical currencies by virtue of their technical nature.

These pretensions are rooted in a “technologism” that dissociates technology and society, a first pitfall to overcome, dominant in the literature focused on CMs’ technical traits. The second pitfall is an inverse “sociologism” that reduces any socio-political nature to their libertarian origins. Beyond this, CMs are composite, negotiated infrastructures where technology and the social world mutually influence each other in a political interplay.

Our approach crosses monetary institutionalism, economic ethnography and the sociology of science and technology, and relies on quantitative and qualitative material drawn from a multi-level survey (online and offline) combining documentary analysis, participant immersions, participant observations and interviews. CM governance is examined through two crises - Bitcoin CVE 2018 and Ethereum's hard Fork after “The DAO”.

The design of Bitcoin and Ethereum, notably the PoW consensus and the monetary issuance of UCNs, results from ideal and material hybrid bargaining. A protocol becomes CM only as an infrastructure, *confronted* with uses, other arrangements enabling connection, maintenance and evolutions that renegotiate its form, content and normativity. Neither reducible to Nakamoto’s designs nor its protocol boundaries, Bitcoin is ‘seamless’ through its *carnivalesque* three-phase development (proof of concept, sin, and maturation). In comparison, Ethereum’s own normativity contrasts it with Bitcoin’s, from which it seeks to emancipate. In the controversy surrounding the monetary status of CMs, we assert that CMs are currencies, rejecting orthodox monetary perspectives – in terms of exclusivity and homogeneity – relegating CMs to the status of financial assets. From a monetary institutionalist’s point of view, CMs are empirically used as accounts and payments, and are community currencies. Their monetary uniqueness lies in their unprecedented fiduciary logic of distributed consensus : their value and purchasing power are guaranteed by institutions and social players within the bounds of their polycentric governance. The crisis phenomenon allows us to identify two types of CM crises – *vulnerability* crises and *evolution* crises – and a two-fold crisis governance: *huis clos*, routinized with local consensus or *public*, conflictual with global consensus. The former is overseen by specialists (Core Dev), while in the event of dissensus, the latter widely mobilizes all stakeholders to seek community legitimacy through debate and consensus-building measures. In all cases, polycentric governance enables consensus-formation while guaranteeing traceability, verification and participation in decision-making. In the end, we find that social consensus (the space of discretion) always takes precedence over disrespectful codes of community spirit (the space of rule).

**Keywords :** Cryptocurrency, Bitcoin, Ethereum, Polycentric governance, Ethnography, Monetary institutionalism, Sociologies of Science and Technology, Crises, Money

## TABLE DES MATIÈRES

|  |           |
|--|-----------|
| <b>REMERCIEMENTS .....</b>   | <b>2</b>  |
| <b>RÉSUMÉ ET MOTS CLÉS.....</b>  | <b>4</b>  |
| <b>ABSTRACT AND KEYWORDS .....</b>   | <b>5</b>  |
| <b>TABLE DES MATIÈRES .....</b>  | <b>6</b>  |
| <b>TABLE DES TABLEAUX .....</b>  | <b>11</b> |
| <b>TABLE DES ILLUSTRATIONS .....</b>   | <b>12</b> |
| FIGURES.....   | 12        |
| CHRONOLOGIES .....   | 12        |
| <b>PRÉCAUTIONS D'ÉCRITURE.....</b>   | <b>13</b> |
| <b>SIGLES UTILISÉS .....</b>   | <b>14</b> |
| <b>INTRODUCTION GÉNÉRALE.....</b>  | <b>15</b> |
| A.     LA GOUVERNANCE DES CM : CONSTRUCTION DE NOTRE OBJET DE RECHERCHE.....   | 17        |
| 1) <i>Un intérêt pour la monnaie et les « Objets Monétaires Non Identifiés » .....</i>   | 18        |
| 2) <i>La controverse sur le caractère monétaire des cryptomonnaies.....</i>  | 19        |
| 3) <i>Révéler l'« indicible » gouvernance des CM contre les prétentions libérales technicistes.....</i>                                    | 21        |
| B.     LA GOUVERNANCE DES CM DÉVOILÉE PAR LEURS CRISES : UN INSTITUTIONNALISME ARTICULÉ À UNE  |           |
| SOCILOGIE DES SCIENCES ET TECHNIQUES.....  | 24        |
| 1) <i>L'institutionnalisme monétaire pour caractériser les CM comme monnaies.....</i>  | 24        |
| Notre insatisfaction vis-à-vis de la théorie monétaire dominante.....  | 25        |
| Analyser le phénomène monétaire sans l'amputer : un institutionnalisme premier .....   | 27        |
| 2) <i>Gouvernance des CM : perspectives sociologiques .....</i>  | 28        |
| Anthropologie, ethnographie et sociologie de la monnaie : l'empirie des usages.....  | 29        |
| Au-delà des « boîtes noires » : les CM, des infrastructures « sans coutures » .....  | 30        |
| 3) <i>La gouvernance de Bitcoin et d'Ethereum dévoilée par leurs crises.....</i>   | 32        |
| Les fonctions heuristiques et hermétiques des « crises » .....   | 32        |
| Du périmètre de nos terrains : deux crises différencieront Bitcoin et Ethereum .....   | 33        |
| C.     UNE DÉMARCHE ETHNOGRAPHIQUE, POUR UN TERRAIN D'ENQUÊTE MULTI-NIVEAU .....   | 34        |
| 1) <i>Enquêter sur la gouvernance des CM : contraintes et enjeux.....</i>  | 34        |
| Enjeux méthodologiques.....  | 34        |
| La relation enquêteur-enquêtés .....   | 36        |
| 2) <i>Stratégie d'accès et matériaux de terrain récoltés .....</i>   | 39        |
| La face « en ligne » des CM : d'une entrée par voie de recherche documentaire au saut de l'« immersion participante ».....                 | 43        |
| « Creuser au fond du terrier » : les recherches documentaires, une source essentielle de connaissance de ce champ .....                    | 43        |
| S'approcher des acteurs non humains : des immersions participantes nombreuses et « fructueuses » ..  | 44        |
| L'envers « hors ligne » : au contact des acteurs par observations et entretiens .....  | 46        |
| Observations participantes d'évènement hors ligne : premiers contacts en présence d'acteurs humains .....                                  | 46        |
| Entretiens.....  | 46        |
| D.     OBJECTIFS, APPORTS ET ORGANISATION GÉNÉRALE DE LA THÈSE .....   | 47        |
| E.     DÉCLARATION D'INTÉRÉTS.....   | 51        |
| <b>CHAPITRE I - L'ÉMERGENCE DU PHÉNOMÈNE DES CRYPTOMONNAIES (CM) : BITCOIN ET<br/>ETHEREUM COMME INFRASTRUCTURES SOCIOTECHNIQUES .....</b> | <b>52</b> |
| I.1     QUAND BITCOIN DÉFINIT SON MONDE... : L'ALOI POLITIQUE D'UNE CM PIONNIÈRE .....   | 55        |
| I.1.1 <i>Du terreau matériel et idéal aux racines de Bitcoin.....</i>  | 58        |
| Une monnaie frappée au coin de philosophies politiques et d'expériences pratiques .....  | 59        |
| Une création hétérodoxe, entre recherche académique et recherche appliquée .....   | 65        |
| I.1.2 <i>Bitcoin : une chimère théorico-pratique très politique.....</i>   | 68        |
| Des composants sociotechniques anciens singulièrement recomposés .....   | 69        |
| L'usage de la PoW : un « jeu » d'incitations très politique .....  | 73        |
| I.1.3 <i>Le fonctionnement de Bitcoin suivant le script original de Nakamoto.....</i>  | 78        |

|   |            |
|---|------------|
| Production individuelle d'une transaction* Bitcoin.....   | 80         |
| (0) Les Préalables : disposer d'un portefeuille et d'UCN .....  | 80         |
| (1) Créer et diffuser une transaction* Bitcoin .....  | 80         |
| Production collective d'un consensus sur un registre transactionnel commun.....   | 81         |
| (2) Le traitement distribué des transactions* par « minage » : vérification, ordonnancement, production et diffusion d'un enregistrement candidat* valide ..... | 82         |
| (3) Vérification et intégration d'un bloc candidat valide dans le registre canonique commun .....   | 82         |
| (3 bis) Réorganisation de l'historique, Fork de chain et bloc orphelin .....  | 83         |
| I.2 QUAND LE « MONDE REDÉFINIT » BITCOIN DE MANIÈRE CARNAVALESQUE.....  | 84         |
| I.2.1 <i>Un développement infrastructurel au-delà du protocole Bitcoin</i> .....  | 89         |
| La phase de « preuve de concept » (de juillet 2008 à mars 2012) .....   | 89         |
| La phase de « péché » (d'avril 2012 à octobre 2013) .....   | 93         |
| La phase de « maturation » (de novembre de 2013 à aujourd'hui) .....  | 96         |
| I.2.1 <i>Un protocole débordé de « carnavalesques » improvisations d'acteurs</i> .....  | 100        |
| Des renégociations pratiques : réintermédiation de l'accès à Bitcoin et de l'activité de traitement des transactions.....                                       | 100        |
| Un protocole Bitcoin qui s'adapte : des régulations transactionnelles très politiques .....   | 106        |
| I.3 ETHEREUM : UNE RUPTURE ASSUMÉE D'AVEC BITCOIN ET LES PREMIERS ALTCOINS.....   | 109        |
| I.3.1 <i>De la constellation des Altcoins : construire « sur » ou « à côté » de Bitcoin</i> .....   | 111        |
| « Namecoin », entre complémentarité et indépendance vis-à-vis de Bitcoin.....   | 111        |
| Des CM qui s'émancipent de plus en plus de l'architecture Bitcoin .....   | 114        |
| Guerre des « métaprotooles » : modifier Bitcoin pour en interdire certains usages .....   | 118        |
| I.3.2 <i>Ethereum : continuité et rupture d'avec Bitcoin et les expériences passées</i> .....   | 123        |
| Ethereum : une conception par des <i>insiders</i> reconnus de l'écosystème des CM .....   | 123        |
| Ethereum : une synthèse matérielle et idéelle critique des expériences passées .....  | 125        |
| I.3.3 <i>Ethereum, des recompositions d'alliances contre les rigidités de Bitcoin</i> .....   | 128        |
| Ethereum : des arbitrages sociotechniques différenciés .....  | 128        |
| Ethereum contre Bitcoin ? Emprunts et différences de fonctionnement .....   | 131        |
| Ethereum : des réformes du consensus et du monnayage en forme de révolution.....  | 134        |
| I.4 CONCLUSION DU CHAPITRE I .....  | 140        |
| <b>CHAPITRE II - DÉPASSER LA CONTROVERSE DU STATUT MONÉTAIRE DES CM PAR UN INSTITUTIONNALISME INTÉRESSÉ AUX USAGES.....</b>                                     | <b>142</b> |
| II.1 « LES CM NE SONT PAS MONNAIE ! » : ARGUMENTS CONTRE LE CARACTÈRE MONÉTAIRE DES CM .....  | 147        |
| II.1.1 <i>La critique des CM depuis les grands courants de théorie monétaire</i> .....  | 148        |
| Les critiques instrumentales fondées sur des fonctions monétaires canoniques .....  | 148        |
| Une monnaie « créature de l'État » : les critiques nominalistes et chartalistes.....  | 151        |
| II.1.2 <i>Les CM comme épreuve d'explicitation de l'argent : des « monstres monétaires » difficilement qualifiables</i> .....                                   | 154        |
| Des objets non couverts par les catégories juridiques et empiriques de la monnaie .....   | 154        |
| Statut règlementaire des CM : non-qualification, disqualification et requalification .....  | 156        |
| II.2 « POURTANT, ELLES FONT MONNAIE » ! À L'AUNE D'UN NOMINALISME « NON ÉTATISTE » ATTENTIF AUX USAGES .....  | 160        |
| II.2.1 <i>Des chimères monétaires inédites, reléguées à des usages spéculatifs</i> .....  | 161        |
| Les CM : des chimères monétaires inédites... de mauvais aloi .....  | 162        |
| Des critiques paradoxales et syncrétiques, confinant les CM au rôle d'actif financier.....  | 163        |
| II.2.2 <i>L'Institutionnalisme Monétaire Francophone : un nominalisme non étatique, apte à contenir les CM</i> .....  | 165        |
| Au-delà de la monnaie, l'argent : questionner la monétisation à l'aune des usages.....  | 167        |
| La monnaie comme système de paiement : monétisation et liquidité de dettes hétérogènes .....  | 168        |
| La monnaie à l'épreuve : quand dettes, confiance et souveraineté se confrontent .....   | 170        |
| II.2.3 <i>Au-delà des critiques instrumentales et chartalistes : des CM ni unitaires, ni exclusives</i> ...   | 173        |
| L'irréductible hétérogénéité des monnaies d'hier et d'aujourd'hui .....   | 173        |
| Monnaies nationales et monnaies parallèles, un espace monétaire toujours contesté .....   | 175        |
| Des cryptomonnaies parallèles : usages monétaires des UCN BTC et ETH .....  | 177        |
| L'impérieuse mise en forme des UCN BTC et ETH .....   | 177        |
| Usage en compte et en paiement .....  | 179        |
| De l'usage - non monétaire - en réserve de valeur .....   | 182        |
| II.3 AU-DELÀ DE LA REVENDICATION D'UNE ABSENCE DE GOUVERNANCE ! .....   | 185        |
| II.3.1 <i>D'un concept de gouvernance problématique à la problématique de la gouvernance des CM</i> .....   | 186        |
| Du concept de gouvernance et de sa polysémie : un concept normatif premier .....  | 187        |
| Retournement positif du concept : réintégrer le pouvoir et la politique .....   | 188        |

|   |            |
|---|------------|
| <i>II.3.2 Quand les CM réactivent un débat monétaire ancien : conflit symbolique et matériel autour de la « bonne » gouvernance des CM.....</i>             | 190        |
| De la bonne monnaie à la bonne gouvernance : une approche normative partagée par les <i>coiners</i> et leurs détracteurs.....                               | 191        |
| De la « règle contre la discréption » à la « discréption-contrainte ».....  | 192        |
| Les CM : une radicalisation théorique et pratique de la règle ? .....   | 194        |
| Une opposition quant à la « bonne » gouvernance des CM.....   | 195        |
| Pour les coiners : une absence de gouvernance, marque d'une monnaie absolument « bonne ».....   | 196        |
| Pour les professionnels de l'argent : une absence de gouvernance, marque d'une monnaie absolument « mauvaise » .....  | 197        |
| Les autorités monétaires et leurs capacités de régulation en péril ? .....  | 199        |
| <i>II.3.3 Caractériser la gouvernance des CM hors normativité en surplomb : enjeu théorique et pratique d'un éclaircissement catégoriel primordial.....</i> | 202        |
| Communautés hétérogènes, controverses, gouvernance duale et polycentrique.....  | 203        |
| Une anarchie catégorielle problématique .....   | 210        |
| Caractériser la gouvernance des CM : une voie de remise en ordre ? .....  | 212        |
| <b>II.4 CONCLUSION DU CHAPITRE II.....</b>  | <b>216</b> |
| <b>CHAPITRE III - AU-DELÀ DES CODES : LA GOUVERNANCE DISCRÈTE DES CM, DÉVOILÉE PAR LEURS CRISES .....</b>   | <b>220</b> |
| <b>III.1 CRISE BITCOIN CVE 2018 17144 : D'UNE CRISE À DE NOMBREUSES AUTRES.....</b>   | <b>224</b> |
| <i>III.1.1 Présentation périodisée de la crise Bitcoin CVE 2018 .....</i>   | <i>225</i> |
| Une mise en crise longue et silencieuse .....   | 227        |
| Insémination/gestation : une « étrange confluence d'événements » potentiellement catastrophiques  | 227        |
| D'un déclenchement confidentiel par « divulgation responsable » .....   | 232        |
| Une remise en ordre rapide .....  | 235        |
| La phase d'évaluation : définition des problèmes, des solutions et d'une stratégie de résolution.....   | 235        |
| La phase de résolution : « mensonge blanc » contre « chapeau noir ».....  | 237        |
| <i>III.1.2 Restituer cette crise dans l'histoire de celles traversées par Bitcoin .....</i>   | <i>241</i> |
| De la diversité des crises aux crises protocolaires des CM .....  | 242        |
| Enjeux des crises Bitcoin : labellisations indigènes et exemples historiques .....  | 243        |
| Crise de « faux monnayage », ou l'immutabilité des règles de monnayages en question .....   | 247        |
| Crise de « scission de chaîne » : l'unicité des paiements mise en péril .....   | 249        |
| Crise de « DOS » : dégradation de l'accessibilité au réseau et de la praticité des paiements .....  | 251        |
| D'autres types de crises passées et encore à découvrir .....  | 252        |
| <b>III.2 DES MARQUES D'UNE POLITIQUE DE CRISES : UNE GOUVERNANCE DE HUIS CLOS ROUTINIÈRE.....</b>   | <b>254</b> |
| <i>III.2.1 Des acteurs au cœur de la gouvernance sur le protocole.....</i>  | <i>255</i> |
| De l'âme des acteurs non humains : d'un « esprit du code » excédant sa « lettre » .....   | 255        |
| La diversité des acteurs non humains en question : l'hégémonie de « Bitcoin Core » en crise ? .....   | 259        |
| Qui peut modifier Bitcoin ? Bitcoin Core, un groupe en charge de maintenir et sécuriser Bitcoin ? .....   | 262        |
| <i>III.2.2 Où modifier Bitcoin ? Un « repo Bitcoin Core » encadré et hiérarchisé.....</i>   | <i>265</i> |
| Le répertoire « Bitcoin Core » et son administration .....  | 265        |
| D'une hiérarchie formelle selon le principe « du moindre privilège » à la désignation informelle des mainteneurs « Core » .....                             | 269        |
| Une technocratie soumise à consensus communautaire : entre confiance et défiance .....  | 273        |
| <i>III.2.3 Bitcoin CVE 2018 : une gouvernance de huis clos suspendue à l'absence de dissensus public</i>  | <i>277</i> |
| Maintenance ou innovation ? Deux procédures d'évolution protocolaire différenciées.....   | 277        |
| Gouvernance de huis clos : consensus local <i>ex ante</i> entre une poignée d'acteurs en réseau* .....  | 281        |
| Unanime et inaperçu : l'Audience Publique sans vague d'une crise et sa résolution.....  | 284        |
| <b>III.3 UNE GOUVERNANCE PUBLIQUE D'EXCEPTION : LE HARD FORK D'ETHEREUM CONSÉCUTIF À L'ATTAQUE DE « THE DAO » .....</b>                                     | <b>287</b> |
| <i>III.3.1 Une mise en crise brutale, publique et tapageuse .....</i>   | <i>288</i> |
| Périodisation du Hard Fork* de « The DAO » .....  | 289        |
| Phase d'insémination : démesure d'un fonds d'investissement distribué sur Ethereum .....  | 291        |
| Le déclenchement : des alertes variées précédant l'attaque de « The DAO » .....   | 298        |
| <i>III.3.2 Une remise en ordre complexe, contrainte et controversée : moyens et enjeux d'un consensus multi-acteur .....</i>                                | <i>303</i> |
| Une cellule de crise à l'image des stratégies de remédiation : diversifiée .....  | 304        |
| 50 nuances de « Code is Law » : un diagnostic et des stratégies de remédiation controversés .....   | 306        |
| « Ne rien faire » (1).....  | 307        |
| « Sauve-qui-peut » <i>au sein</i> de « la lettre du code ».....   | 310        |
| « Se sauver soi-même au détriment des autres » (2-b) .....  | 310        |

|  |              |
|--|--------------|
| « Contre-attaquer : action collective et coordonnée en vue d'un intérêt commun » (2 – c, d, e).....  | 311          |
| <b>III.3.3    Gouvernance ouverte et publique pour des Forks controversés .....</b>  | <b>314</b>   |
| « To Fork or not to Fork » : enjeux et controverses théoriques autour des Forks.....   | 314          |
| La production d'un Fork : processus incertain, multi-acteur et multiniveau .....   | 316          |
| Arènes et dispositifs d'expression du désaccord : le camp du <i>Hard Fork*</i> rallié par la majorité.....                                       | 320          |
| <b>III.3.4    « Fork You ?! » : une scission surprise fondatrice et ses enseignements .....</b>  | <b>322</b>   |
| Un <i>Hard Fork</i> et ses attendus théoriques.....  | 322          |
| Un <i>Hard Fork</i> contentieux inédit : la sécession d'Ethereum Classic.....  | 324          |
| Se séparer pour mieux se retrouver : fin d'une remise en ordre et ses enseignements .....  | 326          |
| <b>III.4    CONCLUSION DU CHAPITRE III .....</b>   | <b>329</b>   |
| <b>CONCLUSION GÉNÉRALE.....</b>  | <b>332</b>   |
| RÉSUMÉ DE LA THÈSE.....  | 332          |
| DÉCRYPTER LA CRYPTO PAR L'APPROCHE INFRASTRUCTURELLE.....  | 334          |
| DE L'ACÉPHALISME APOLITIQUE DES CM À L'ÉPREUVE D'UNE SOCIOLOGIE DES CRISES.....  | 336          |
| UNE INTÉGRATION COHÉRENTE DES CM DANS LE CHAMP DE LA THÉORIE MONÉTAIRE.....  | 337          |
| UN EFFORT DE TRADUCTION ATTENTIF AUX ET À L'ATTENTION DES ACTEURS .....  | 337          |
| LES CM : BOUCS ÉMISSAIRES COMMODES D'UN SYSTÈME MONÉTAIRE EN CRISE ? .....   | 338          |
| <b>BIBLIOGRAPHIE.....</b>  | <b>341</b>   |
| <b>LIVRET 2 : GLOSSAIRE &amp; ANNEXES .....</b>  | <b>I</b>     |
| GLOSSAIRE : CRYPTOMONNAIE ET PROTOCOLE DE REGISTRE DISTRIBUÉ .....   | II           |
| ANNEXES .....  | X            |
| <i>Annexe I : Données synthétiques relatives à l'écosystème des CM pris dans son ensemble .....</i>  | <i>XII</i>   |
| Annexe I.1 : Capitalisation totale et taux de dominance sur le marché des crypto-actifs (~5868 actifs listés sur Coingecko), au 01/09/2020 ..... | XII          |
| Annexe I.2 : Capitalisation totale et taux de dominance de marché des crypto-actifs (~5868 actifs listés), au 01/09/2020 .....                   | XIV          |
| Annexe I.3 : Évolution du nombre d'utilisateurs de la plateforme Coinbase .....  | XVI          |
| Annexe I.4 : Chronologies circonstanciées du phénomène des Initial Coin Offering (ICO), de juillet 2013 à juin 2017 .....                        | XVII         |
| <i>Annexe II : Données synthétiques relatives à l'écosystème de Bitcoin .....</i>  | <i>XVIII</i> |
| Annexe II.1 : L'UCN bitcoin et sa décimalisation (matérielle et symbolique) .....  | XVIII        |
| Annexe II.2 : Une offre monétaire programmatique : entre émission anticipée et effective .....   | XIX          |
| Annexe II.3 : Capitalisation de marché du BTC, en prix de marché <sup>(1)</sup> et réalisée <sup>(2)</sup> , en USD.....                         | XX           |
| Annexe II.4 : Nombre d'adresses actives <sup>(1)</sup> et taille moyenne des enregistrements (en bytes), quotidien                               | XXI          |
| Annexe II.5 : Nombre de transactions <sup>(2)</sup> et transferts <sup>(3)</sup> quotidiens.....   | XXI          |
| Annexe II.6 : Taille globale de tous les transferts quotidiens, BTC et USD <sup>(1)</sup> .....  | XXII         |
| Annexe II.7 : Taille moyenne des transferts, en BTC et USD, quotidien <sup>(2)</sup> .....   | XXII         |
| Annexe II.8 : Taille médiane des transferts, en BTC et USD, quotidien <sup>(1)</sup> .....   | XXIII        |
| Annexe II.9 : Somme des frais de transaction, en BTC et USD, quotidien <sup>(2)</sup> .....  | XXIII        |
| Annexe II.10 : Frais de transaction, moyen et médian, en BTC et USD, quotidien <sup>(1)</sup> .....  | XXIV         |
| Annexe II.11 : Revenu cumulé des « mineurs » en USD <sup>(2)</sup> .....   | XXIV         |
| Annexe II.12 : Quantité Hash/s cumulée <sup>(1)</sup> et prix du BTC, en USD, quotidien .....  | XXV          |
| Annexe II.13 : Évolution de l'index de consommation électrique de Bitcoin, en TWH annualisé <sup>(2)</sup> .....                                 | XXV          |
| Annexe II.14 : Volatilité de l'UCN BTC, en USD sur 30, 60 et 180 jours <sup>(1)</sup> .....  | XXVI         |
| <i>Annexe III : Données synthétiques relatives à l'écosystème d'Ethereum .....</i>   | <i>XXVII</i> |
| Tableau III.1: L'UCN Ether et sa décimalisation (matérielle et symbolique) .....   | XXVII        |
| Annexe III.2 : l'offre monétaire programmatique d'Ethereum : entre émission anticipée et effective .....   | XXIX         |
| Figure III.3 : Capitalisation de marché de l'ETH en prix de marché (1), en USD .....   | XXX          |
| Annexe III.4 : Nombre d'adresses actives <sup>(1)</sup> et taille moyenne des enregistrements (en bytes), quotidien .....                        | XXXI         |
| Annexe III.5 : Nombre de transactions <sup>(2)</sup> et transferts <sup>(3)</sup> quotidiens .....   | XXXI         |
| Annexe III.6 : Taille globale de tous les transferts quotidiens, ETH et USD <sup>(1)</sup> .....   | XXXII        |
| Annexe III.7 : Taille moyenne des transferts, en ETH et USD, quotidien <sup>(2)</sup> .....  | XXXII        |
| Annexe III.8 : Taille médiane des transferts, en ETH et USD, quotidien <sup>(1)</sup> .....  | XXXIII       |
| Annexe III.9 : Somme des frais de transaction, en ETH et USD, quotidien <sup>(2)</sup> .....   | XXXIII       |
| Annexe III.10 : Frais de transaction, moyen et médian, en ETH et USD, quotidien <sup>(1)</sup> .....   | XXXIV        |
| Annexe III.11 : Revenu cumulé des « mineurs » en USD <sup>(2)</sup> .....  | XXXIV        |
| Annexe III.12 : quantité Hash/s cumulée <sup>(1)</sup> et prix de l'ETH en USD, quotidien .....  | XXXV         |
| Annexe III.13 : Volatilité de l'UCN ETH, en USD sur 30, 60 et 180 jours <sup>(2)</sup> .....   | XXXV         |
| Annexe III.14 : Les cofondateurs d'Ethereum .....  | XXXVI        |
| Annexe III.15 Ethereum Versus Ethereum Classic .....   | XL           |

|  |              |
|--|--------------|
| Annexe III.15.1 : Répartition du taux de Hash moyen entre ETH et ETC, quotidien <sup>(1)</sup> .....                               | XLI          |
| Annexe III.15.2 : Miner de l'ETH ou de l'ETC : un dilemme philosophique et économique <sup>(2)</sup> .....                         | XLI          |
| Annexe III.15.3 : Évolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum<br>Classic <sup>(3)</sup> ..... | XLII         |
| Annexe III.15.4 : Évolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum <sup>(4)</sup> .....            | XLII         |
| <i>Annexe IV: Données synthétiques relatives à nos stratégies et dispositifs d'accès au terrain.....</i>                           | <i>XLIII</i> |
| Annexe IV.2 : Détails des immersions participantes.....  | XLIII        |
| Annexe IV.2 : Détails des observations participantes .....   | L            |
| Annexe IV.3 : Statut(s) et Rôle(s) couvert(s) par les acteurs de nos entretiens .....  | LIII         |
| Annexe IV.4 : Liste des entretiens menés et notice biographique succincte des enquêtés.....  | LVI          |
| <i>Annexe V: Retours circonstanciés sur les composants clefs et le fonctionnement d'une CM.....</i>                                | <i>LXVII</i> |
| Annexe V.1 : Cryptographie asymétrique et souveraineté individuelle .....  | LXVII        |
| Annexe V.2 : Clefs privées, clefs publiques et adresses Bitcoin .....  | LXVII        |
| Annexe V.3 : La fonction de Hachage SHA 256 .....  | LXVIII       |
| .....  | LXVIII       |
| Annexe V.4 : L'arbre de Merkle .....   | LXVIII       |
| Annexe V.5 : Cas d'une réorganisation malicieuse de type « Attaque 51% ».....  | LXX          |
| Annexe V.6 : Relations hiérarchiques entre les trois couches d'un protocole de registre distribué .....                            | LXI          |

## TABLE DES TABLEAUX

|   |     |
|---|-----|
| Tableau 1 : Deux CM, deux crises, documentées suivant quatre dispositifs .....                            | 41  |
| Tableau 2 : Les quatre types de double dépense idéal-typiques sur Bitcoin .....                           | 228 |
| Tableau 3 : Nombre et parts relatives des nœuds vulnérables .....   | 240 |
| Tableau 4 : Labélisation indigène des vulnérabilités de Bitcoin .....                                     | 244 |
| Tableau 5 : Les deux grandes familles de crises protocolaires .....                                       | 258 |
| Tableau 6 : Nomenclature des contributions possibles aux répertoires « Bitcoin Core » .....               | 268 |
| Tableau 7 : Les priviléges d'administration du répertoire Bitcoin core .....                              | 270 |
| Tableau 8 : Les différents canaux d'information et de discussion mobilisés lors de la crise CVE 2018..... | 282 |
| Tableau 9 : L'équipe Slock It.....  | 292 |
| Tableau 10 : Les différents acteurs de la contre-attaque.....   | 313 |
| Tableau 11 : Ethereum, un réseau constitué d'implémentations diversifiées .....                           | 318 |

## TABLE DES ILLUSTRATIONS

### FIGURES

|   |     |
|---|-----|
| Figure 1 : Stratégies d'accès au terrain : quatre dispositifs et deux grands temps .....                | 40  |
| Figure 2 : Le théorème d'impossibilité de CAP .....   | 67  |
| Figure 3 : Le fonctionnement synthétique de Bitcoin à travers la réalisation d'une transaction....      | 79  |
| Figure 4 : Réorganisation et « bloc orphelin ».....   | 83  |
| Figure 5 : Division sociale du travail protocolaire et spécialisation des acteurs .....                 | 102 |
| Figure 6 : Une ontologie politique des CM en forme de triangle d'incompatibilité .....                  | 129 |
| Figure 7 : Cartographie préliminaire des parties prenantes à la gouvernance des CM.....                 | 208 |
| Figure 8 : Distinguer actifs numériques, crypto-actifs, monnaie numérique et cryptomonnaie....          | 215 |
| Figure 9 : D'une sédimentation de modifications des codes Bitcoin de 2011 à 2017 créant la faille ..... | 230 |
| Figure 10 : La divulgation du Bogue CVE 2018, ses étapes, ses risques et ses acteurs .....              | 233 |
| Figure 11 : Les quatre grands domaines de crise d'une CM .....  | 242 |
| Figure 12 : Deux procédures différencierées permettant de modifier les codes sources Bitcoin Core ..... | 278 |
| Figure 13 : Statuts, rôles et fonctionnements clefs de « The Dao » .....                                | 295 |
| Figure 14: : Trois types de stratégies de remédiation .....   | 303 |

### CHRONOLOGIES

|   |     |
|---|-----|
| Chronologie 1 : Bitcoin, un objet sociotechnique aux inspirations hétérogènes .....   | 57  |
| Chronologie 2 : L'institutionnalisation carnavalesque de l'infrastructure Bitcoin .....   | 88  |
| Chronologie 3 : Périodisation des événements entourant la crise ouverte par le bogue CVE 2018 .....   | 227 |
| Chronologie 4 : Bitcoin, une histoire rythmée de crises à gérer .....   | 246 |
| Chronologie 5 : Les différents acteurs disposant ou ayant disposé de droits spécifiques d'accès (« commit right ») et du rôle de « Core Mainteneurs » sur le répertoire Bitcoin Core..... | 271 |
| Chronologie 6 : Périodisation de la crise consécutive à l'attaque de « The Dao ».....   | 290 |

## PRÉCAUTIONS D'ÉCRITURE

- **Language *Emic*, *Etic* et *traduction*** : En sociologie et ethnographie, le langage *emic* (indigène) des acteurs se distingue du langage *etic* des chercheurs, différenciant leurs catégories de pensée. Face à une indétermination conceptuelle initiale, nous sommes parti du langage *emic* pour forger un langage *etic*, dont la visée est d'offrir un cadre conceptuel rigoureux, rendant le champ d'étude intelligible pour le monde académique et compréhensible pour les acteurs. Pour faciliter la compréhension de ce jargon, nous avons constitué un glossaire (voir Glossaire et Annexes).
- **Glossaire** : Pour faciliter la compréhension du jargon des *coiners*\* par les non-initiés, nous avons créé un glossaire (voir Glossaire et Annexes). Les termes définis dans le glossaire sont en italique et suivis d'un astérisque (\*) lors de leur première occurrence. Par la suite, ils ne sont suivis que d'un astérisque (\*).
- **Annexes** : Les annexes contiennent à la fois des données quantitatives et qualitatives. Trois jeux de données quantitatives ont été constitués : l'un pour l'écosystème global (Annexe I), et les deux autres pour Bitcoin (Annexe II) et Ethereum (Annexe III). Les données qualitatives renvoient à nos stratégies et dispositifs d'accès au terrain (Annexe IV), et à l'explicitation de notions clés du fonctionnement des CM (Annexe V). L'ensemble de ces données, utilisées dans les trois chapitres de la thèse, est renvoyé en annexes pour éviter redondance et surcharge, et pour en faciliter l'accès : comme le glossaire, les annexes sont conçues comme un livret détachable.
- **Règle grammaticale de genre** : Pour simplifier la lecture, nous utilisons le masculin neutre au pluriel. Bien que nous soyons conscient des problèmes liés à cet usage (masculinisation du langage, hiérarchie des sexes, etc.), il nous semble approprié compte tenu de la prédominance masculine dans ce domaine et de l'usage de l'anonymat/pseudonymat qui complique l'identification des genres.
- **Traduction** : La majorité des matériaux utilisés sont en anglais. Pour faciliter la lecture, nous avons traduit tous les extraits en français. Les textes originaux apparaissent en notes de bas de page, soit directement, soit *via* des liens vers les documents.
- **Règles bibliographiques** : Seuls les articles académiques et la littérature grise (rapports et notes) incluent des informations bibliographiques complètes (noms des auteurs, date de publication, pagination). L'absence de pagination indique soit que le matériau est issu de prises de position d'acteurs académiques et/ou d'institution plus informelle (article de journaux, vidéo, blogs), soit de sources indigènes. S'agissant de source numérique où la pagination est inexistante ou variable, elles sont présentées avec les seuls noms et dates de publication. Des liens hypertextes sont ajoutés en notes de bas de page si nécessaire.
- **Anonymat et protection des enquêtés** : Nous avons offert à tous les participants la possibilité d'être anonymisés. Ceux qui ont autorisé l'utilisation de leur vrai nom apparaîtront avec leur prénom et nom complet, et ceux ayant demandé à rester anonymes seront désignés par un pseudonyme (Anon suivi d'un numéro, voir Annexe IV.4). Certains matériaux « en off » ne seront pas attribués à leurs auteurs pour protéger leur identité. Nous avons créé un personnage anonyme (SuperAnon) pour porter ces paroles.

## SIGLES UTILISÉS

Tout au long de ce travail, certains termes seront, pour leur première occurrence, écrits en toutes lettres avec leur sigle entre parenthèses, puis, pour la suite du document, ils n'apparaîtront plus que sous leur forme abrégée. Ces sigles s'expliquent par notre volonté de faciliter la lecture en évitant la surcharge, comme par le fait qu'ils recouvrent en partie l'usage que peuvent en faire les acteurs (ex: "ticker" boursier renvoyant à l'unité de compte considérée).

**BTC** : bitcoin comme unité de compte native

**PoS** : *Proof of Stake*\* pour Preuve d'enjeux

**CBDC** : *Central Bank Digital Currency* pour Monnaie Digitale de Banque Centrale

**PoW\*** : *Proof of Work*\* pour Preuve de travail\*

**CM** : CryptoMonnaie(s)

**UCN** : Unité de Compte Native

**ETH** : ether comme unité de compte native

**UTXO\*** : *Unspent transaction output*\* pour Sortie de transactions non dépensées

**EF** : Ethereum Foundation

**WP** : *White Paper* ou Livre Blanc

**P2P** : Peer-to-Peer pour Pair-à-Pair

## INTRODUCTION GÉNÉRALE

« La difficulté n'est pas de comprendre les idées nouvelles, elle est d'échapper aux idées anciennes qui ont poussé leurs ramifications dans tous les recoins de l'esprit des personnes ayant reçu la même formation que la plupart d'entre nous. »

« *The General Theory of Employment, Interest and Money* »,  
John Maynard Keynes, p. 6, préface de la 1<sup>ère</sup> édition anglaise (1936)

En 2008, sous pseudonyme et durant l'une des pires crises bancaires et financières du XXI<sup>e</sup> siècle, une contestation monétaire radicale fut lancée : Bitcoin. Avec lui commence le phénomène des *cryptomonnaies*\* (CM), dont les *codes sources ouverts*\* ont permis la création d'une diversité d'objets monétaires non identifiés, présentés sous ce néologisme. Aujourd'hui, près de 13 131 CM s'échangent sur 532 bourses d'échange, pour une capitalisation de près d'un trillion de dollars (culminant à plus 3 trillions, en fin 2021)<sup>1</sup>. Certaines expériences, comme Ethereum, offrent des services financiers complexes (dépôts et crédits, véhicules d'investissement, produits dérivés de toutes sortes, etc.). Leurs ambitions ? Ouvrir « *un nouvel espace de liberté pour plusieurs années* »(Nakamoto 2008a), « *démocratiser la monnaie* » et lui rendre sa dimension de « *commun* » (Wirdum 2014 ; Singer 2021).

Selon son créateur Satoshi Nakamoto (2008), Bitcoin répond à la crise financière et à sa gestion. Ses rares écrits<sup>2</sup>, ses choix architecturaux ou l'inscription indélébile dans ses données de genèse d'une « Une » du *Time* sur un plan de sauvetage bancaire<sup>3</sup> sont autant de critiques des systèmes monétaires. La critique qui accompagne la création de Bitcoin s'inscrit dans un mouvement ancien de contestation des banques et des gouvernements, et dans une histoire de la monnaie riche en innovation. Cette critique ne vise pas à infléchir les règles d'un système dont Nakamoto n'attend rien. Perçu comme relevant d'une collusion entre les autorités politiques et bancaires, ce système honni sera défié par le flanc : par l'offre d'un système monétaire *à côté* des systèmes de paiement et de règlement nationaux. Les monnaies parallèles, notamment les monnaies locales et complémentaires (MLC) avaient déjà produit une critique en actes mais à moindre échelle (Blanc 1998a; Blanc 1998b; Blanc 2009a). La critique de Nakamoto diffère tant par le fond idéologique que par la forme pratique. Les monnaies locales et complémentaires visent à instituer des systèmes monétaires faisant la part belle à l'humain et aux relations sociales, réinstillant proximité, confiance, valeurs partagées et délibérations dans les affaires monétaires. Les *e*-monnayeurs rejettent tout cela, du moins en apparence (Dodd 2017, p. 8). Les MLC contestent l'enfermement technocratique de la gouvernance monétaire nationale, à laquelle les membres revendiquent d'être associés. À l'opposé, les *coiners*\* en défendent la suppression pure et simple : il s'agit de lui substituer une gouvernance par la technique.

Nakamoto suit un raisonnement opposé à celui des promoteurs des MLC : critiquer la gouvernance de l'argent n'implique pas de remettre l'humain en son centre. Sa monnaie sera « *sans*

<sup>1</sup> Source : <https://www.coingecko.com/fr/global-charts> [consultation au 27/07/2022].

<sup>2</sup> L'ensemble de ses écrits est regroupé sur le site <https://satoshi.nakamotoinstitute.org/> [consultation au 27/07/2022] ou dans l'ouvrage, *The Book of Satoshi* (Champagne 2014).

<sup>3</sup> Le titre de la « Une » du *Time* du 3 janvier 2009, « Le chancelier de l'Échiquier sur le point d'un second plan de sauvetage des banques », a été ajouté par S. Nakamoto dans les données non transactionnelles de l'*enregistrement de genèse*\* (ou *genesis block*\*) lors du lancement de Bitcoin (cf. Chap. I.).

*confiance* »<sup>4</sup>. Le « *problème fondamental de la monnaie traditionnelle* » est la confiance imposée et nécessaire à son fonctionnement (Nakamoto 2009a). Les autorités et les acteurs bancaires et financiers s’érigent ainsi en « *tiers de confiance* » et « *médiateur[s] de conflit* », ce qui leur confère autorité et pouvoir dans la gouvernance d’ensemble. Cette position engendre des coûts (Nakamoto 2008c), ou pire, des abus : « *Il faut faire confiance à la banque centrale pour ne pas avilir la monnaie, mais l’histoire des monnaies fiduciaires est pleine de violations de cette confiance. Il faut faire confiance aux banques pour détenir notre argent et le transférer par voie électronique, mais elles le prêtent par vagues de bulles de crédit avec à peine une fraction en réserve. Nous devons leur confier notre vie privée, leur faire confiance pour ne pas laisser les voleurs d’identité vider nos comptes.* » (Nakamoto 2009a)<sup>5</sup>. Le changement doit passer pour Nakamoto par la création d’un système monétaire *ex nihilo*, fondé sur des bases radicalement opposées, sans coercition, en un lieu où les États ont peu de prises : le « *cyberespace* ». Les règles monétaires de Bitcoin sont définies et rendues exécutoires au sein d’un réseau\* d’acteurs suivant un *protocole informatique\** que l’on rejoint sous pseudonyme et par choix. Aucun agrément préalable n’est nécessaire. Aux priviléges verticaux du système hiérarchique répondent l’horizontalité et l’universalité d’un protocole de communication et d’un réseau\* pair-à-pair (P2P) ouvert et accessible à tous. Ce protocole est censé permettre à des machines indifférenciées – les « *nœuds\** » – via un système de règles et procédures standardisées, de s’entendre sur la validité d’un ensemble de *données endogènes\** : la possession et la cession d’unités de compte natives (UCN\*), les bitcoins de Bitcoin<sup>6</sup>. Pas de crédit en contrepartie de la création monétaire, mais la participation au traitement et à la sécurisation des transactions du système de paiement : les nouvelles UCN\* sont distribuées aux *nœuds\** pour inciter leur participation « *honnête* » (*Ibid.*). Pas de bases de données fermées et opaques pour centraliser les comptes, ni de priviléges et de « portes dérobées » accessibles à un collège restreint d’acteurs. Gages de souveraineté individuelle, la transparence et l’auditabilité doivent être totales grâce à une architecture holoptique donnant à tous la faculté de voir l’ensemble de ce qui s’y déroule. Aux guichets et boîtes noires des logiciels propriétaires bancaires est substituée une variété de logiciels à *codes sources ouverts\**, garantissant aux usagers l’auditabilité de leurs propriétés. Pour Nakamoto, l’unicité du *registre\** des comptes ne passe pas par une gestion centralisée. Le coup de génie de son *algorithme de consensus\** est de permettre à une multitude de *nœuds\** indifférenciés concurrents de travailler chacun dans leur coin à produire des copies redondantes du grand livre comptable, tout en convergeant collectivement sur un *registre\** transactionnel canonique (appelé *chaîne de blocs\**). Bitcoin répond à l’opacité des canaux bancaires et financiers par une parfaite accessibilité à l’ensemble des adresses et transactions, passées et en attente. La « *décentralisation* » du réseau\* entre une multitude d’acteurs garantirait, en limitant les points uniques de contrôle, les propriétés annoncées et la résilience d’ensemble : face au grand nombre, personne ne pourrait censurer des transactions\*, ni falsifier les données endogènes\* répliquées dans les registres\* ou modifier les codes logiciels protocolaires de l’ensemble des *nœuds\**.

En résumé, des protocoles informatiques produiraient à eux seuls des systèmes monétaires et de paiement résolvant les problèmes des monnaies nationales et ceux des monnaies électroniques,

<sup>4</sup> Nakamoto l’affirme en conclusion. Il propose un système de paiement qui ne « *repouse pas sur la confiance* » (« *without relying on trust.* ») (Nakamoto 2008c). Le mot confiance (« *trust* ») lui-même est mobilisé 14 fois dans le papier de 8 pages.

<sup>5</sup> Pour la version originale, voir <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source> [consultation au 27/07/2022].

<sup>6</sup> Sous l’appellation générique Bitcoin, on distingue conventionnellement le protocole et ses processus d’une part, et la devise en tant qu’unité de compte d’autre part, dénommés respectivement Bitcoin (grand B) et bitcoin (petit b) ou BTC. Nous étendons la dénomination Bitcoin aux acteurs, processus, dispositifs, institutions et conventions excédant le protocole.

duplicables car numériques<sup>7</sup>. Il n'y aurait plus de violation de confiance par des actes arbitraires, mais des règles et procédures automatiques, édictées par un protocole que tous les participants doivent suivre. La monnaie s'affranchirait de tout cadre juridictionnel, ne relevant d'aucun centre ni d'aucune intermédiation, sauf celle (technique) du protocole. Les codes protocolaires la soustrairaient aux relations sociales, aux débats et conflits, et la politique monétaire ne serait plus soumise à délibération. Cette « décentralisation » produirait des systèmes monétaires « *neutres* » et « *apolitique* », avec des monnaies « *saines* » d'une crédibilité inégalée (*Antonopoulos Bitcoin Q&A* 2018) : leur monnayage (quantité d'UCN\*, modalités d'émission et de circulation) « *immutable* », « *objectif* », « *transparent* » et « *automatique* » garantirait une cohérence temporelle à toute épreuve. Ces monnaies reposeraient *sur* (et enjoindraient *à*) une souveraineté individuelle nouvelle. Elles offririaient un choix inédit : celui de « *placer [son] argent et [sa] foi dans un cadre mathématique exempt de politique et d'erreur humaine* » (T. Winklevoss, cité par Mullin (2013), où « *un algorithme remplace la fonction du gouvernement* » (Al Gore, cité par OConnell (2016)).

La découverte de ces ambitions monétaires, perçues par certains comme un « *rêve* » et par d'autres comme un « *cauchemar* » monétaire « *libertarien* » (De Filippi 2013; Karlstrøm 2014), nous fit sourire à l'époque autant qu'elle nous questionna. Comme beaucoup, nous avons accueilli avec dédain ces CM qui entraient dans l'histoire avec Bitcoin. Comment pouvait-on parler de monnaie alors que ces diverses affirmations paraissaient si opposées à ce que recouvre théoriquement et pratiquement classiquement ce concept ? Les prétentions de cette idéologie visant à faire de la monnaie une pure mécanique protégée des relations sociales et des intermédiaires devaient être interrogées. Cette thèse est consacrée à l'étude de la gouvernance réelle des CM à distance de l'imaginaire des *coiners*\* comme de leurs détracteurs. Nous cherchons à décrypter les formes singulières de cette gouvernance qui est loin d'être entièrement confiée aux codes, tout en dérogeant au cadre hiérarchique des monnaies nationales. Cet écart, comme nous le défendrons, ne doit cependant pas conduire à dénier à ces objets le statut de monnaie, mais ouvre au contraire un champ nouveau de réflexion sur la monnaie.

Dans la suite de cette introduction, nous aborderons la construction de notre objet de recherche - la gouvernance des CM - et nos questionnements (A). Nous expliciterons ensuite notre cadre théorique, qui combine une approche monétaire institutionnaliste et une démarche ethnographique empruntant à la Sociologie des Sciences et Technique (STS) (B). Puis nous présenterons la méthodologie de notre enquête multi-niveau, les dispositifs et stratégies utilisés pour accéder au terrain, ainsi que les matériaux récoltés (C). L'économie générale de la thèse sera abordée en quatrième partie (D). Nous conclurons cette introduction par une déclaration d'intérêts (E).

## A. LA GOUVERNANCE DES CM : CONSTRUCTION DE NOTRE OBJET DE RECHERCHE

L'objet de notre recherche et sa problématique se sont construits lentement. Nous explicitons d'abord le contexte et les motivations de notre recherche, avant de nous intéresser à notre positionnement épistémologique, théorique et méthodologique (Avenier et Thomas 2011).

---

<sup>7</sup> Il s'agit du *problème de double dépense*\* (Nakamoto 2008).

## 1) Un intérêt pour la monnaie et les « Objets Monétaires Non Identifiés »

Notre intérêt pour les CM découle d'un intérêt ancien pour la question monétaire. Commencé en octobre 2018 sous la direction d'E. Chiapello, ce travail a été précédé d'une entame de doctorat, sous la direction de J. Sapir, inspiré par la crise bancaire et financière qui avait accompagné la fin de notre cursus de Master 2 (fin 2009). Ayant interrompu ces premiers travaux de recherche formels pour des raisons économiques, nous nous sommes néanmoins intéressé à l'objet CM durant la phase d'activité professionnelle<sup>8</sup> et de recherche informelle qui suivit. Notre contact avec ce champ date de 2015 et s'inscrit dans la continuité de nos réflexions passées sur la gouvernance du système monétaire. Nous avions entendu parler de Bitcoin dès 2011, mais c'est plus tardivement que notre intérêt fut éveillé par la survie du phénomène, par le développement de son écosystème et par l'accroissement progressif de sa couverture médiatique et académique. Une lecture approfondie du *Working Paper* (WP) de Bitcoin et nos premières « *immersions participantes* »<sup>9</sup> nous ont révélé le caractère novateur des CM. Ces dernières offraient la chance inouïe d'étudier un phénomène rare dans le champ de la monnaie : l'émergence *ex nihilo* d'*« une nouvelle forme d'argent »* (Kavanagh et Miscione 2017, p. 10) qui, malgré des fondations non étatiques, connaissait des développements inégalés.

La multiplication des travaux académiques de ces dernières années contraste avec leur absence relative au début du phénomène. Des différences existent selon le champ disciplinaire. Les recherches les plus précoces et les plus nombreuses viennent de la science informatique. Bitcoin y a été largement « étudié dans la communauté des systèmes distribués » (Bano ; et al. 2017, p. 1). Le « *consensus de Nakamoto* » fondé sur *la preuve de travail\** (PoW\*), premier algorithme de consensus\* permettant des systèmes de protocole de registre\* ouvert, y est le « *composant le plus débattu* » (Bonneau et al. 2015, p. 104). Bien que ce corpus des travaux soit important pour comprendre les mécanismes et enjeux « techniques » de ce champ, il n'est pas central dans notre travail. Le phénomène des CM a connu une couverture croissante dans le champ médiatique avant de susciter des travaux académiques en économie et sciences sociales. Un portrait sombre était brossé, insistant sur les usages illégaux, les arnaques, les attaques informatiques et le caractère erratique des cours boursiers. Les phases d'euphorie spéculative et de panique polarisaient l'attention. À l'intérêt des médias s'est ajouté celui des régulateurs et des gouvernements<sup>10</sup>. Les projets d'entreprises privées d'envergure, comme Facebook et son projet désormais mort-né Libra/Diem, ont accru les inquiétudes et accéléré les travaux sur les *Central Bank Digital Currency* (CBDC). Les autorités monétaires, bancaires et financières, ainsi que les administrations fiscales, s'y sont intéressées relativement tôt produisant une littérature grise prenant la forme de rapports et notes d'information (European Central Bank 2012, 2015 ; Banque de France 2013) mais peinant cependant à établir des qualifications homogènes et stabilisées.

---

<sup>8</sup> Nous avons dû travailler, d'abord comme chargé de TD à l'Université Paris 1 (2010-2012), puis comme enseignant de SES, dans un lycée associatif pour enfants en difficulté (de 2012 à 2018). De 2016 à 2019, encore en relation avec le laboratoire CEMI, nous avons dispensé à l'EHESS un séminaire intitulé « *Espace(s) monétaire(s), monnaies parallèles, crypto-monnaies et crises institutionnelles* » (24 heures). À partir de 2017, nous avons aussi enseigné sur la monnaie et les CM à l'ESGI, à l'ESILV et l'ESC Clermont Ferrand.

<sup>9</sup> L'« immersion participante » est un dispositif propre d'accès au terrain mobilisé lors de réalisation d'ethnographies du virtuel. Il recouvre la participation active du chercheur au côté de ses enquêtés dans les mondes numériques. (Amato 2008; Berry 2012, cf. section C suivante).

<sup>10</sup> Voir les déclarations de la directrice du FMI, Mme Lagarde (Lagarde 2017, 2018) ou encore celles de Mark Carney, de la *Bank of England* (Carney 2019), ou la tribune du ministre de l'Économie français B. Le Maire (Le Maire 2019) par exemple.

Dans le champ émergeant des CM, régnait l’indistinction du fait de classifications « *inconsistantes* » et « *anarchiques* » (Vergne et Swain, 2017) et d’un manque relatif de littérature académique (Bonneau et al. 2015 ; Bano; et al. 2017 ; Walch 2017 ; Rauchs et al. 2018). Les médias (Vergne et Swain 2017), la littérature indigène et grise (Walch 2017a) utilisaient indistinctement les termes de CM, de « *Blockchain\** », de « *crypto-actifs\** », de « *monnaies digitales\** », de « *cybermonnaie* »<sup>11</sup>. On vantait une technologie miracle offrant non seulement des monnaies « saines », mais aussi une meilleure gestion des chaînes d’approvisionnement, de l’identité et des cadastres, des votes démocratiques, etc. (Iansiti et Lakhani 2017 ; Lehr et Lamb 2018). Bien qu’étant encore novice, cette diversité nous apparaissait problématique. L’appellation générique de *protocoles à registre\* distribué* masquait ainsi des systèmes diamétralement opposés (Rauchs et al. 2018). Certains objets présentés comme CM relevaient simplement de monnaies digitales\* ou de crypto-actifs\*, sans révolutionner la monnaie comme Bitcoin. Reposant sur la crédibilité et la solvabilité d’émetteurs centraux, ils n’étaient que d’anciennes recettes sous des atours techniques nouveaux. L’absence de langage *etic*, comme cadre conceptuel rigoureux et unifié, était problématique pour les chercheurs, les régulateurs, mais aussi pour les citoyens, face à un langage *indigène* évoluant au gré des stratégies économiques et discursives des acteurs. Ce contexte et les interrogations sur les ambitions libérales technicistes des CM nous ont convaincu de contribuer à ce champ encore en friche, voire délaissé<sup>12</sup>.

Il était prévisible que les médias se concentrent sur la surface spectaculaire de ces objets. Il était compréhensible que les praticiens refusent de les considérer comme monnaie, car ils ne correspondaient pas aux définitions et catégories réglementaires existantes. Cependant, les chercheurs ne sont pas nécessairement limités par ces définitions. Nous avons donc été surpris par les réactions que les CM suscitaient dans le monde académique.

## 2) La controverse sur le caractère monétaire des cryptomonnaies

Non seulement il y avait peu de recherches (en sciences sociales et en économie), mais les textes existants montraient un dédain pour un objet vu comme tout (lubie de techno-libertarien, tulipe 2.0, arnaque, pyramide de Ponzi, etc.) sauf monnaie. La majorité des économistes et des praticiens vouait Bitcoin aux gémonies sans vraiment s’y être intéressé (d’où l’absence de travaux académiques pour les premiers), le décriait dans les journaux, sur les réseaux\* sociaux ou dans des blogs. Prix « Nobel » d’économie en tête (Tirole 2017; Krugman 2018; Shiller 2018), ils affirmaient que ces objets n’avaient de monétaire que leurs prétentions. Ils jugeaient les CM sans valeur intrinsèque, imparfaites技iquement et économiquement, et utiles uniquement pour des activités illégales ou spéculatives. Ils y voyaient seulement « *Bulle, fraude et trouble* » (Krugman 2018) avec un destin prévisible. Si les CM ne s’effondraient pas d’elles-mêmes, il fallait les interdire pour protéger le « *système monétaire et financier* », la société et la planète de tous les dangers qu’elles représentent (Stiglitz 2017; Servet et Dufrêne 2021). Ces objets étaient condamnés par les professionnels de l’argent qui en prophétisaient souvent la mort<sup>13</sup>.

---

<sup>11</sup> En 2017, le terme de « cybermonnaie » est adopté par la commission d’enrichissement de la langue française (voir liste publiée au Bulletin Officiel le 23/05/2017, <https://www.enseignementsup-recherche.gouv.fr/fr/bo/17/Hebdo28/CTNR1713838K.htm> ; [consultation au 27/07/2020]).

<sup>12</sup> Cette recherche au long cours a été l’occasion d’échanger sur les CM avec des étudiants intéressés et de constater que certains avaient été empêchés de travailler sur le sujet : un mémoire de Master 2 sur Bitcoin n’était pas un sujet « intéressant ».

<sup>13</sup> Sa mort a été annoncée tant de fois que le site Bitcoin Obituaires, créé non sans ironie par des *bitcoiners*, en fait la recension. <https://99bitcoins.com/bitcoin-obituaries/> [consultation au 02/07/2022].

Ces discours étaient cependant contredits par des faits têtus. En une décennie, Bitcoin a maintenu un taux de *disponibilité*\* de plus de 99,987%<sup>14</sup>, avec une valeur d'encours transférée, un nombre de transactions\* et d'utilisateurs en croissance constante (cf. Annexes n°1, 2 et 3). Notre dédain premier pour ces objets, partagés avec ces auteurs, s'est mué en intérêt aigu. Il fallait mettre à l'épreuve le caractère paradoxal de leurs prétentions libérales technicistes, non pas en expliquant pourquoi théoriquement ces expériences devaient échouer, mais en révélant empiriquement les conditions de leur survie et de leur développement.

Loin des prises de position médiatiques virulentes, quelques travaux académiques plus nuancés existaient cependant : des travaux ont ainsi étudié les propriétés de Bitcoin et les déterminants de son prix de marché (et d'éventuelles manipulations de cours, Halaburda et Gandal 2014 ; Gandal et al. 2018) ; les risques et les enjeux macroéconomiques des CM (Brito et Castillo 2013 ; Aglietta, Ponsot et Ould-Ahmed 2014 ; Böhme et al. 2015 ; Raskin et Yermack 2016), ainsi que les implications sur les taux de change et l'évitement des contrôles de capitaux (Pieters 2016). Plusieurs travaux ont aussi porté exclusivement la chaîne de blocs\* et ses applications, y compris par les banques centrales (Danezis et Meiklejohn 2015 ; Raskin et Yermack 2016 ; Koning 2016 ; Pfister 2017). Dans le champ juridique, un vaste pan de la littérature s'est concentré sur les problèmes de l'encadrement légal du Bitcoin et des autres CM, plateformes et pratiques qu'il a inaugurées (Walch 2017). Le statut monétaire des CM, revendiqué en concurrence des monnaies traditionnelles, reste discuté, voire contesté, mais est aussi reconnu marginalement par certains travaux (Yermack, 2013 ; Maurer et al, 2013 ; Ali et al, 2013 ; Jeong 2013 ; Böhme et al, 2015 ; Raskin et Yermack, 2016 ; Dodd, 2017). Les propriétés singulières et usages restreints des CM démontrent en effet que les CM remplissent maladroitement les trois fonctions monétaires canoniques (unité de compte, moyen de paiement et réserve de valeur, voir Yermack, 2013 ; Ali et al, 2013). Pour d'autres cependant, Bitcoin et les CM ne sont « *pas [des] monnaie[s], mais [de] simples instruments monétaires désincarnés* » et il ne faut pas les considérer comme telles (Dupré, Ponsot et Servet 2015, p. 11). Bien que reconnues comme moyens de paiement, elles sont encore reléguées, selon les autorités monétaires et fiscales, au statut d'actifs financiers. Ce n'est pas totalement erroné – une monnaie prise comme devise perd sa qualité monétaire en devenant un actif de *portefeuille*\* –, mais cela semble réducteur et les confine à un statut secondaire. De fait, les CM comme « *Bitcoin [sont] difficile[s] à intégrer dans une conception politique de la monnaie [qui s'avère] peut-être [...] incomplète* » (Jeong, 2013, p. 27).

Les critiques de Bitcoin sont, comme toute critique, situées. Les critiques des chercheurs du corpus orthodoxe ne sont pas surprenantes. Dans ce corpus, la monnaie et les innovations monétaires et financières ont peu de place. En revanche, il était plus surprenant de voir ces objets relégués hors du champ de la monnaie par des auteurs de l'institutionnalisme monétaire francophone (IMF) (Dupré, Ponsot et Servet, 2015). Lors des colloques, nous avons parfois reçu des remontrances

---

<sup>14</sup> En informatique, le *taux de disponibilité* (ou « *uptime* ») est un indicateur de performance lié à la disponibilité d'un système, qui mesure la durée de bon fonctionnement, exprimée en pourcentage du temps durant lequel il fonctionnait ou était prêt à être utilisé. Bitcoin, depuis 2009, n'aurait connu que 14 heures, 47 minutes et 9 secondes de non-disponibilité\*, voir <https://www.buybitcoinworldwide.com/bitcoin-upptime/> [consultation au 04/07/2022].

acerbes : considérer ces objets comme des monnaies était une erreur rédhibitoire<sup>15</sup>, à la limite de l'excommunication. Paradoxalement, les auteurs dont l'appareillage conceptuel nous était essentiel se révélaient parmi les plus critiques. Nous reconnaissions comme d'autres manquer « *d'informations concernant tant ses utilisations que la gestion collective des capacités d'accès et de reproduction de cette liquidité* » (Dupré, Ponsot et Servet 2015, p. 4), mais cela nous incitait plutôt à entreprendre des recherches exploratoires qu'à formuler des conclusions définitives. Quelques rares travaux se sont néanmoins appuyés sur ce corpus institutionnaliste pour questionner les prétentions de Bitcoin à être une monnaie (Desmedt et Lakomski-Laguerre 2015; ou notre article co-écrit avec A Slim, Rolland et Slim 2017) : les CM y sont abordées comme des monnaies conçues comme systèmes de paiement (Cartelier 1996) associés à des communautés de paiement organisées (Knapp 1924; Orléan 2019), que nous souscrivions ou non aux représentations et croyances presque religieuses<sup>16</sup> de ces communautés. Cette approche implique que les CM ne peuvent pas être dépourvues d'une structure de gouvernance, même sommaire. C'est ce que cette thèse entend contribuer à révéler.

### **3) Révéler l'« indicible » gouvernance des CM contre les prétentions libérales technicistes**

Notre volonté d'interroger les prétentions monétaires des CM trouvait aussi sa source dans la capacité de ces objets à renouveler le débat portant sur la « bonne » monnaie et sa gouvernance. Cette controverse ancienne, structurée autour de la formule « *la règle contre la discréption* », interroge le rôle du politique dans les affaires monétaires. La question centrale est celle de la neutralité de la monnaie, perçue comme intrinsèquement bénéfique pour l'économie (Théret 2008, p. 12). Les partisans de la neutralité de la monnaie (ou de sa neutralisation) privilégient la stabilité de l'unité de compte et prônent des règles strictes pour limiter les interférences politiques sur la quantité de monnaie en circulation : la « bonne gestion » de la monnaie par les banques centrales implique que la discréption soit contrainte (de Boyer des Roches et Rosales 2003; Kindleberger 2004; Tutin 2009). Les partisans de la discréption estiment au contraire que la qualité d'une monnaie dépend de la capacité des autorités monétaires à réaliser des actions discrétionnaires pour éviter un effondrement systémique : monnaie et politique monétaire sont affaire d'arbitrages relatifs, et la stabilité de l'unité de compte ne doit pas compromettre la viabilité du système de paiement (Kindleberger 2004; De Boyer des Roches et Rosales, 2003). Ces lignes de fracture sont récurrentes

<sup>15</sup> Nous pensons au colloque international « *Institutionnalismes Monétaires Francophones* », tenu du 1<sup>er</sup> au 3 juin 2016 à Lyon, où avec Assen Slim, nous avons présenté : « *Le Bitcoin, institutionnalisation d'une monnaie sans institutions* » ; de même, lors de la 54<sup>ème</sup> rencontre du Séminaire Franco-Russe, des 12-13-14 février 2018, à Moscou où nous présentions « *Crypto-monnaies et monnaies digitales : entre contestation monétaire et récupération technologique* ». Avant même notre intervention, au détour d'une discussion ouverte sans lien à notre sujet, un participant affirma que Bitcoin n'est pas monnaie. Le même participant a pris la parole près de 15 minutes au début de notre présentation de 45 minutes, exposant ses arguments sans attendre les nôtres. Après avoir péniblement récupéré la parole, nous avons répondu point par point avec un brin d'ironie. Notre interlocuteur reconnut un manque d'information et montra finalement de l'intérêt pour les éléments présentés. L'année suivante, il n'y eut aucune interruption et nous reçumes des félicitations du même intervenant. Ce qui nous a le plus surpris dans toutes ces expériences, ce ne sont pas tant les critiques, légitimes et attendues, que le ton condescendant envers un simple docteur bousculant leurs représentations *a priori*.

<sup>16</sup> Cette dimension « religieuse », ce « supplément de foi supra-théorique » (Simmel 2009), au cœur de toute monnaie, prend des formes singulières au sein de la communauté Bitcoin (de Vauplane 2018; Laycock 2022, Observation participante), avec des « croyances », des récits (« sa conception Immaculée »), un prophète (Satoshi Nakamoto), des évangélistes (comme R. Ver, investisseur et promoteur dénommé « Bitcoin Jesus » avant d'être excommunié), des rituels et cérémonies (« pizza day », maintenir des noeuds\*, les jours de « having », Sedgwick 2020b), des objets sacrés (le WP\*), des « sectes », factions et gnose (voir F. Ersham <https://twitter.com/FEhrsam/status/933520783581646848?s=20&t=GAMk0hZEyPvYWsNPMw> [consultation au 29/07/2022]).

dans l'histoire de la pensée monétaire : présentes dans les débats préclassiques, elles réapparaissent dans les controverses entre l'école de la monnaie (*Currency School*) et l'école de la banque (*Banking school*), entre monétaristes et keynésiens (*Ibid.*; Tutin 2009). Les politiques de libéralisation financière et l'émergence du Nouveau Consensus Monétaire, succédané de monétarisme, ont marqué la victoire de la règle et d'une vision quantitativiste (Galbraith, 2008). Accompagnée de prescriptions en termes d'indépendance, de transparence et de crédibilité pour les politiques monétaires et les autorités responsables (Friedman 2008 ; King 1999 ; Feiertag et Margairaz (dir) 2012), cette victoire théorique et pratique, bien que totale dans les esprits<sup>17</sup>, ne l'est pas totalement les faits. En effet, les décennies passées ont nécessité un recours intensif à des politiques monétaires que ce corpus théorique condamnait, d'ailleurs qualifiées pour cela même de « non conventionnelles ».

Pour les *coiners\**, les CM réussissent là où les expériences passées ont échoué. Bitcoin se pose « *ironiquement* » et « *paradoxalement* » comme « *absolument apolitique* » et « *neutre* » (Keir 2022). Le paradoxe réside « *dans l'existence même du bitcoin* » : « *si le protocole lui-même est apolitique, cet acte de création est profondément politique.* » (*Ibid.*). L'ironie renvoie au fait qu'« *un monde [...] profondément polarisé et politisé [a pu conduire à la création d']un système immuable et apolitique [...] indifférent à toute croyance ou idéologie [...] résolument neutre [...] vis-à-vis de la race, de la religion, de l'ethnie, du sexe, de la taille, de la couleur des cheveux, de la couleur de la peau, de la couleur des yeux, du type de corps, de la forme du corps, du nom, de la langue, de la localisation, de la richesse ou de toute autre myriade de facteurs d'identification et de distinction.* » (*Ibid.*; rejoint par Antonopoulos 2013). Un carcan logiciel immutable garantirait cette neutralité, dotant les CM de monnayage empreint, à des degrés divers, d'un « *métallisme numérique* » (Maurer et al, 2014, p. 2) et rendant la régulation monétaire indépendante des régulations politiques. Encadrant la quantité totale d'unités monétaires émises (limitée à 21 millions d'unités pour Bitcoin) ainsi que les modalités de leur émission, distribution et circulation, les codes protocolaires préserveraient, selon ces analyses, la valeur de la monnaie de l'inflation induite par la discréption politique. Sous cet angle, ces expériences tentent de dépasser les ambitions monétaires les plus rigoristes, comme celles du *Free Banking*, soulignées par de nombreux auteurs (De Filippi 2013 ; Dréan 2013 ; Karlstrøm 2014 ; Desmedt et Lakomski-Laguerre 2015). Le *Free Banking* vise à abolir le monopole des États et des banques centrales dans l'émission et la circulation de la monnaie, ambition centrale de l'école autrichienne (Von Mises 1912 ; Hayek 1976) dont se revendiquent certains *coiners*\*.

Ce positionnement radical des CM explique en partie leur réception par les économistes. Cependant, ce « *métallisme numérique* » cache mal leur dimension nominaliste : le pouvoir d'achat des UCN\*, sans adossement à un actif ou passif de tiers, est fondé d'abord sur une promesse d'acceptation future (Maurer, Nelms et Swartz 2013, p. 14). Cette promesse auto-référentielle est étayée par un ensemble d'institutions, d'acteurs, de relations et de représentations sociales. Ainsi, les CM, comme toute monnaie, sont fondées en confiance et en autorité légitime, éléments essentiels de définition de la monnaie pour Simmel (2009) ou Simiand (cité par Orléan, 2008).

La littérature portant spécifiquement sur les CM et les questions de gouvernance est faible et ambivalente. Ces travaux soulignent l'existence d'une dimension sociale articulant la « *matérialité pratique* » de Bitcoin aux dimensions axiologiques et sémiotiques de la communauté (Maurer,

---

<sup>17</sup> Victoire soulignée par l'« *ensemble de normes théoriques communes, d'analyses partagées et de choix politiques semblables : consensus sur la stabilité, la libéralisation financière et l'indépendance des [banques centrales]* » parmi des praticiens et des banquiers centraux qui s'érigent en communauté épistémique transnationale (Feiertag et Margairaz 2012, p. 243).

Nelms et Swartz 2013; Desmedt et Lakomski-Laguerre 2015), mais se concentrent surtout sur le protocole « technique ». Ils insistent sur l’architecture technologique et les relations au sein de la chaîne\* (qu’ils finissent par réifier) comme modalité unique de gouvernance. Selon nous, ces analyses font accroire que l’ensemble des institutions et des relations de sociabilité au cœur de l’argent se fondent dans la technique. Il faudrait accepter que « *Bitcoin fournit une réflexion utile sur la socialité de l’argent, bien qu’il intègre cette socialité de confiance dans son code lui-même* » (Maurer, Nelms et Swartz 2013, p. 3). La confiance se cristallise dans le code, voire seulement dans l’« *algorithme cryptographique* » (*Ibid.*, p. 4 ; rejoint par Ponsot 2021)<sup>18</sup>. Les *bitcoiners*\* auraient une « déférence aux codes » absolue, contenue dans le slogan « *Code is Law* », réductible à une confiance individuelle garantie par la nature technique de leur « *autorité algorithmique* » (Lustig & Nardi 2015). Les relations sociales, la maintenance logicielle, les débats politiques internes, ayant lieu hors chaîne\* et sans lesquels les CM ne seraient rien, sont laissés dans un angle mort, voir niés explicitement (Dupré, Ponsot et Servet 2015). Ces textes invitent à leur dépassement, soulignant que « *la fiabilité de l’argent est basée sur une confiance partagée entre les individus et soutenue par de multiples institutions et infrastructures techniques* » (Mallard, Méadel et Musiani 2014, p. 3). Desmedt et Lakomski-Laguerre (2015, p. 15) s’interrogent pour leur part : « *Derrière le code, n’y a-t-il pas un concepteur [...], une communauté ? Outre le réseau\* en P2P constitué par les noeuds\*, comment s’organise cette communauté ? Par quels canaux concrets œuvre-t-elle pour la légitimation de sa monnaie ? Il conviendrait alors d’examiner plus avant une telle organisation, pour comprendre son fonctionnement et spécifier les rôles, statuts et positionnements des différents acteurs qui la composent : mineurs, promoteurs, responsables de sites officiels, utilisateurs, etc. Cette démarche plus empirique devrait faire l’objet d’un travail ultérieur* ». C’est ce à quoi nous nous sommes attaché dans cette recherche.

L’infrastructure technique et ses composantes sont fondamentales pour cerner les CM, ce qui a attiré l’attention de nombreux chercheurs. Mais s’y limiter est insatisfaisant et il faut donc penser que les CM relèvent d’une gouvernance duale<sup>19</sup> (De Filippi et Loveluck, 2016 ; Rolland et Slim, 2017). D’abord, il y a la gouvernance *par* l’infrastructure qui encadre les interactions et résout les conflits sur l’historique des transactions\* via l’*algorithme de consensus*\*, comme avec le « consensus de Nakamoto » pour Bitcoin (cf. Chap. I). Cependant, cette gouvernance mène à une autre, plus sociale et politique, la gouvernance *sur* l’infrastructure. Faire monnaie implique des problèmes et des solutions hybrides, concernant l’entretien ou la modification des codes protocolaires, les conditions d’accès et de circulation des UCN\*, les usages légitimes, etc. Les problèmes et solutions que doit résoudre la gouvernance *sur* l’infrastructure se situent au-delà de la technique, dans des espaces de débat et de décision socialement construits, exogènes au protocole. Des débats et conflits opposent des acteurs aux positions, intérêts et représentations variés. Les discussions techniques dissimulent des considérations politiques et normatives sur ce que doit être la « bonne » monnaie. La désintermédiation est illusoire (De Filippi & Loveluck, 2016 ; Dodd, 2017 ; Rolland & Slim, 2017 ; Hsieh, Vergne et Wang 2018). Nous montrerons encore que des secteurs et groupes d’acteurs sont cruciaux « aux têtes » d’une gouvernance *sur* l’infrastructure, qui n’est ni centralisée, ni « acéphale » (Favier et Takkal Bataille 2017), mais polycentrique. Des acteurs créent, entretiennent, corrigent et modifient continuellement les codes logiciels essentiels aux CM. D’autres servent d’intermédiaires financiers (services de *passerelles*\* comme les bourses d’échange, les

---

<sup>18</sup> Et dans une moindre mesure, chez Lakomski-Laguerre et Desmedt (2015, p. 12), « *une forme de confiance (celle qui a été façonnée par l’État et les banques)* » est remplacée par « *une autre (celle ancrée dans la technologie)* ».

<sup>19</sup> Ces auteurs adaptent la distinction conceptuelle proposée par DeNardis et Musiani (2014) concernant la gouvernance d’Internet, qui leur a permis de démontrer le développement d’un « *recours à l’infrastructure* » (« *turn of infrastructure* ») visant à faire de la « *gouvernance par l’infrastructure* » une extension des moyens et conflits de la (géo)politique des États (notamment des États-Unis, avec l’exemple de l’iCANN, institution essentielle d’Internet, que la CM Namecoin vise à décentraliser, cf. Chap. I).

portefeuilles\* gérés par des tiers, etc.), permettant aux UCN\* d'avoir une sphère d'usage et une valeur d'échange. D'autres encore produisent et diffusent des informations et de la connaissance. Ils offrent des outils de mesure, des avis, des modélisations (traitement des données *au sein de la chaîne*\*, évaluation des frais de transaction\*, modèle d'évaluation des prix, etc.), des récits (« narrative ») participant à forger des croyances, des représentations et un sens partagé. Ces investissements de forme (Thévenot 1986), *hors chaîne*\*, sont essentiels pour les utilisateurs et les acteurs souhaitant développer des services autour de ces technologies. L'intériorisation de connaissances, de conventions, d'habitudes, de sens même, est nécessaire pour stabiliser, rendre efficaces et coordonner leurs engagements.

La thèse s'attachera à mettre au jour la gouvernance duale et polycentrique des CM. Cette gouvernance inspirée par la décentralisation revendiquée et soutenue par une multitude de choix infrastructurels éclaire d'un jour particulier le développement et l'institutionnalisation des CM, dont il faudra rendre compte en prêtant attention tant au rôle des médiations techniques qu'à celui des conflits et des modes d'expression et de résolution de ceux-ci. Aborder à ces questions sans tomber dans le technicisme nécessite un cadre théorique et conceptuel que nous présentons maintenant.

## B. LA GOUVERNANCE DES CM DÉVOILÉE PAR LEURS CRISES : UN INSTITUTIONNALISME ARTICULÉ À UNE SOCIOLOGIE DES SCIENCES ET TECHNIQUES

Cette section et la suivante situeront notre recherche - son « design » (Avenier et Thomas 2011, p. 1) - et les matériaux empiriques utilisés<sup>20</sup>. Nous avons évoqué le contexte et les motivations de notre recherche. L'explicitation de notre inscription épistémologique et théorique retranscrira le processus qui nous a conduit à élaborer notre approche, combinant un institutionnalisme monétaire et une sociologie économique, empreinte de sociologie des sciences et techniques (STS). Cet assemblage devenu indispensable nécessite que soit explicitée et questionnée sa cohérence interne et externe<sup>21</sup>. Il faudra en faire de même pour notre intérêt pour la crise, carrefour conceptuel de ces deux corpus.

### 1) L'institutionnalisme monétaire pour caractériser les CM comme monnaies

Nous n'étions pas dénué de concepts et théories au début de ce travail. Un Master de deux années à Nanterre dans le cursus « Économie des Institutions » nous avait formé à la pluridisciplinarité et à l'institutionnalisme économique. Pour nous, l'économie doit s'appréhender selon la définition substantielle<sup>22</sup> de K. Polanyi et non en suivant la sophistique économiste

---

<sup>20</sup> Dans le « *paradigme constructiviste radical ou pragmatique* » dans lequel notre travail s'inscrit, les connaissances dépendent du processus de leur élaboration. Légitimer les connaissances élaborées et les matériaux présentés exige des explications détaillées des processus et résultats, ainsi que des décisions et inférences effectuées. Indissociable de l'élaboration des connaissances, ce travail de légitimation suppose une explicitation détaillée des matériaux empiriques et des conditions de leur constitution (Avenier et Thomas, 2011, p. 10).

<sup>21</sup> Une cohérence interne doit être établie « *entre le paradigme épistémologique* » de la recherche, « *sa finalité* » (élaborer ou tester des connaissances), « *le type de recherche mené (quantitatif, qualitatif, mixte), les techniques de recueil et de traitement mobilisés, les critères de validité mis en avant.* » (Avenier et Thomas 2011, p. 5) Cependant, cette cohérence, aussi élégante soit-elle, ne suffit pas, car une recherche doit coller aux faits. La cohérence externe « *implique que l'on juge une théorie dans sa confrontation avec le monde et pas seulement sur ses critères de cohérence interne ou de conformité aux axiomes initiaux.* » (Sapir 2019, p. 4 d'après U. Mäki)

<sup>22</sup> Polanyi définit l'économie comme l'interaction de l'homme et son environnement selon la dépendance manifeste du premier face au second quant à sa subsistance, ainsi que l'institutionnalisation socio-historique de ce processus (Chavance 2011).

formelle de Robbins, qui projette « *rétrospectivement les représentations issues de l'économie de marché sur toute l'histoire humaine* » (Chavance 2011, p. xi)<sup>23</sup>. Dans la lignée des institutionnalismes depuis l'historicisme allemand, nous rejetons la vision du marché comme une mécanique ahistorique et asociale<sup>24</sup>. Nous préférions l'induction et l'abduction aux inférences déductives et axiomes de l'économie standard : l'observation des faits réels et l'analyse de contextes relatifs étaient notre point de départ obligé, menant à des hypothèses confirmées ou infirmées par inférence déductive. Appréhender l'objet CM nécessitait des connaissances préalables sur la monnaie. Nos lectures exploratoires de la première thèse, puisant largement dans le corpus hétérodoxe (Polanyi 1944; Chavance 2011; Cartelier 1996; Orlean A. & Aglietta M. 1982; Aglietta et Orléan 1998; Aglietta et Orléan 2002; Simmel 2009), nous avait préparé. Pour les CM, ce corpus nous sembla d'emblée plus fécond que le corpus néoclassique orthodoxe.

## Notre insatisfaction vis-à-vis de la théorie monétaire dominante

Une démarche utilitariste et d'individualisme méthodologique fonde la théorie monétaire standard. Elle mobilise un agent représentatif maximisateur d'utilité, *l'homo œconomicus* à rationalité instrumentale, paramétrique et solipsiste (Cartelier 1996)<sup>25</sup>. Une théorie substantielle de la valeur utilité / rareté soutient l'édifice théorique. Toute monnaie d'hier ou d'aujourd'hui, qu'elle soit marchandise ou fiat, est conçue comme ayant une valeur intrinsèque, déterminant son utilité, donc sa demande. Chez Aristote la marchandise-monnaie est vue au travers des fonctions d'unité de compte, de moyen d'échange et de réserve de valeur, mais son « origine » est inférée d'un collectif institué, de la convention et de l'autorité. Mais l'économie marginaliste rejette cette inférence holiste fondant l'existence de la monnaie. Pour Jewons (1876) et Menger (1892), seul l'intérêt individuel sous-tendant les échanges doit l'expliquer, comme le soutient le « mythe du troc » où la monnaie n'est qu'un facilitateur d'échanges pouvant avoir lieu sans elle (Orléan 1992; Servet 2001, entre autres). L'approche standard est dichotomique, séparant les phénomènes « réels » (relevant de l'économie de marché et des prix relatifs) des phénomènes « monétaires » (prix nominaux). La question du rôle de la monnaie dans la formation des prix (variations réelles ou nominales) se double de son influence sur l'économie réelle (Tutin 2009). Il en résulte une représentation de la monnaie comme « voile » neutre, recouvrant des échanges déterminés sans elle, accompagnée d'une formalisation en termes de théorie quantitative de la monnaie (cf. Encadré n°1 Chap. II.1.1). La détermination du prix et des quantités de monnaie doit se conformer à une logique de marché. Dans une économie vue comme un ensemble de marchés interdépendants, la monnaie n'est que le énième bien (Pliphon 2008) qui, via l'aiguillon du lucre, contraint le marché à l'équilibre. L'échange se réduit aux relations interindividuelles contractuelles et aux arbitrages sous contrainte,

<sup>23</sup> Robbins définit la science économique comme l'analyse du « *comportement humain en tant que relation entre des fins et des moyens rares à usages alternatifs* » (Robbins, cité par Maucourant et Plocimiczak 2012, p. 1). Pour Polanyi (2011), cette définition illustre la « sophistique économiste » de la théorie néoclassique qu'il critique (Chavance 2011, p. xi).

<sup>24</sup> Les questions épistémologiques de la « *querelle des méthodes* » (« *Methodenstreit* ») entre Schmoller et Menger ont « *façonné les divisions disciplinaires dans les sciences sociales à la fin du XIX<sup>e</sup> siècle et au début du XX<sup>e</sup> siècle* ». Il est « *significatif que l'analyse de la monnaie* » y ait pris une place centrale, avec des partisans de la règle opposés à ceux de la discréption, incarnés ici par « *les théories de la "créance" ou du "crédit"* [en concurrence] depuis le quinzième siècle [de] la conception aristotélicienne dominante de la marchandise » (Ingham 2004, p. 24).

<sup>25</sup> La fonction d'utilité, au centre de la théorie du consommateur, axiomatise : une connaissance parfaite des biens échangeables (cf. hypothèse de nomenclature, Cartellier et Benedetti (1994), cités par A. Orléan 2003, p. 5) ; des préférences individuelles fixes, complètes, réflexives, transitives et ordonnables (l'utilité est ordinaire) ; et une rationalité (cf. une optimisation sous contrainte). Cette dernière est paramétrique et solipsiste, car seules importent les quantités de biens et services consommés (les prix étant donnés) et chaque choix d'un agent est indépendant de celui des autres.

supposés produire naturellement un optimum social où les plans individuels sont cohérents et l'utilité de chacun est maximisée. Si le réel et le nominal s'écartent, c'est que la monnaie, ou plus exactement ceux en charge de la gouverner, n'ont pas tenu leur rôle de stabilisation. D'où la question de sa neutralisation et la focalisation sur un encadrement de son émission apte à assurer la fourniture de la « bonne » quantité de monnaie.

L'économie néoclassique accorde une place réduite à l'objet monnaie, qui sert à compter mais ne compte pas (Zelizer 2005). Son « *existence* » reste « *le défi le plus sérieux posé [...] au théoricien* » puisque « *le modèle le mieux développé de l'économie (la version Arrow-Debreu de l'équilibre général walrasien) ne [peut] lui trouver la moindre place* » (F. Hahn [1982], cité par Aglietta 1988, p. 1.). La cohérence interne de l'économie classique rencontre une incohérence externe<sup>26</sup>. Les avancées réalisées au sein de l'économie *standard étendue*<sup>27</sup> ouvrent plus de questions qu'elles n'en résolvent<sup>28</sup>. La *sophistique économiste* à l'œuvre fonde la définition de la monnaie sur sa définition moderne. L'argent et les médiums monétaires doivent remplir parfaitement les fonctions monétaires canoniques dans un espace économique unitaire et exclusif. Cela, malgré une histoire ancienne, mais aussi récente (Polanyi 2011; Cohen 1998; Gilbert et Helleiner 1999; V.A . Zelizer 2005) où la monnaie n'est jamais aussi unitaire qu'elle le paraît (Zelizer 1989) : hier comme aujourd'hui, aucun instrument « *ne peut couvrir à lui seul l'ensemble des usages possibles* » (Blanc 2009b). Les difficultés de ce corpus à cerner la monnaie sont redoublées face à des objets plus composites. L'histoire du champ monétaire et financier regorge d'innovations, variables d'évolution que ce corpus peine à intégrer<sup>29</sup>. Les innovations monétaires relèvent d'*« épreuves d'explicitation »* qui forcent les académiques et praticiens à clarifier la définition de la monnaie, comme les innovations financières remettent en question la définition du marché (Muniesa, 2017, p. 3). Au début du XVIII<sup>e</sup> siècle, l'innovation de J. Law, les monnaies de crédit papier détachées des métaux précieux, suscita ainsi à la fois l'enthousiasme pour leur financement innovant et l'effroi des partisans des monnaies métalliques, préfigurant le débat du XIX<sup>e</sup> siècle entre la *Banking school* et la *Currency school* (de Boyer des Roches et Rosales 2003; Kindelberger 2004, p. 62 et suivantes; Tutin 2009, p. 14-15). Des problèmes théoriques similaires se posent pour les monnaies parallèles. La théorie économique « *tient rarement compte* » des unités de compte propres servant en paiement et en compte à côté de la monnaie légale et, « *lorsqu'elle le fait, c'est avec difficulté (substitutions de monnaies) ou en liaison avec des phénomènes très spécifiques (hyperinflation) qui ne procèdent*

<sup>26</sup> Cinq questions restent ouvertes : la valeur positive des « fiat monnaies » face aux biens et titres disposant d'une utilité et d'un rendement qu'elles n'ont pas ; l'imposition d'une contrainte de « cash in advance » *ad hoc* ; la relation entre stocks et flux ; et l'intégration de la théorie de la demande transactionnelle de monnaie à l'analyse de l'équilibre du marché (Cartelier 2001, p. 994 ).

<sup>27</sup> Cette désignation capture l'intégration dans le cadre néoclassique de modes de coordination alternatifs au marché, en réponse aux incohérences externes, telles que les « *défaillances* » et « *imperfections* ». Bien que différente de la théorie standard, elle en dérive : l'opportunisme et l'intérêt individuel égoïste axiomatisés comme déterminants des comportements permettent d'endogéniser un marché dont la place, paradoxalement, n'est pas relativisée, mais absolutisée (Favereau 2010, p. 6).

<sup>28</sup> Les modèles de l'économie *standard étendue*, comme les « *modèles de prospection* » ou ceux « *à génération imbriquée* » contribuent à la compréhension des phénomènes monétaires. Cependant, leurs apports reposent sur des hypothèses *ad hoc* – hétérogénéité des agents, caractéristiques particulières de certains biens – compromettant la cohérence interne (Cartelier 2001; A. Orléan 2002; Alary 2009).

<sup>29</sup> Le corpus orthodoxe considère à tort les banques comme transformatrices passives de « *high power money* » et ignore leur rôle dans les innovations monétaires et financières (Minsky, 1985). À l'inverse de Kindelberger et Minsky, qui en font la clef de leur théorie des crises : les assouplissements monétaires qu'elles permettent (effet levier, desserrement des contraintes financières, décloisonnement) participent de l'apparition des bulles, contribuant à l'euphorie du *boom* et à l'intensité des *crashes* (contagion de la panique, dissémination des risques, etc. ; Kindelberger 2004 ; Minsky 1985).

*que d'une portion du phénomène* » (Blanc 1998a, p. 6). L'analyse des CM pâtirait-elle des mêmes apories ?

Finalement, l'approche classique est insatisfaisante. La monnaie est-elle objet d'un choix individuel marchand ? Simplifie-t-elle des échanges qui auraient lieu sans elle ? Ou renvoie-t-elle au contraire à un cadre socio-politique, que l'individualisme méthodologique ne peut saisir, un préalable au marché que ce dernier n'est pas en mesure seul de fixer ?

### **Analyser le phénomène monétaire sans l'amputer : un institutionnalisme premier**

Les approches *aprioristes*, *ahistoriques* et *asociales* précédentes négligent le passage de l'individu au(x) collectif(s). Or ce rapport individu-collectif est central dans la monnaie selon les courants hétérodoxes pour lesquels la monnaie est une dette, liée à une incertitude radicale de nature sociale, et relève d'autorités (Wray 2010, p. 37). L'institutionnalisme monétaire francophone (IMF) s'inscrit dans ces approches.

Pour l'IMF, la monnaie est un rapport social fondamental entre sujets économiques. Dans ce corpus théorique, il n'y a pas de valeur préexistante aux échanges et la monnaie est consubstantielle à la valeur comme aux échanges. Contrairement au mythe économique du troc, aucune société ne « *fut complètement démunie* » d'argent, lequel est « *un fait social* » : c'est « *d'une institution, d'une foi* » dont il est question, « *nullement [d']un fait matériel et physique [...] ; sa valeur est celle de sa force d'achat, et la mesure de la confiance qu'on a en elle* » (Mauss 1914, p. 3-4). La monnaie-institution est ici conçue comme un système de paiement, un ensemble de règles fondamentales à la coordination. La fonction considérée comme première est l'unité de compte, mesure préalable sans laquelle les échanges n'auraient pas de termes à honorer : elle rend les échanges possibles avant de les faciliter. Son langage métrologique de la valeur économique structure les relations de dettes et de créances entre les acteurs de la division du travail (Cartelier 1996 ; Aglietta et Cartelier 1998). La monnaie soulève des questions relatives à la qualité des créances et vient avec des incertitudes (défaut de paiement) générant la création de palliatifs institutionnels de confiance combinant hiérarchie et autorité (pouvant se faire pouvoir<sup>30</sup>). La monnaie est conçue comme un accord de groupe : chacun y voit l'expression légitime et consensuelle de la valeur. Historiquement, elle est liée aux pouvoirs souverains imposant leur monnaie et exigeant les impôts réglés par elle. Mais autorité et pouvoir ne se confondent pas avec leurs formes étatiques modernes. L'IMF adopte une approche nominaliste qui n'est pas « *étatiste* », contrairement aux théories chartalistes ou néo-chartistes (Orléan 1998 ; Desmedt et Piégay 2007). Le rôle de l'État et des administrations dans l'*« acceptation, l'émission et la régulation de la monnaie* » moderne est essentiel, mais insuffisant, puisque la légitimité de la monnaie s'éprouve en situation.

L'IMF tente de concilier une analyse théorique transhistorique de la monnaie avec « *une approche historique [des] pratiques monétaires observables* » (Courbis, Froment et Servet 1990, p. 5). Sont d'abord définis des invariants théoriques universaux servant de points fixes heuristiques. Ensuite, ces invariants génériques permettent d'analyser les variations pratiques (synchroniques et diachroniques) de manière comparative. Ces universaux monétaires sont la dette, la confiance, et la souveraineté. La question de la *dette* renvoie aux diverses créances de différents émetteurs, et soulève des questions sur la qualité des signatures. La logique fiduciaire du sceau s'oppose aux titres et monnaies privées sous logique contractuelle de signature. La *confiance* articule trois dimensions :

---

<sup>30</sup> Dans cette thèse, nous utiliserons la distinction webérienne entre le pouvoir, vu comme capacité d'imposer sa volonté contre toute résistance, et l'autorité, vue comme capacité d'imposer une décision grâce à la reconnaissance de sa légitimité.

méthodique, hiérarchique et éthique (Aglietta et Orléan 2002 ; Théret 2008). La monnaie étant un ensemble de règles, il faut examiner les autorités qui les énoncent, les appliquent et les sanctionnent. Le lien entre monnaie, *souveraineté*, pouvoir et autorité est essentiel, mais ne se limite pas à l'État et à ses règles formelles qui soulèvent des réflexions en termes de légitimité. Toute souveraineté incarnée fait face « *d'une façon ou d'une autre [à] la souveraineté des utilisateurs de monnaie* » (Courbis, Froment et Servet 1990, reprenant le concept de J. Rueff, p. 23).

Ce cadre théorique de l'IMF a produit un corpus important d'études traitant de phénomènes monétaires variés, notamment les innovations et expérimentations. Il nous est apparu cependant trop abstrait et théorique pour traiter seul de la gouvernance des CM. Nous empruntons donc aussi au cadre d'analyse et de développement institutionnel (IAD/SES<sup>31</sup>) développé dans les travaux d'Elinor Ostrom et de l'école de Bloomington. Ces derniers ont élaboré un appareillage conceptuel qui a l'avantage de traiter de gouvernance explicitement. Le cadre ostromien développé autour des ressources communes, « *Common Pool Ressources* » (CPR) - physiques ou immatérielles – est tourné tout entier vers l'analyse de la diversité des modes de gouvernance, par des communautés « autogérées » et « polycentriques »<sup>32</sup>. Conçu pour déchiffrer la diversité institutionnelle et ses modalités d'évolution, ce cadre semble indiqué. Fait d'une collection d'analyses empiriques disparates, couvrant des arrangements institutionnels divers, il ne presuppose pas de hiérarchie entre des types de coordination ou des régimes de propriété. Il s'agit d'un cadre *anormatif* et *agnostique*. La gouvernance y est conçue sans présupposer des formes et fonctions qu'elle devrait revêtir, puisqu'elle renvoie à une configuration toujours située de règles, d'interactions et de faisceaux de droits. À la malléabilité de cette boîte à outils répond sa systématicité : quel que soit le degré de décentralisation du système de gouvernance étudié, il est possible d'analyser le cadre des interactions, de définir qui a quels droits et en quels termes. Il s'agit d'un cadre institutionnaliste rigoureux, systématique et ouvert à l'empirie comme aux données qualitatives (Chanteau et Labrousse 2013; Allaire 2013).

Pour identifier les dénominateurs communs de la monnaie, l'IMF suppose la pluridisciplinarité, qui prendra la forme dans cette thèse de l'anthropologie et de la sociologie économique associées à sociologie des sciences et techniques (STS).

## 2) Gouvernance des CM : perspectives sociologiques

Notre ancrage dans l'institutionnalisme économique nous a amené à lire des textes monétaires importants en dehors du champ économique. L'ouvrage *Philosophie de l'argent* (Simmel 2009) occupe une place à part dans la mesure où il a initié un renouveau programmatique ayant entraîné une reconfiguration disciplinaire contestant le « *double partage emboîté* » des sciences sociales, qui prévalait et où prenait place la monnaie<sup>33</sup> (Polanyi 2011 ; Viviana A . Zelizer 1989 ; Dufy et Weber 2007). En France, ce renouveau sur les questions monétaires inclut les chercheurs de l'IMF (Alary

---

<sup>31</sup> Le cadre SES, pour « *Social ecological system* », n'est autre que l'élargissement de l' « *Institutional Analysis and Development framework* », qui est le plus souvent mobilisé dans la littérature (Chanteau et Labrousse 2013, p. 6).

<sup>32</sup> Ce cadre est construit sur une collection d'études de cas d'administration communautaire de CPR. Initialement tournées vers les systèmes de gouvernance de ressources physiques et matérielles – halieutique, hydrique (Ostrom 1990 ; Hess et Ostrom 2007) –, ces recherches ont été étendues à une variété de « nouveaux communs » (Hess et Ostrom 2003 ; Hess et Ostrom 2007 ; Hess 2000 ; Hess 2008 ; Kranich 2007 ; Bollier 2007 ; Mangolte 2013 ; Coriat et Broca 2015 ; Amabile, Peneranda et Haller 2018). Notre problématique n'est pas d'affirmer ou d'infirmer que les CM sont des communs au sens d'Ostrom, bien que cela soit aussi intéressant que possible.

<sup>33</sup> Est séparé le « *reste du monde* », domaine de l'anthropologie, des « *sociétés occidentales* », elles-mêmes découpées entre la « *sphère économique* » de l'économie (qu'elle sépare entre le réel et le nominal) et les « *reste(s) de la société* », des autres sciences humaines (Dufy et Weber 2007, p. 16-17).

et al. 2016) et, dans d'autres pays, des auteurs inscrits à la croisée de l'ethnographie, de l'anthropologie et de la sociologie économique<sup>34</sup>.

### **Anthropologie, ethnographie et sociologie de la monnaie : l'empirie des usages**

Malgré leurs différences, ces approches renouvelent la question monétaire, critiquent les vues économiques orthodoxes et partagent une méthode. À l'opposé des approches instrumentales, elles partent des pratiques et usages, non de fonctions désincarnées. Polanyi (1944, 2011) conteste l'hypostase d'une monnaie remplissant toujours parfaitement les fonctions monétaires canoniques : l'empirie démontre que les usages monétaires se répartissent sur une multiplicité d'objets et d'usages aux fonctions différencierées. Les systèmes monétaires « *primitifs et archaïques* » diffèrent des systèmes « *modernes* » par leurs espaces économiques pluriels et cloisonnés, utilisant des « *Special Purpose Money* » (SPM) aux fonctions bien distinctes : la séparation entre « trésor » et « produit de base » montre des canaux monétaires différents selon les médiums qui circulent, les usages qu'ils remplissent et les personnes qui y ont accès (Polanyi 2011). Les monnaies modernes, après la « grande transformation » de la révolution industrielle, auraient remplacé ces SPM coûteuses et inefficaces par des « *All Purpose Money* » (APM) unitaires et intégrées, remplissant pleinement lesdites fonctions monétaires. La distinction entre SPM et APM montre, par l'anachronisme des APM, le caractère partiel et situé de la définition de la monnaie du corpus orthodoxe, eu égard à la dominance historique des systèmes de SPM. Zelizer (1989), pionnière du renouveau, va plus loin. Elle critique les APM de Polanyi comme étant une hypostase réifiante des monnaies modernes, qui ne sont ni « tout usage », ni parfaitement homogènes.

Zelizer (1989) oppose une approche systématique de la construction sociale de la monnaie aux visions hégémoniques des « monnaies de marché »<sup>35</sup>. Cette approche permet de penser l'altérité et les « imperfections » monétaires au travers de différentes conversions et *marquages*, altérité vue comme des différenciations plus ou moins subjectives que la monnaie subit objectivement du fait de ses usages<sup>36</sup> (Zelizer 1989 ; Zelizer 2005 ; Blanc 2009). Cette approche renouvelée n'oppose plus les SPM aux APM, car le système monétaire moderne, bien qu'unitaire en apparence, est façonné par ses utilisateurs, au-delà des règles et des formes monétaires instituées par le pouvoir souverain.

Ces approches partagent de penser l'argent comme le produit de trois éléments : les systèmes de compte instituant valeur et équivalences (règles et dispositifs variés comme la comptabilité et la gestion, la fiscalité, etc.), les instruments monétaires (différents objets) et les relations sociales dans

---

<sup>34</sup> A. Zelizer assume explicitement sa proximité programmatique avec les auteurs de l'IMF, reconnaissant s'être « *rendu compte que ces sociologues alternatifs de l'économie [Aglietta, Orléan, Blanc, etc.] avançaient dans la même direction qu['elle]* » (Florence Weber et Zelizer 2006, p. 128).

<sup>35</sup> Malgré la diversité des approches, de la théorie économique standard à Marx, Simmel, Weber, Zelizer (1989) circonscrit cinq hypothèses problématiques et les remplace : (i) les caractéristiques et les fonctions monétaires ne sont pas uniquement économiques ; la monnaie existe aussi en dehors du cadre marchand et est influencée par des facteurs culturels et sociaux ; (ii) considérer la monnaie comme homogène, divisible, liquide est une erreur, car ces caractéristiques dépendent de la qualité des médiums, des cadres institutionnels et des acteurs ; (iii) il existe une pluralité de types de monnaies (« *monies* ») dans nos sociétés modernes - et les différences monétaires importantes ne résident pas seulement dans la quantité, mais dans des facteurs qualitativement différents - ; (iv) la dichotomie entre valeur monétaire et non monétaire est arbitraire ; voir les monnaies modernes comme profanes et utilitaristes est un tropisme, la monnaie peut être singulière et non échangeable ; (v) le pouvoir de corruption des valeurs non pécuniaires par l'argent est contrebalancé par le fait que le social influe sur la monnaie (Zelizer 1989, p. 347).

<sup>36</sup> Zelizer a étudié différentes « *monies* » : le revenu de la maîtresse de maison au sein d'un ménage ; le don d'argent, l'argent de la charité et de l'aide sociale (bons d'achat, paiements en nature). Elle montre que la culture et les structures sociales limitent les processus de monétisation, imposant à différents moments de la séquence des paiements, des contrôles et restrictions à la liquidité monétaire selon les usages, utilisateurs, système d'allocations, de contrôle et autres différenciations (Zelizer 1989, p. 351-367).

lesquelles ils sont utilisés, ainsi que transformés. Pas de monnaie sans usages. Toute analyse monétaire doit partir des usages, de leur contexte matériel et de leurs significations indigènes, car il est impossible de dissocier ce que font les acteurs de leurs intentions et de leur identité (Zelizer 1989 ; Blanc 2009). Aux usages sont attachés des cadres cognitifs, ainsi que des valeurs et représentations des coéchangistes, des groupes et, plus largement, de la société considérée, qu'il est crucial d'analyser (Dufy et Weber 2007). Ces cadres sont constitués par un langage et des procédures de qualification, dont il est impératif d'observer les règles et évolutions. Pour Zelizer et l'IMF, la monnaie est un signifiant social qui témoigne des fondations d'une communauté politique qu'elle participe à ériger. Aucune recherche ne peut faire l'économie d'une analyse des usages, représentations et dispositifs institutionnels qui s'articulent pour faire monnaie. Pour comprendre les arrangements et dispositifs des CM et répondre aux préférences technicistes qui les accompagnent, nous avons ajouté une dernière corde conceptuelle à notre arc théorique.

### **Au-delà des « boîtes noires » : les CM, des infrastructures « sans coutures »**

Malgré leur opposition apparente, les détracteurs et promoteurs des CM partagent une vision réifiante de la monnaie qui confine au fétichisme. Les préférences des uns ou le réductionnisme des autres reposent sur un tropisme techniciste voyant les CM comme des « boîtes noires », au sens de Bruno Latour : illusion d'une pure technique autonome et stabilisée, se maintenant « *par elle-même comme réalité discrète et déterminée, indépendante de tout point de vue* » social et politique (Quéré 1989, p. 102). Les STS se sont constituées contre ce « *technologisme* » : la technologie et la société sont « *deux objets fabriqués* » (Latour 2006, p. 4) qu'il est stérile de vouloir séparer en « *deux mondes* », même conceptuellement (Akrich 1989, p. 31-32). Il faut nous départir de cette dichotomie arbitraire, comme de beaucoup de catégories « *qui nous conduisent à décrire un monde déjà fait* » (Callon 2006, p. 3) : fin et moyen (Latour 2000), *on chain\** et *off chain\**... Il est impossible d'adhérer à l'idée d'une technique obéissant uniquement à une rationalité propre et neutre. Pour dépasser ce « *technologisme* », comme éviter les ornières de la vision opposée du « *sociologisme* »<sup>37</sup>, la technique est considérée comme « *un tissu sans couture* », un objet socio-technique (Latour 2006; Akrich 1989). Nos e-monnaieurs, comme Edison, naviguent « *en eaux troubles entre le social, le technique, l'économique, etc., négociant les contenus mêmes de leurs innovations avec les acteurs qu'ils souhaitent enrôler, y incorporant les résultats de différentes épreuves de toute nature qu'ils s'imposent* » (Akrich 1989, reprenant Hughes, p. 32). La métaphore de l'absence de couture souligne qu'un objet socio-technique mêle toujours, au fur et à mesure de son développement, des problématisations, grammaires argumentatives et références hétérogènes, non purement techniques.

En tant que composite, un objet socio-technique incorpore dans son design un scénario qui traduit une « *description du monde social dans lequel* » il doit fonctionner. Les dessins de l'innovateur traduisent ses desseins, d'où une neutralité impossible qui a deux implications : les ressources et contraintes inscrites dans les dispositifs techniques influent sur le monde social, et les acteurs du monde social, en retour, peuvent détourner ces dispositifs du scénario original. Les dispositifs techniques et agencements sont des objets puissants de partition du monde physique et social, ils agissent, font agir, et leurs configurations attribuent positivement des rôles à certains acteurs - humains ou non - et en relèguent d'autres, ainsi qu'elles déterminent (ou interdisent)

---

<sup>37</sup> Le *sociologisme* se réfère à des « *modèles plus savants* », où la technologie est conçue comme « *une construction éminemment sociale* ». Ces démarches, bien qu'elles permettent « *de caractériser des styles techniques [,] de retracer la genèse des formes prises par tels ou tels dispositifs* », et de se « *défaire de l'idée [d']une rationalité purement technique* », perdent la capacité d'expliquer les « *destins différenciés* » des objets techniques en réduisant « *l'ensemble des choix techniques [...] à des déterminations sociales* » (Akrich 1989, p. 31-32), voire idéologiques pour les CM.

certains modes de relations (Akrich 1989, 2010). Bien qu'ils « *constituent des éléments actifs d'organisation des relations des hommes entre eux et avec leur environnement* », rien n'assure leur bon fonctionnement, ni que l'« *utilisateur-projet* » incorporé dans les desseins originaux correspond à l'« *utilisateur réel* » : tout objet technique rencontre des hiatus « *entre la conception et l'utilisation* » (Akrich, 2010, p. 205 et 208). En ce qui concerne les CM, les écarts au scénario prennent notamment la forme de failles, de bogues, d'attaques informatiques, ou d'insatisfactions diverses. Ces situations, qu'il s'agisse d'usages encadrés par les codes qui s'écartent de leurs attendus ou d'une demande explicite de certains acteurs de faire évoluer le scénario (optimisation ou modification radicale du protocole, par exemple), illustrent le caractère toujours (re)négocié et composite d'une CM. Dans ces cas, la technologie, incapable de se corriger par elle-même, a besoin du travail d'alliés humains organisés. La gouvernance *sur* l'infrastructure réapparaît alors, où un « conflit / débat » n'est pas seulement technique, mais aussi socio-économique (De Filippi et Loveluck 2016; Rolland et Slim 2017). Les évolutions protocolaires sont exemplaires. Faire évoluer une CM, c'est redéfinir les moyens et les fins. Cela mobilise des acteurs, leurs perceptions des fins et moyens désirables, et induit des arbitrages révélant des intérêts, contraintes et opportunités situées.

Plus que de simples objets socio-techniques, les CM correspondent à la définition et aux propriétés d'une infrastructure - physique ou numérique<sup>38</sup> - selon les STS et les *Infrastructural Studies* (Star 1999 ; Bowker 1996 ; Edwards et al. 2009, cf. Chap. I). De Filippi et Loveluck (2016) et Kavanagh et Missione (2017) l'ont souligné pour Bitcoin. Une infrastructure est relationnelle et écologique, apparaissant « *comme une propriété relationnelle, et non comme une chose dénuée d'usage* » (Star, 1999, p. 377). Inscrite « *dans un équilibre entre l'action, les outils et l'environnement construit* », une infrastructure ne le devient réellement que « *par rapport à la pratique organisée* » d'acteurs disparates. À cause de son échelle, différents points de vue sur elle cohabitent selon la position des acteurs et groupes qui en parlent. Leur analyse requiert une « *inversion infrastructurelle* », qui met en avant les éléments sous-jacents des pratiques qui s'y rapportent et lui donnent corps (Bowker, 1994, cité par Starr, 1999, p. 380). Dans ce corpus de travaux, une infrastructure n'est pas construite, mais émerge, croît et se développe, suivant des processus, des étapes (création de standards, de passerelles\*...), grâce au travail d'une myriade d'acteurs humains (Edwards et al. 2009). Il est donc crucial de s'intéresser aux activités routinières indispensables à leur fonctionnement, comme aux mains qui les effectuent. Comme pour l'IMF ou la sociologie économique, il faut analyser l'écheveau des représentations, des structures matérielles et relationnelles, pour comprendre une infrastructure.

Il est significatif que les travaux les plus proches de notre objet et de nos problématiques proviennent de chercheurs inscrits dans le champ des STS (Mallard, Méadel et Musiani 2014 ; Karlstrøm 2014 ; De Filippi et Loveluck 2016; DuPont 2018 ; Musiani, Mallard et Méadel 2018). Ces travaux mettent en lumière les rôles essentiels d'arrangements techniques divers, au cœur desquels se trouvent des formes de coopération et la construction de valeurs partagées. Ainsi, plutôt que de partir d'une définition figée *a priori* et réifiante de la gouvernance (et son lot de prescriptions formelles), notre approche la saisit plus positivement, comme un ensemble de processus dynamiques, indéterminés et informels, renvoyant à des situations singulières (nos terrains de crise, cf. infra) et aux interactions qui s'y nouent. Elle s'y conçoit comme un ensemble de règles, logiques, cadres et structures d'actions collectives, au-delà de leurs seuls aspects institutionnels formels.

---

<sup>38</sup> Les « *e-infrastructures* » sont considérées comme des infrastructures en raison de leur intégration dans l'économie et la vie sociale, offrant « *des systèmes et des services robustes, fiables et largement accessibles [ressemblant] dans leur forme et leur centralité, aux équivalents numériques des infrastructures canoniques de la téléphonie, de l'électricité et du réseau ferroviaire* » (Edwards et al. 2009, p. 365).

### 3) La gouvernance de Bitcoin et d'Ethereum dévoilée par leurs crises

Pour aborder la gouvernance des CM, nous avons choisi d'examiner les phénomènes de crise. Bien que leurs formes et enjeux varient, les crises sont des objets d'études privilégiés, tant pour l'IMF qui les utilise pour étudier la monnaie, que pour les STS, où un corpus spécifique s'est développé.

#### Les fonctions heuristiques et herméneutiques des « crises »

Dans le champ monétaire, les crises sont souvent considérées comme des moments privilégiés d'étude où la monnaie se « dévoile », révélant ses dimensions historique, sociale et politique (Théret, 2007). Les crises interrompent le « *fonctionnement routinier de la monnaie* », obligeant les observateurs à questionner les stabilités passées. Elles révèlent le fond social et politique des systèmes monétaires qu'elles touchent, dans leurs dimensions matérielle et idéelle (*Ibid.*, Simmel 2009). Les fonctions, instruments, usages et acteurs de la monnaie y apparaissent plus fragmentés et dissociés.

Dans les STS aussi, la crise, ainsi que les controverses technologiques, ont une place de choix. En tant que « *point de fusion où la technologie prend forme* », s'y découvrent les « *nombreuses négociations qui précèdent et délimitent les choix techniques* » : l'objet socio-technique, quelque réifié qu'il soit, s'entrouvre (Callon 2006, p. 3). Deux des propriétés reconnues à une infrastructure s'y rapportent : une infrastructure « *devient visible lors de la panne* » et elle est « *fixée par incrément modulaires, pas tout d'un coup ou globalement* » (Star 1999, p. 382). Étant grande, en couches et complexe, l'infrastructure signifie différentes choses localement et n'évolue pas depuis le haut, car tout changement prend du temps et nécessite des négociations avec tous les acteurs impliqués (*Ibid.*). Dénaturaliser la crise exige « *d'abandonner la recherche des causes et de se défaire de la distinction entre l'état routinier du monde et le phénomène critique* » (Aguiton, Cabane et Cornilleau 2019, p. 11). Seront donc interrogées dans cette thèse les catégories arbitraires opposant la routine au dysfonctionnement, le bogue à l'attaque, le normal à l'exceptionnel. La crise révèle un hiatus entre le scénario projeté du concepteur et celui réellement mis en scène par les usages. Elle informe sur l'état du monde social considéré comme « *normal* » et celui qui ne l'est pas. La crise n'est pas donnée, mais se fabrique. Le regard des STS nous engage à étudier « *la politique de la crise* » et « *son gouvernement* », d'un bout à l'autre - de la mise en crise à la remise en ordre - afin de faire apparaître les ressorts, enjeux et acteurs de cette entreprise (*Ibid.*). Dans la crise, l'objet socio-technique prouve qu'il est toujours en train de se faire et se défaire, au gré des stratégies d'acteurs impliqués. Il convient d'interroger les conditions de « *survenue* », de « *normalisation* », d'*« aggravation* » ou de « *contention* » de la crise, jusqu'à sa « *résolution* ». Au cœur de la gouvernance de crise, on trouve des acteurs humains pour qui elle n'a rien d'exceptionnel, puisqu'ils travaillent avec elle au quotidien. Ils en produisent les diagnostics et en prennent la maîtrise grâce à des outils, dispositifs et procédures *ad hoc*, qu'ils ont contribué à implémenter. La crise met au jour les arrangements en place visant à l'anticiper, à l'empêcher, voire, si elle advient, à la contenir et à la corriger. Le gouvernement des crises représente « *un site de démarcation du visible et de l'invisible* » (*Ibid.*, p. 18). S'y dévoile l'irréductible normativité des étiquettes, des statuts des parties prenantes (victimes, responsables, etc.), des définitions retenues du tolérable, des degrés de gravité, de priorité et d'urgence.

## Du périmètre de nos terrains : deux crises différencieront Bitcoin et Ethereum

Notre thèse que les CM font monnaie en induit une seconde : la singularité monétaire des CM réside dans la présence (et non l'absence) d'une gouvernance polycentrique (cf. Chap. II). Ce travail analysera cette spécificité au travers de l'étude de deux crises, l'une concernant Bitcoin, l'autre Ethereum. Examinons ces choix.

Choisir un terrain n'est jamais facile et, dans ce champ, une difficulté tenait à son étendue. Lorsque nous découvrons les CM, on en compte déjà des centaines, voire des milliers, et cet espace n'a cessé d'évoluer extensivement<sup>39</sup> et intensivement (au sein d'une même CM, les technologies et usages s'étoffent). Nous avons pris connaissance et/ou assisté à de nombreux événements, plus ou moins importants, qui ont touché l'écosystème des CM au cours de ces années, et il apparaît clairement qu'aucune CM n'est jamais fixée dans sa forme et son contenu. Négociées, les CM connaissent des évolutions techniques, économiques, institutionnelles et relationnelles. De ce constat ont surgi des contraintes pratiques : nous faisions face à des masses considérables de données et de documents potentiellement à traiter (Berry, 2012). L'objet est également vaste géographiquement. Ces systèmes monétaires impliquent un éclatement communautaire, une multiplicité d'arrangements plus ou moins locaux/globaux, suivant les réseaux\* relationnels de leurs membres. Nous avons donc restreint notre terrain à la suite d'une phase exploratoire (cf. section C. ci-après), choisissant spécifiquement Bitcoin et Ethereum, les deux CM les plus capitalisées, ainsi que les plus dynamiques en termes de développement et de communautés. Elles sont selon nous idéal-typiques de ce que recouvre le concept de CM : partageant les caractéristiques communes attendues d'une CM - ouverture formelle à « tous », *résistance à la censure\**, consensus multipartite fondé sur la *PoW*<sup>40</sup>, etc.), elles diffèrent sur le plan de leur architecture et de leur gouvernance, alimentant des controverses entre leurs communautés. Pour restreindre encore notre terrain, nous avons choisi d'analyser pour chacune d'elles un moment de « crise » particulier : le bogue CVE 2018 #17144 pour Bitcoin et la crise ouverte par l'attaque de « The DAO » pour Ethereum (cf. Chap III).

Ces deux crises se révèleront aussi typiques de deux types de crises et de deux formes de gouvernance différencieront que cette thèse s'emploie à expliciter. Le premier type est ce que nous appellerons une « *crise de vulnérabilité* » et l'autre une « *crise d'évolution* ». Chaque type est défini relativement à la situation conçue comme normale, quand ce qui est permis par les codes protocolaires - la « lettre du code » - est conforme à ce qui est attendu et considéré comme légitime par le consensus social – l'*« esprit du code »*. Deux formes de hiatus peuvent en effet apparaître entre la lettre et l'esprit du code. Se dessinent tout d'abord les *crises de vulnérabilité*, liées à une faille relevant d'une situation où les codes donnent des résultats qui sont pour les acteurs en contradiction explicite avec ce qui est attendu. Par exemple, si la lettre du code permet d'envoyer deux fois les mêmes UCN\* (cas explicite de *double dépense*\*), et ce faisant de créer des bitcoins en dehors des règles de monnayage canoniques, la contradiction avec le consensus social est flagrante. C'est ce qui s'est joué, au moins théoriquement, dans la crise Bitcoin CVE 2018 #17144. Les *crises d'évolution*, quant à elles, se révèlent différentes dans leurs processus de mise en crise et de remise en ordre. Elles correspondent à une situation où le code ne permet pas de faire ce que les acteurs aimeraient implicitement qu'il fasse. Bien qu'il fasse ce qui était attendu de lui, ce code est contesté

---

<sup>39</sup> Bien qu'il en apparaisse et disparaisse chaque jour, leur nombre augmente tendanciellement. Voir le panorama « exhaustif » de l'évolution de l'écosystème des CM, entre avril 2013 et juin 2017 (ElBahrawy et al. 2017).

<sup>40</sup> Ethereum, le 15/09/2022, a transitionné d'un algorithme de consensus\* en preuve de travail (*PoW*) à un algorithme en preuve d'enjeu (« PoS »). Bien que prévu dès l'origine (voir Kessler 2022 ; Miller 2022, cf. Chap. I), ce travail couvrira uniquement la version en *PoW*, seule en fonctionnement à l'époque de notre recherche.

par certains souhaitant le voir évoluer, par exemple en demandant à modifier le protocole d'Ethereum afin de bloquer les fonds d'une adresse suite à un vol. Ce qui s'est joué dans la crise de « The DAO ».

Pour analyser les modes de résolution de ces deux types de crises, nous nous appuierons sur la conceptualisation de deux formes particulières et mutuellement exclusives de gouvernance présidant à la remise en ordre : une forme que nous qualifions « *de huis clos* », à l'œuvre dans la crise analysée de Bitcoin, qui s'oppose à une autre « *publique et ouverte* », déployée dans le cas de « The DAO » d'Ethereum. Crises *de huis clos* ou *publiques et ouvertes* dévoilent les deux faces opposées d'une même pièce, celle de la gouvernance des CM. Chaque face renvoie à l'établissement de diagnostics et de solutions différenciés, relevant de cadres procéduraux et relationnels spécifiques (règles et procédure applicables, acteurs et dispositifs impliqués).

## C. UNE DÉMARCHE ETHNOGRAPHIQUE, POUR UN TERRAIN D'ENQUÊTE MULTI-NIVEAU

Nous précisons maintenant les matériaux empiriques de cette thèse. Comme toute enquête est « *tributaire des conditions d'entrée sur le terrain* » toujours singulières, renvoyant aux « *caractéristiques du terrain et des enquêtés, à celles du chercheur, et aux interactions qui s'établissent entre eux* » (Bué 2010, p. 78), nous expliciterons d'abord le contexte de collecte de ce matériau. Notre recherche, basée sur une démarche et des données qualitatives, est idiographique. Ce choix s'est affirmé à mesure de notre avancée. Face à un champ émergeant, il était pertinent de mobiliser une approche éprouvée en contexte de découverte(Avenier et Thomas 2011). Nos réflexions méthodologiques ont lié ensemble notre objet, nos terrains d'enquête et nos perspectives de recherche.

### 1) Enquêter sur la gouvernance des CM : contraintes et enjeux

Expliciter nos matériaux nécessite, au préalable, de « *faire état du contexte particulier de [notre] terrain et d'expliquer, en lien avec la spécificité de celui-ci, les stratégies et les façons de faire adoptées pour mener l'enquête* » (Pastinelli 2011, p. 38). Au départ, en tant que parfait étranger à la science informatique, cet accès fut complexe. En plus de cerner notre objet, il nous fallait aussi cerner les acteurs en présence afin de nouer contact. À la crainte de l'étrangeté s'ajoutait celle liée aux difficultés que nous pensions rencontrer lors de prises de contact<sup>41</sup>.

#### Enjeux méthodologiques

Le premier enjeu tient à la définition de l'objet CM comme infrastructure au sens de Star (1999). Son périmètre large renvoie à une pluralité d'usages et à des pratiques disparates. Le tournant infrastructurel réclame d'« *aller dans les coulisses* » pour « *faire remonter à la surface le travail invisible* » qui s'y effectue et l'ensemble des éléments qui s'y rapportent (*Ibid.* p. 385). Encore faut-il arriver à situer, même sommairement, la scène. Si, à son amorce, toute recherche n'a pas à proprement parler d'objet, notre choix d'« *étudier le non-étudié* » et ses « *choses ennuieuses* » (Star 1999, p. 382) dans un contexte pour nous étranger rendit la chose plus ardue encore. Saisir les significations indigènes, les cadres cognitifs des protagonistes nécessitait la

---

<sup>41</sup> Nous savions que « *faire des recherches dans un contexte où les gens pensent pouvoir tirer profit de la démarche du chercheur est bien différente de faire une enquête là où sa présence apparaît comme dérangeante* » (Pastinelli 2011, p. 37), et anticipions de rencontrer nous-même la seconde situation. Finalement, nous avons rencontré les deux, ce qui nous a forcé à adopter des stratégies spécifiques suivant les interlocuteurs.

maîtrise d'un langage propre (d'où la nécessité de constituer un glossaire, cf. annexe de cette thèse). Ce jargon, mixture de langage d'ingénieur informatique, de cryptographe et de financier, déstabilisait les définitions et catégories préexistantes : le *vocabulaire de la monnaie* était « transformé par celui des machines » (adaptation libre de Muniesa 2017, p. 1). À cela s'ajoutait la question, inhérente aux infrastructures, du passage « à une échelle plus grande que les espaces traditionnellement étudiés par l'ethnographie », puisque « les groupes sont distribués géographiquement et temporellement, et peuvent impliquer des centaines de personnes et de terminaux », imposant « la récolte et le traitement d'une quantité large de données (transaction\* log, ...) afin d'arriver à comprendre le jeu réciproque des actions en ligne et hors-ligne » (Star 1999, p382). Les CM doivent leur réalité matérielle à Internet comme à leurs *parties prenantes\** dont les identités et statuts ne sont pas forcément présents. Leur *topos* évolue en dynamique, suivant des frontières technologiques et communautaires plus que géographiques. À la manière des infrastructures physiques qui n'ont pas émergé d'un coup, les CM émergent « *d'abord à des échelles de temps, d'espace et de service plus petites, en tant que systèmes de second ordre construits sur et autour de l'Internet et d'autres cadres d'information existants* » (Edwards et al. 2009, p. 366). Outre les relations transactionnelles *on chain\**, acteurs humains et non humains cohabitent dans des arènes de débats et discussions qui se déploient *off chain\**, tant dans le « cyberespace » que dans le « réel ». Les premières renvoient à de nombreux canaux de communication, plus ou moins publics, sur différents types de plateforme (réseaux\* sociaux, *forges logicielles\**, canaux IRC<sup>42</sup>, listes de diffusion, etc.). Dans le réel, les communications traversent des communautés dispersées, mais passent aussi par le travail de certains acteurs (individus ou organisations) qui organisent des rencontres, conférences, présentations, etc., là encore, plus ou moins ouvertes et ciblant différents types d'audience (développeurs\*, investisseurs, etc.).

Les enjeux de méthode dépendent des perspectives de recherche, et l'espace électronique n'a pas le même statut suivant le point de vue du chercheur (Pastinelli 2011, p. 40). Pour les interactions médiatisées par les protocoles de registre\* distribué ouvert\* que nous étudions, les CM recouvrent bien « *des pratiques ou des phénomènes qui n'ont d'existence qu'en ligne, qui sont nés des communications électroniques* » (*Ibid.*), ce qui imposait d'emblée le cyberespace comme terrains d'enquête. Nous ne nous sommes cependant pas cantonné à la réalisation d'une « netnographie »<sup>43</sup> et avons aussi mené des entretiens et pris part à une diversité d'événements (cf. infra). Bien sûr, pour observer les communautés de *coiners\** et les relations qui s'y tissent, Internet devenait pour nous un terrain d'enquête - un lieu, un espace ou un outil - privilégié. Les CM impliquent certes des relations en ligne, ne pouvant s'observer que là où elles existent, mais dans quelle mesure l'observation de cette face visible était-elle suffisante ? Dans une logique infrastructurelle, l'espace numérique n'est pas autonome. À la fois virtuel et réel, sa réalité matérielle repose synchroniquement sur des pratiques qui s'y rapportent. Circonscrire le contexte dans lequel les pratiques et discours prennent sens conduit à interroger la façon dont les *coiners\** prolongent et articulent leur vie en ligne et hors ligne. Plus qu'une ethnographie du virtuel, il fallait « *en finir* » avec elle, rompre d'avec la « *réification d'un espace électronique [qui fait] abstraction de la large diversité des pratiques, contextes et phénomènes en cause [...] en train de prendre forme et [toujours] appelés à se transformer* » (Pastinelli 2011, p. 39).

---

<sup>42</sup> Pour Internet Relay Chat, un système de messages instantanés et de canaux de discussion.

<sup>43</sup> Concept de Kozinet (2002), la netnographie correspond non pas à une enquête sur Internet mais *via* Internet. Elle correspond à « *une nouvelle méthode de recherche [et] d'analyse de contenu ou de discours d'espaces électroniques [...] qui pourrait avantageusement remplacer les groupes de discussion et les entrevues individuelles pour le chercheur* » (Pastinelli, 2011, p. 41).

## La relation enquêteur-enquêtés

Il est temps de revenir sur *le*, ou plutôt *les* (Bué 2010), rapports enquêteur-enquêtés développés lors de nos enquêtes. L'enquête ethnographique mène le chercheur, au même titre que les enquêtés, à s'impliquer activement. Cette implication mutuelle détermine en partie la forme et le contenu des relations, et influence les résultats que le chercheur en tire (Duclos 2014). À s'en tenir à sa mise en récits, la gouvernance de Bitcoin et Ethereum ne devrait pas avoir grand-chose à voir avec celle de la coalisation locale de partis politiques analysée par Bué (2010) ; pourtant, notre terrain fut lui aussi « *démultiplié en plusieurs espaces sociaux, à la fois imbriqués, interdépendants et concurrents* », et notre enquête s'est apparentée « *à une dynamique entre des acteurs sociaux aux attentes et intérêts distincts* » à laquelle nous participions (p. 77-78). De ce fait, « *la présentation de soi ou la distance aux enquêtés, la gestion de la pluralité des relations d'enquête* » furent des enjeux particulièrement prégnants pour nous (*Ibid.*, p. 78), que ce soit lors de notre entrée sur le terrain, ou par la suite, selon les développements que prenaient nos recherches. A cours de nos terrains, nos rapports enquêteur-enquêtés ont évolué dynamiquement, sont devenus pluriels et ambivalents. Les formes de méfiance réciproques originelles, de défiance même, ont laissé la place, au gré des rencontres et échanges, à des relations plus paritaires ou symétriques voire, pour un petit nombre d'entre elles, amicales.

De notre côté, la défiance originelle s'explique par notre point d'entrée nourri par nos premières recherches documentaires *via* la littérature grise et notre forme initiale de netnographie. En 2015, les ressources disponibles sur Bitcoin et les CM étaient très majoritairement anglo-saxonnes, et même états-uniennes. À l'éthos monétaire premier de leur design, opposé frontalement au nôtre, s'ajoutait une gangue idéologique située à l'*« extrême droite américaine »* imprégnant nombre de ressources (Golumbia 2015, p. 119-120). La répulsion que nous pouvions avoir pour ce « *cyber-libertarianisme* », mêlant rhétorique « *anti-gouvernementale* » et « *anti-banque centrale et/ou banque commerciale* », sera peu à peu dépassée par notre rapprochement avec des acteurs français. Ceci permit de construire une certaine distance lors de nos premières approches d'acteurs. Ce qui, au vu de nos premiers contacts, s'avéra judicieux : il était erroné « *d'homogénéiser Bitcoin en termes politiques* [comme le fait] *Golumbia* », car « *il s'agit d'un point de vue inutilement unilatéral* » (Dodd 2017, p. 6-7) qui laisse de côté l'essentiel : l'hétérogénéité en valeur des communautés de *coiners*\* et les conflits que cela induit. Nous n'étions pas seul à avoir des *a priori* : notre statut de doctorant en sciences humaines nous rangeait parmi les académiques et ce faisant, nous étions de la partie adverse. Nous avons expérimenté en pratiques la discorde existant entre les experts monétaires et les *coiners*\* (cf. Chap. II). Si, au départ, nous en avons fait les frais<sup>44</sup>, par la suite, les soupçons préalables dissipés, notre présence et notre statut ont pu évoluer positivement. Le reproche le plus communément mobilisé par les *coiners*\* à l'encontre de leurs détracteurs nous semblait compréhensible : il renvoie en effet à l'*« asymétrie constitutive du rapport enquêteur-enquêté qui tend à faire du premier le sujet de la recherche et du second son objet [...] : qui étions-nous [...] pour prétendre être ceux qui, d'abord, sauraient poser les bonnes questions ? »* (Duclos 2014). Face à un champ émergeant, articulant des objets disparates relevant de disciplines spécialisées et à mille lieues de nos compétences initiales, arborer le « *regard surplombant de l'observateur extérieur* » (*Ibid.*) était pour nous problématique scientifiquement. Afin « *que les acteurs ne soient pas amputés d'une partie d'eux-mêmes* », il fallait dépasser cette « *asymétrie* », ce « *privilege* » « *accordé aux sciences sociales* » (Callon 1986, p. 171-172) comme en éviter les

---

<sup>44</sup> Lors d'une de nos premières observations participantes, un « social meet up » Bitcoin au Sof's Bar, un participant nous interpella de la sorte : « *sociologie à l'EHESS, tu es communiste* » après notre divulgation du fait que notre thèse s'inscrivait en socio-économie et que nous la réalisions à l'EHESS [Observation participante n°3, voir annexe n°IV.2].

écueils<sup>45</sup>. Il nous fallait aussi dissiper le soupçon prégnant d'incompétence – chez nos acteurs, mais aussi pour nous-même ! -, alors que de nombreuses critiques acerbes largement publicisées se voyaient disqualifiées par leur manque de connaissances empiriques solides et de maîtrise technique. Bien que les extraits suivants s'adressent à des auteurs spécifiques - pourtant loin d'être les plus critiquables –, leur teneur est symptomatique des reproches émis à l'égard du monde académique. Selon cet enquêté, on entendrait en effet trop « *parler des gens comme Primavera, De Fillipi ou Emin je ne sais plus qui là, le gars de Cornell [Emin Gün Sirer, NdA] et je trouve qu'ils disent pas mal de bêtises en fait [...] ils émettent des avis sur les caractéristiques des réseaux\** », leur décentralisation et tout ça, qui sont malheureusement faux. [...] qui mélangent tout [...] sans avoir les fondamentaux pour en parler » [P. Noizat, Entretien n°24]. Lorsqu'ils veulent étudier la « *gouvernance technique* » des CM, les chercheurs en sciences humaines se trouvent « *dans le domaine des ingénieurs* », ouvrant un problème de méthode à aborder avec humilité<sup>46</sup> : « *comme un mécanisme d'horlogerie [qui n'est] appréciable que si vous êtes l'homme de l'art [...]. Il faut être humble. [Pour pouvoir] parler de la technologie il faut vraiment faire cette démarche de coder. [...] Si vous prenez Claude Levis Strauss, [...] il a été le premier à dire l'importance des langues primitives pour comprendre les peuples. Je pense que c'est pareil pour les ordinateurs, si vous n'apprenez pas leur langage, vous êtes un visiteur hein. Vous n'êtes pas du tout scientifique dans la démarche* » [P. Noizat, Entretien n°24]. C'est ainsi que tournera court notre « entretien » avec M. Falke [Non-Entretien n° 27], qu'il nous avait demandé de réaliser sur un forum public. Notre questionnaire ne parlait pas le bon langage, allait à l'encontre de presque toutes les conventions tacites du forum, là où nous nous étions naïvement arrêté à notre interprétation des règles formelles d'usage. Si la majorité de nos questions nous semblait porter sur le client Bitcoin, notre questionnaire fut retiré moins de 10 minutes après sa publication du fait de son caractère « *hors-sujet* » et « *non adapté au format* » d'un forum (les questions personnelles, par exemple) « *construit autour de l'obtention de réponses à des questions techniques objectives* », visant à décourager celles « *subjectives ou basées sur des opinions, ou qui ne peuvent être répondues que par des personnes spécifiques* » (*Ibid.*, voir annexe n°IV.4). Alors que notre travail montre que la gouvernance sur l'infrastructure repose justement sur des individus spécifiques, non interchangeables dans la pratique. Pour nos interlocuteurs, ce qui ne s'expliquait pas par de l'incompétence pouvait l'être par la malice. Ainsi peuvent-ils taxer leurs détracteurs de relayer de la « *propagande, voire [de la] désinformation* » [P. Noizat, Entretien n°24], ce qui renvoie au conflit idéologique les opposant aux systèmes monétaires et financiers traditionnels et à leurs intérêts organisés. De même, la qualification juridique des actions de nos protagonistes était entourée d'incertitudes pesant sur la libération de leur parole : le cas « *The DAO* », avec ses enjeux de réputation, ses conflits violents et menaces de procès, est sur ce point exemplaire. Nos premières tentatives de contact nous montrèrent que l'obtention d'entretien n'allait pas être chose aisée : nombreux sont les acteurs contactés à n'avoir jamais répondu, quand d'autres n'ont fait qu'y opposer un refus, arguant de leur appréhension des risques encourus (nous pensons au CEO de Slock-it et à certains de ses salariés ayant pris part aux opérations de sauvetage de « *The DAO* », par exemple).

Si nous ne sommes pas arrivé aux compétences en codes attendues par l'interviewé cité plus haut, nos appréhensions premières ont chevillé en nous une volonté de maîtrise pointilleuse du sujet. C'est seulement après une longue maturation, dans le confort asynchrone de l'observation passive

---

<sup>45</sup> C'est cette asymétrie et les difficultés de trois ordres (stylistique, théorique et méthodologique) qu'elle produit, que se propose de dépasser la sociologie de la traduction de Callon (1986).

<sup>46</sup> P. Noizat, [Entretien n°24] dans ce passage, fait référence au statut de juriste de De Filippi, pour expliquer « *les limites de [mes] collègues* » ; dans le même temps, Gün Sirer est un chercheur reconnu en science informatique. Lors de nos premières observations participantes, on nous a fait comprendre qu'ici nous n'étions pas considéré comme sachant et expert, et qu'il nous faudrait d'abord apprendre d'eux. Ce que nous avons fait docilement avant toute recherche d'entretien.

de réseaux\* sociaux, billets de blog et forums, que nous avons débuté nos observations participantes. Et « humblement » d'abord. Ce temps fut nécessaire, car, si la nouveauté du début faisait qu'il était facile de repérer des éléments saillants, il fallait encore élaborer le bon vocabulaire, distinguer l'important de l'anecdotique et prendre ses distances par rapport au langage indigène (Amoto 2008). Affinant notre compréhension de ces objets comme des référentiels de leur communauté, nous avons peu à peu trouvé *notre place* dans la communauté : outre notre présence qui devenait récurrente lors d'évènements, l'ouverture et le maintien à l'EHESS de l'un des premiers séminaires dédiés aux CM et nos interventions publiques (médiatiques ou non<sup>47</sup>) finirent par nous situer. Dans sa deuxième année, le séminaire accueillit des acteurs de la communauté, dont « Bitcoin.fr », un média spécialisé francophone, allait assurer la publicisation, et parfois la retransmission vidéo<sup>48</sup>. Petit à petit, nos connaissances du sujet, comme nos problématisations, ont évolué, et ce faisant, nos relations au sein de la communauté. Certains ont commencé à reconnaître nos connaissances « techniques » et à envier notre maîtrise des codes et références académiques – chose qui leur manquait parfois face à *des clients ou des institutionnels*. Les relations enquêteur-enquêtés, établies lors des premiers contacts, allaient se transformer en des relations professionnelles, voire amicales<sup>49</sup>. Avec le premier cercle, nos échanges furent plus informels, les sujets abordés moins limités et, comme pour Duclos, (2014, p. 10), « *ce fut notre manière de parvenir à un dialogue où sans jamais fusionner, nous avons pu nous rapprocher, où sans que l'ethnographe cesse d'avoir le dernier mot, sa voix [peut] s'articuler à celle des personnes rencontrées pour tracer ensemble le chemin de la connaissance* ». C'est ce cheminement – dans les connaissances et les relations – qui nous ôta le statut de « visiteur », particulièrement pour ce qui a trait à la gouvernance et aux crises sur Bitcoin et Ethereum. Cette position relative prise dans le champ, aidée par l'entremise d'un premier cercle, facilita la prise de contact avec des acteurs plus éloignés<sup>50</sup>. Dès lors, dans ces domaines, nous allions prendre part aux controverses indigènes (mais étaient-elles encore indigènes ?), sans rougir – ce que nous nous étions empêché de faire au début - trouvant même parfois le soutien d'acteurs de poids<sup>51</sup>. Pour critiques que soient nos positions, elles étaient considérées comme « plus nuancées » et moins « hors-sol »

---

<sup>47</sup> Nous pensons à notre intervention dans le cadre des « Rendez-vous de l'histoire de Blois », à la rencontre « *Du Bitcoin à la blockchain\* : peut-on avoir confiance dans la monnaie virtuelle ?* », en octobre 2017. De cet événement découlera un passage à l'émission « *La tête au carré* » sur France Inter et l'ouverture d'une période de forte sollicitation médiatique, mais aussi par des acteurs de l'écosystème. Nous continuerons à intervenir sur la thématique des CM lors de différents évènements : des conférences académiques, mais aussi des workshops (Webinar « *Blockchain Governance* », de l'ACPR ; 12/01/2021) ou des conférences plus ou moins grand public (rencontres locales, stage régional de l'Association des Professeurs de Sciences Économiques, etc.).

<sup>48</sup> [https://www.youtube.com/results?search\\_query=rolland+mael](https://www.youtube.com/results?search_query=rolland+mael) [consultation au 04/08/2022].

<sup>49</sup> Nous pensons à Adrian Sauzade, avec qui nous avons réalisé le cours d'*« Introduction aux marchés de cryptomonnaies »*, de 2018 à 2020 à l'ESILV, au sein du cursus ouvert par C. Grunspan. Pour ce cours, nous avons recruté comme chargés de TD des acteurs correspondant à notre premier cercle de rencontres. Depuis, de 2020 à 2023, nous l'avons assuré seul.

<sup>50</sup> P. Noizat, que nous savions avoir des idées arrêtées de type *Bitcoiner maximaliste\** (Lajeune 2021), reconnut avoir discuté de nous avec des membres de la communauté, nous expliquant à notre endroit que : « *la gouvernance c'est le sujet par lequel vous m'avez convaincu de participer, parce que je trouve cela intéressant* » [...] « *vous avez vous-même cité un bug récent dans votre mail pour me contacter. Donc je trouvais cela intéressant, parce que vous avez dès lors la bonne approche* » [...] « *j'étais intéressé de parler avec vous parce que je pense que vous avez une vision un petit peu plus... moins biaisée en tout cas, peut-être sur la chose* » [...] « *j'ai trouvé que votre approche avait un caractère beaucoup plus scientifique que ce que j'avais pu voir* » [P. Noizat Entretien n°24].

<sup>51</sup>. Lors d'un échange Twitter mobilisant une crise spécifique (BIP#0042, cf. Chap. III), un *bitcoiner* français va mettre à l'épreuve nos compétences en ameutant (en « taguant ») d'autres connaissances de la communauté. Il affirme que ledit bogue n'existe pas et que nous avons cru à un poisson d'avril par incompétence, (voir <https://twitter.com/daboloskov/status/1246527105627635713?s=20> et suivant [consultation au 02/08/2022]). Veillant à croiser nos sources, nous avons nous-même « taggé » des développeurs\* Core, pour qu'ils infirment ou confirment l'existence du bogue. L. Dash Jr, P. Wuille et M. Corallo (trois développeurs\* très reconnus) confirmeront la véracité de ce que nous avions précédemment affirmé.

que d'autres. Nous sommes ainsi devenu – un peu malgré nous - l'un des « *rares économistes ami* » avec qui, malgré des oppositions connues, il était plaisant de discuter<sup>52</sup>. Aux garanties internes de réputation s'ajouta une garantie externe, en l'espèce une vigilance particulière sur les questions d'anonymat et de confidentialité. Préserver l'anonymat de nos enquêtés fut dès le départ, suivant les référentiels de ce champ, une question importante. Cela relève aussi d'une déontologie du chercheur qui est aujourd'hui encadrée (Cefai 2009). Quand, en ethnographie, « *confidentialité et anonymat sont (...) les deux faces d'un même problème, celui de garantir aux enquêtés une dissociation entre leur parole – parfois aussi leurs actes – et leur identité, soit par rapport à ceux qui les connaissent, autres enquêtés ou proches (confidentialité), soit par rapport à la masse anonyme des lecteurs potentiels (anonymat) [et] cette intrication des jeux d'anonymat et de confidentialité concerne tous les chercheurs qui travaillent en milieu d'interconnaissance.* » (Zolesio 2011, p. 179 reprenant Béliard et Eidelman) Ainsi, la possibilité d'entretien sous un anonymat strict a toujours été offerte *a priori*, quand les acteurs acceptant de répondre en leur nom conservaient le choix d'exiger que certaines de leurs paroles soient conservées « *en off* », d'où la création d'un acteur fictif [« SuperAnon »], nous permettant d'intégrer ces matériaux tout en protégeant nos sources (cf. Annexe n°IV.4).

Finalement, quelque singulier que soit ce terrain, il partage des similarités avec n'importe quel autre. Une *forge logicielle*\* n'est pas le conseil d'administration d'une banque centrale, mais les principes d'enquête restent inchangés : il s'agit toujours d'analyser des contenus, des relations que ces dernières soient dans le « virtuel » ou dans le « réel » (Pastinelli 2011, p. 37). Les spécificités du phénomène observé ne nous imposent nullement d'abandonner les outils dont disposent l'anthropologie ou l'ethnographie. Nous nous en sommes tenu au triple questionnement maussien de « *qui sont ces gens, que font-ils et qu'en pensent-ils* » tout en réfléchissant « *au rapport à la technique ou au dispositif lui-même, mais ce, toujours en remettant en perspective ce qu'[on] peut observer en ligne avec la manière dont se manifestent et se vivent les mêmes liens dans d'autres contextes, puisque ce sont ces liens qui sont le point de départ et le cœur de la recherche et non pas le dispositif technique* » (*Ibid.*, p. 45 et 47-48). Les particularités de ces infrastructures d'un nouveau genre conduisent à ce que notre travail prenne la forme d'« *une combinaison d'analyse historique et littéraire, d'outils traditionnels comme les entretiens et les observations, d'analyse de systèmes et d'études d'utilisabilité* » (Star 1999, p. 382). Cette combinaison de dispositifs hétérogènes reste à présenter.

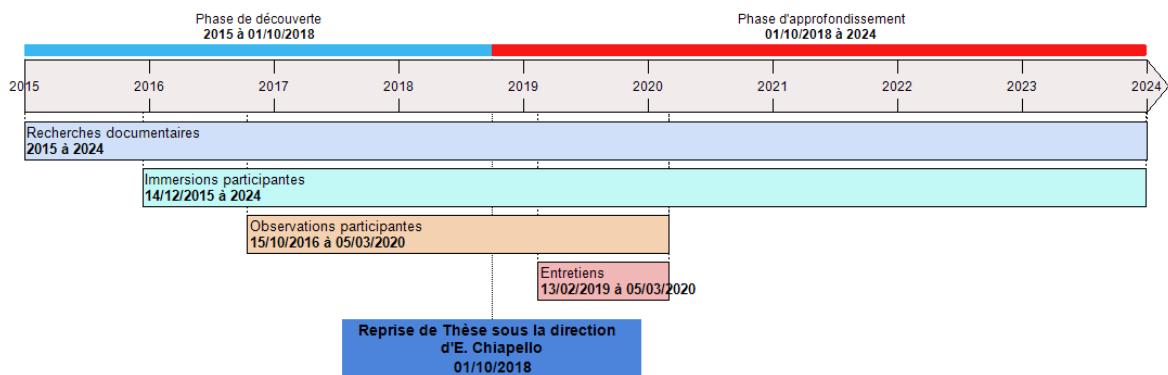
## 2) Stratégie d'accès et matériaux de terrain récoltés

Affronter les difficultés précédentes et étudier les deux faces - en ligne et hors ligne - des CM, nécessita des stratégies différenciées d'accès à nos terrains, sises sur quatre dispositifs distincts (Figure 1). Rétrospectivement, ils ont été mobilisés suivant deux grands temps d'enquête (Tableau 1).

---

<sup>52</sup> Les auteurs de *Bitcoin Métamorphose, De l'or des fous à l'or numérique ?*, J. Favier, B. Huguet et A. Takkal Bataille, nous ont adressé l'ouvrage avec pour autographe de J. Favier : « *Pour l'un de nos rares économistes ami !* », ou celui plus provocant de B. Huguet : « *Maël, toujours une joie d'échanger en espérant participer au débat d'idées libérales ? :-)* »

**Figure 1 : Stratégies d'accès au terrain : quatre dispositifs et deux grands temps**



Source : Rolland Maël

**Tableau 1 : Deux CM, deux crises, documentées suivant quatre dispositifs**

| <b>Bitcoin et crise CVE 2018 #17144 (Cas n°1)</b> |  | <b>Ethereum et crise de “The DAO” (Cas n°2)</b>   |
|---|--|---|
| <b>Matériaux / données collectées</b>             |  | <b>Matériaux / données collectées</b>   |
| <i>Recherches Documentaires</i>                   | Différentes publications : billets de blogs, articles de journaux, échanges sur les réseaux* sociaux (Reddit, Twitter, etc.), log des forges logicielles, etc.<br><br>[n= 253 ; académique n=°34 ; indigène n=°213 ; grise n=°6]   | Différentes publications : billets de blogs, articles de journaux, échanges sur les réseaux* sociaux (Reddit, Twitter, etc.), log des forges logicielles, etc.<br><br>[n= 137 ; académique n=°4 ; indigène n=°132 ; grise n=°1]   |
|   | [Littérature concernant Bitcoin et Ethereum, les protocoles de registre* distribué, les CM, la monnaie, ...<br><br>[n=°271 ; académique n=°164 ; indigène n=°25 ; grise n=°82]]  |   |
|   | Total : 661  |   |
| <i>Immersions participantes</i>                   | Différents types d’interaction en ligne impliquant des activités on chain* et off chain*<br><br>[recensés en annexe n° IV.1]   | Différents types d’interaction en ligne impliquant des activités on chain* et off chain*<br><br>[recensés en annexe n° IV.1]  |
| <i>Observations participantes</i>                 | Participation à des événements de la communauté Bitcoin française ; observations diverses, échanges avec les organisateurs, les conférenciers, les auditeurs, etc.<br><br>[n= 18; durée moy. ~3h, annexe n°IV.2]   | Conférence ETHCC Paris 2017 et 2018 ; Meet up et autres événements AssETH ; observations diverses, échanges avec les organisateurs, les conférenciers, les auditeurs, etc.<br><br>[n= 10 ; durée moy. ~8h ; annexe n° IV.2]   |
|   | Total : 28   |   |
| <i>Entretiens</i>                                 | 16* entretiens : avec prise de notes et enregistrements audio, dont 6 ont été réalisés en face-à-face, 9 via une plateforme en ligne de type Skype, seul le « non-entretien » fut asynchrone.<br><br>[n= 16* ; durée moy. 1h21 min ; synthèse des statuts et rôles couverts en annexe n°IV.3 ; informations biographiques en annexe n° IV.4] | 17* entretiens : avec prise de notes et enregistrements audio (sauf pour 2, prise de notes seulement), dont 9 ont été réalisés en face-à-face et 8 via une plateforme en ligne de type Skype.<br><br>[n= 17* ; durée moy. 1h22 min ; synthèse des statuts et rôles couverts en annexe n° IV.3 ; informations biographiques en annexe n° IV.4] |
|   | Total : 27*  |   |

\* : Le nombre total d’entretiens est de 27 (« non-entretien » inclus et dispositif « superAnon » exclu), certains interviewés (6 sur l’ensemble) portent la double casquette de *bitcoiner* et d’*etheriste* et sont ainsi comptabilisés dans chacune des colonnes.

Source : Rolland Maël

Le mouvement esquissé d'un décentrement de notre démarche théorique originelle, liée à l'institutionnalisme monétaire francophone, vers l'empirie d'Ostrom, de l'ethnographie économique et finalement des STS, a accompagné notre enquête. Ce sont nos recherches préliminaires, très théoriques, reposant sur des recherches documentaires d'ordre général, qui allaient nous convaincre de la nécessité d'aller au-delà, au plus près du guichet : nous confronter aux protocoles eux-mêmes, aux couches socio-techniques qui permettent d'y accéder et à leurs acteurs (humains ou non). Le premier temps d'enquête fut une phase de découverte et d'acclimatation (en bleu). Nous y avons mobilisé majoritairement deux types de dispositifs ethnographiques plutôt « froids » (en bleu et vert) : des recherches documentaires d'abord, des immersions participantes ensuite. Froids au sens où, par leurs voies d'observation passive et asynchrone, ils nous offraient une mise à distance et le choix du degré de notre engagement, qui, faible au départ, allait pouvoir s'affermir par la suite. Au commencement, nous faisions face à une forêt vierge. Aucun chemin apparent. Si notre cadre théorique était la boussole, encore nous fallait-il, pour qu'elle serve, disposer d'une carte et de coordonnées, aussi imprécises soient-elles. Nous avons donc fait feu de tout bois et n'avons limité nos recherches à aucune direction précise. Cette phase nous dota d'une vision d'ensemble qui allait nous permettre de circonscrire nos cas d'étude et d'entamer des recherches sur des éléments plus spécifiques via la réalisation de nos premières observations participantes. En outre, elle nous permit de comprendre qu'un travail empirique qualitatif, de type ethnographique, allait contribuer à nourrir notre recherche. Cette première phase nous a fourni une représentation préliminaire du champ, des multiples arrangements socio-techniques et de ses acteurs, comme de leurs agencements spécifiques. Cette représentation nous a permis d'aiguiller notre recherche quant au ciblage des personnes, des matériaux et informations encore nécessaires, et d'affiner notre méthodologie d'enquête, d'évaluer la pertinence de notre approche et de notre sujet, comme de poser les premières hypothèses. Notre deuxième temps d'enquête – la phase d'approfondissement (en rouge) - débute en octobre 2018, et renvoie à notre reprise de thèse sous la direction d'E. Chiapello. À la suite de l'établissement du périmètre de nos cas d'étude, notre travail d'enquête allait se faire plus systématique, ce qui nous a conduit à mobiliser des dispositifs plus « chauds » (en orange et rouge). La phase d'acclimatation passée, nous nous sommes rapproché physiquement de nos acteurs. D'abord, nos observations participantes ont été plus spécifiquement dirigées à l'endroit des crises que nous avions choisi d'étudier. Ensuite, nous avons pu réaliser nos entretiens puisque la phase d'enquête précédente avait permis de dégager les grands contours des événements que nous allions analyser et de cibler les zones d'ombre qu'il fallait, lors de cette seconde phase, documenter. Les données récoltées, confrontées à nos représentations liminaires, nous ont permis finalement d'affiner les contours de ces objets et de leurs communautés : les couches et sous-systèmes structurant les CM, les rôles et les statuts différenciés des membres, les arrangements socio-techniques encadrant leurs relations.

## **La face « en ligne » des CM : d'une entrée par voie de recherche documentaire au saut de l'« immersion participante »**

« *Creuser au fond du terrier* »<sup>53</sup> : les recherches documentaires, une source essentielle de connaissance de ce champ

Les recherches exploratoires ont d'abord été menées grâce à une recherche documentaire mobilisant des sources et matériaux hétérogènes : différents types de littérature (académique, grise et indigène), mais aussi différents types de documents et données accessibles en ligne (données *on chain*\*, débats sur les forums, échanges sur les forges logicielles relatifs à des optimisations, etc.).

Au niveau de la littérature *académique*, et bien que des travaux soient issus de différentes disciplines, nous avons privilégié les textes s'inscrivant en économie et en sociologie, sans pour autant exclure d'autres disciplines. La plupart des travaux de ce corpus a déjà été évoquée précédemment. Elle fut complétée par de la littérature *grise* constituée par des rapports, notes ou prises de position publiés par des institutions, comme des Banques centrales ou des administrations. Dans ces deux premières catégories, nous avons rangé des prises de parole hybrides d'experts (« Prix Nobel » d'économie, ministre, présidents de banque centrale, ne relevant pas directement de leur champ propre mais plutôt du champ médiatique, comme les articles et tribunes dans les journaux - statut dénoté par l'absence de pagination, cette mention étant réservée aux citations tirées de travaux formels, cf. précautions d'écriture et informations préliminaires).

Lors de notre entrée sur le terrain, si les deux premiers corpus (littérature académique et grise) étaient maigres, celui constitué par la littérature et les matériaux *indigènes* était pléthorique. Une grande part du matériau récolté est tirée de ce corpus, constitué d'objets variés émanant d'acteurs divers. Il provient de sources hébergées sur Internet, souvent produites par les acteurs eux-mêmes : registre\* transactionnel, billets de blogs, discussions de forums, média plus ou moins grand public, etc. Nous en avons tiré des données à la fois qualitatives et quantitatives. Les données qualitatives se distinguent selon les acteurs qui les fournissent (développeurs\*, journalistes, billet de blog de personnalités plus ou moins reconnues, etc.), les informations transmises (sources primaires ou secondaires, niveau de technicité, langage, etc.), l'audience ciblée, comme les canaux/réseaux\* mobilisés dans leur publication. Certains matériaux sont d'ordre technique et correspondent directement aux traces des discussions et des propositions techniques réalisées par les développeurs\* via le répertoire de leur *forge logicielle*\*, qui est l'outil de la production publique du code logiciel. Ces discussions visent à l'évaluation des problèmes posés, à la production de correctifs (savoir-faire), mais aussi à la diffusion et à la traduction de ces informations pour l'ensemble de la communauté (faire-savoir). D'autres correspondent à des matériaux à visée plus générale et à une audience plus large, comme c'est le cas pour les textes de journaux spécialisés en ligne, les billets de blogs, les rapports de divulgation de la faille diffusés par l'équipe Bitcoin Core, les échanges communautaires sur différents réseaux\* sociaux, etc. Trois jeux de données quantitatives ont également été constitués : l'un relatif à l'écosystème dans son ensemble (Annexe n°I) et les deux autres dédiés à Bitcoin (Annexe n°II) et à Ethereum (Annexe n°III). Ces données, servant aux trois chapitres de la thèse, sont renvoyées en Annexes afin d'éviter redondance et

---

<sup>53</sup> Référence à l'expression « *Down the rabbit hole* », métaphore d'une entrée dans l'inconnu, tirée de ce qui arrive à Alice au Pays des Merveilles. Cette expression est souvent usitée dans le champ des CM, faisant écho à l'éthos individualiste voulant qu'il faille vérifier par soi-même et non faire confiance (« *Don't trust verify* »). Encore faut-il un savoir, reposant sur des recherches propres, seul porteur de l'autonomie nécessaire, l'expression « DYOR » pour « *Do Your Own Research* » renvoyant à cette injonction : quantité de ressources sont accessibles, à qui veut bien aller creuser dans le cyberspace.

surcharge, et d'en faciliter l'accès (glossaire et annexes sont pensés comme un livret détachable à cet effet).

Face à cette quantité d'informations, il nous a fallu réaliser un tri pour ne pas être noyé sous la masse. Notre capacité d'accès était un critère simple, et notre recherche de ressources et données s'est restreinte à celles pour nous accessibles. Le rôle des matériaux documentaires a évolué, mais ils sont restés essentiels d'un bout à l'autre de notre enquête, permettant notamment sur la fin des recherches plus pointues. Ces recherches documentaires nous permirent de mieux comprendre Bitcoin et Ethereum théoriquement et d'envisager de nous y confronter plus pratiquement.

### *S'approcher des acteurs non humains : des immersions participantes nombreuses et « fructueuses »*

Cette première phase de recherche documentaire nous incita à aller plus loin. En raison d'un premier contact avec les CM en 2015, nous avons commencé, avec un membre du laboratoire CEMI (Assen Slim), la rédaction d'un papier préparatoire. Notre connaissance de notre objet n'était forte que de nos premières lectures et de nos connaissances en théorie monétaire, ce qu'un intervenant prit d'ailleurs soin de souligner lors de la présentation dudit papier, en questionnant notre éventuel usage Bitcoin. Notre réponse négative fit apparaître un problème important : nous glosions sur un objet monétaire à l'architecture novatrice et pointue sans avoir fait l'effort pratique d'en expérimenter l'usage. Le soir même, nous nous confrontions empiriquement à ce nouveau medium, ouvrant l'ère d'une socialisation monétaire nouvelle.

Le point d'entrée de nos expériences immersives (une liste non exhaustive de nos immersions participantes se trouve en annexe n°IV.1) fut l'acquisition et l'utilisation de nos premières UCN\* BTC. Étant donné que nous étions encore réticent à acheter du bitcoin en euro *via* une bourse d'échange, ces premières UCN\* furent gagnées par notre « travail », *via* des sites de « faucet », en contrepartie de la réalisation de micro-tâches (visualisation de publicité, jeux divers, etc.). Intéressé au sujet par Bitcoin, nous fûmes plongé, *via* ces services tiers, dans un univers composé d'une pluralité de CM et d'arrangements socio-techniques permettant d'y accéder comme d'en user. À mesure que ce travail fastidieux nous permettait de constituer un premier portefeuille\* plus que modeste, notre réticence première s'effaça. Aller plus loin dans l'expérience nous fit prendre les casquettes du *trader*, de l'*investisseur*, du *hasher* et nous procurer des CM contre des euros *via* l'intermédiaire de différents services de passerelle\*. Qu'ils offrent de la « location » de puissance de calcul dédiée permettant le *traitement des transactions\** (et de percevoir les récompenses afférentes) ou de réaliser du *trading* sur des places d'échange, ces services induisaient des actions *off chain\**, hors des frontières formelles du *protocole de registre\** *distribué\**. L'importance prise par ces intermédiaires financiers que sont les *passerelles\**, voies de passage quasi-obligé de tout usager (en entrée et sortie), apparaissait pratiquement. Nous frayer un chemin dans cette multiplicité procédurale et ses complexités nous conduit à des activités et pratiques disparates. Il fallut nous tourner vers les lieux spécifiques – de production et de discussion – de ces nouveaux savoirs et en intérioriser les normes et valeurs. À cette occasion, nous allions rejoindre pour la première fois les réseaux\* sociaux (Twitter, Reddit, etc.) et y découvrir les modalités particulières de communication y ayant cours. Nous allions pouvoir assister, voire prendre part, à un grand nombre d'événements et de polémiques : le « *scaling debate* » sur Bitcoin se dénouera ainsi bruyamment sous nos yeux en 2017 ; le déploiement d'Ethereum que nous avions rejoint dans les premiers temps de son lancement ; l'attaque du projet « The DAO » et le *Hard Fork\** retentissant qu'il conduisit à mener – pris comme cas d'étude de cette thèse - alors que nous avions nous-même pris part à sa campagne de financement record ; les premiers NFT sur Bitcoin (participation à la communauté *Rare Pepe Card*) ; le phénomène exubérant des ventes publiques de type *Initial Coin Offering* (ICO) qui culmina en 2017 et attira l'attention tant des investisseurs que des médias et des régulateurs ;

l'émergence de la DEFI sur Ethereum, le « farming », les « airdrop », etc. Si, dès le départ, il n'était pas pensable pour nous qu'un système monétaire, quel que soit son caractère novateur, soit dépourvu d'espaces de gouvernance, de confiance, donc de structure de pouvoir et de conflit, nos expériences pratiques tendaient à confirmer ces intuitions.

Méthodologiquement, si c'est la « *duplicité* » de nos terrains – en ligne et hors ligne – qui nous a conduit à effectuer des « *immersions participantes* » (Amato, 2008), cette forme a des implications déontologiques (politique de divulgation des possessions, conflit d'intérêts, etc.) qui font débat (DuPont 2021). Pour les uns, ne pas posséder d'UCN\* est une garantie d'objectivité<sup>54</sup> et parler de ce champ implique de lui être extérieur. Il est vrai qu'accéder indirectement à des connaissances pratiques était possible au travers des observations participantes. Nous limiter à accompagner et dialoguer avec des usagers pouvait sembler suffisant. Mais, comme d'autres<sup>55</sup>, il nous est apparu nécessaire de connaître notre terrain pratiquement, tout en faisant acte de réflexivité. Puisqu'aux fins de recherche premières de nos achats s'en sont ajoutées d'autres, plus personnelles (comme 52% des répondants de Dupont 2021, déclarant « *avoir acheté des jetons à des fins autres que la recherche* »), nous divulguerons nos conflits d'intérêts potentiels à la fin de cette introduction. Pour nous, à la manière d'Amato (2008) intéressé aux jeux multijoueurs en ligne, seule une pratique effective nous permit de découvrir et d'intérioriser les « *compétences impliquées* »<sup>56</sup> inhérentes à notre champ. Ce dispositif fit ses preuves dans l'obtention et la maîtrise d'un socle de savoirs, savoir-faire et faire-savoir minimum. En outre, cette immersion permettait de ne pas altérer le « *moment initiatique* » « *du premier plongeon* », cette mise en condition initiale et la « *fascination originelle, cette emprise* » décrites par les acteurs (*Ibid.*). Bien qu'elles ne prétendent pas à être ludiques comme les jeux vidéo, ces expériences le sont en partie, et il est indéniable que les nôtres ont pris cette dimension<sup>57</sup>. La fascination suscitée par la première transaction\* BTC envoyée, qui nous avait été décrite, fut réelle pour nous aussi. Cela liait anxiété et satisfaction. Anxiété d'avoir commis une erreur dans la procédure, faisant perdre irrémédiablement les UCN\* envoyées. Satisfaction de pouvoir réaliser une transaction\* en pair-à-pair sans banque et système de paiement hiérarchique et d'en suivre le traitement en temps réel – les *confirmations*\* successives jusqu'à la *finalité du paiement*\* – via un *explorateur de registre*\* accessible en ligne. Ainsi, le choix de l'immersion n'était « *pas seulement une posture [...], un choix méthodologique ou épistémologique, mais une condition inévitable d'accès au terrain* » (Berry, 2012).

Cette première phase d'enquête, faite de nos recherches documentaires et premières « *immersions participantes* », nous dota d'une représentation des ensembles relationnels en jeu, de leurs supports et des espaces pertinents de leurs intrications. Nos expérimentations confirmaient la structuration d'un champ autour d'une pluralité d'acteurs, d'activités et de secteurs économiques en développement ; d'arrangements mêlant des logiques *hors-protocole*\* et *au sein du protocole*\* ; comme des contraintes inhérentes à l'usage (téléchargement d'un *portefeuille*\* et sécurisation de la clef d'*authentification cryptographique*\*, etc.). Cette phase nous fit maîtriser plus que les seules

---

<sup>54</sup> Comme Angela Walch, qui « *ne possède pas de crypto-monnaies* [considérant] que cela compromettrait [s]a capacité à être relative objective dans [s]es recherches » (McCormack et Walch 2019).

<sup>55</sup> Nous pensons à DuPont (2018) qui a participé, comme nous, à l'ICO de « The DAO ».

<sup>56</sup> Par compétence « imbriquée », on entend les compétences d'un membre de groupe, couvrant « *sa capacité opérationnelle, [...] les façons partagées de penser et d'agir; ainsi que le sens commun collectif singulier qu'il connaît et adopte.* » (Amato 2008)

<sup>57</sup> Cette ludicité de l'argent n'est pas étrangère à la socialisation monétaire couramment à l'œuvre dans nos sociétés : donner des pièces à des enfants pour qu'ils paient les courses eux-mêmes, jouer à la marchande, avoir de l'argent de poche, etc., sont autant de voies d'apprentissage et d'intériorisation, plus ou moins manifestes, de rapports sociaux à l'argent.

pratiques et conventions ayant cours *au sein du protocole*\* et permit d'envisager plus sereinement la réalisation, dans le monde réel, d'observations participantes et d'entretiens.

### L'envers « hors ligne » : au contact des acteurs par observations et entretiens

*Observations participantes d'évènement hors ligne : premiers contacts en présence d'acteurs humains*

La dénomination « immersion participante », en plus de partager avec celle de l’« observation participante » l’emphase explicite sur la dimension interactive du dispositif, permet de circonscrire ce qui relève, pour l'une, de pratiques inscrites dans le « cyberspace » et, pour l'autre, de pratiques inscrites dans le « réel » (Amato, 2008). En parallèle des immersions dans ces nouveaux mondes numériques – médiatisées simplement par notre ordinateur connecté à Internet –, nous nous sommes rapproché dans le « réel » des personnes et organisations parisienne (associations, groupements organisant des rendez-vous de type *meetup*, etc.) intervenant dans ce champ.

Dans le « réel », nous avons réalisé 27 observations (cf. recension en Annexe n°2) pour un temps moyen passé de 4 heures 30. Toutes relèvent d'événements collectifs communautaires (17 concernent la communauté Bitcoin, 10 la communauté Ethereum. Ces observations couvrent : des rendez-vous dits « sociaux » (« *Social meet up Bitcoin* ») récurrents qui servent aux acteurs à échanger de manière informelle; des conférences de présentation de projets, d'ouvrages où les échanges sont plus formels et la portée plus restreinte (enjeux techniques, économiques et financiers, etc.) ; des ateliers pratiques (« créer mon premier *smart contract*\* sur Ethereum », par l'Asseth) ; des conférences internationales (conférences « *Breaking Bitcoin* » à Paris et Amsterdam, ou ETHCC à Paris). Nous avons privilégié les événements proches géographiquement en raison des contraintes d'accès. Nous avons été présent aux *Meetup* mensuels de la communauté Bitcoin, nous nous sommes inscrit comme membre de l'association Ethereum France (ex « Asseth ») dès sa fondation, ainsi que comme membre du « Cercle du Coin ». Nous avons également profité de notre séminaire à l'EHESS pour y faire intervenir des praticiens de la communauté. Ces observations nous firent rencontrer nombre d'acteurs de premier plan de la scène des CM en France et, plus généralement, être au contact d'une diversité de technologies, d'usages et de communautés. Cette insertion dans le « réseau\* crypto » parisien nous conduisit à assister à un ou plusieurs événements publics internationaux sur Bitcoin et Ethereum, comme à établir des contacts pour nos entretiens.

### *Entretiens*

Après quelques entretiens, très ouverts et sur des questions génériques, réalisés dans un cercle de connaissances proches, nous avons approché des acteurs plus directement en lien avec les crises étudiées pour des entretiens plus directifs. Nous dénombrons 27 entretiens (cf. liste exhaustive en annexe n°IV.4) : 26 entretiens effectivement réalisés et 1 « non-entretien », ajouté du fait du caractère exemplaire de sa « non-réalisation ». N'est pas compté le personnage fictionnel SuperAnon qui tient le rôle de paravent protégeant l'anonymat et la confidentialité de paroles d'acteurs bien réels, tout en offrant la possibilité d'une restitution d'un ensemble d'avis jugés controversés qu'il nous a été explicitement demandé de retranscrire en *off*. À l'exception d'une information livrée qui ne peut être utilisée<sup>58</sup>, les différents acteurs ont accepté que leurs paroles soient portées par ce personnage. Pour ces entretiens, nous avons privilégié les rencontres physiques

---

<sup>58</sup> Le contenu d'un échange nous a été interdit de tout usage, car les informations données relevaient d'un échange bilatéral rendant impossible toute dissociation. Pour ce que l'on peut en dire, cela démontrait que certaines décisions prises par des acteurs dépendent parfois d'avis reçus de leurs investisseurs importants.

chaque fois que possible. Dans les autres cas, les échanges furent synchrones par dispositif de vidéo-conférence (à l'exception du « non-entretien », asynchrone).

Les 27 entretiens réalisés nous ont permis de rencontrer des acteurs des communautés Bitcoin et Ethereum plus ou moins directement impliqués dans nos deux cas d'étude. Notre démarche est qualitative, et l'échantillon d'acteurs réuni n'a pas en soi à être représentatif. Nous avons néanmoins essayé que soit représentée la plupart des statuts et rôles communautaires clefs (cf. Annexes n°IV.3 & IV.4) : en ce qui concerne les « mineurs », nous avons pu échanger avec des « hasheurs » professionnels (Entretiens n°17 et n°18) et amateurs (entretiens n°28 et n°4) ; pour les « développeurs\* », nous avons échangé avec un « core développeur » Bitcoin (Entretien n°15), et rencontré des acteurs apparentés au groupe des « core développeurs\* » et/ou « chercheurs » travaillant sur la couche protocolaire et sur les logiciels clients pour la fondation Ethereum (Entretiens n°9, n°12 ; n°13, n°26) ; concernant la « couche applicative », nos entretiens touchent à différents statuts (développeur ou non) et segments de la catégorie « autres services » (Entretiens n°1, n°2, n°3, n°4, n°5, n°7, n°10, n°16, n°22, n°23, n°25) ; nous avons aussi couvert le segment des « bourses d'échange » (Entretiens n°11 et n°24), celui des portefeuilles\* et de la sécurisation des crypto-actifs\* (Entretiens n°6 et n°8), celui des « services d'analyse de données » (Entretien n°20) et enfin le segment « média/événementiel » et « conseils, formation, enseignements et recherches » (Entretiens n°14, n°21, n°19, n°23). La majorité des interviewés reconnaît porter - ou avoir porté - plusieurs « casquettes », comme celles d'opérateurs de « nœuds\* complets » (tous, que ce soit personnellement ou *via* leur entreprise), voire de nœuds\* de minage (« hasheurs », sur Bitcoin mais pas seulement) et d'« utilisateurs finaux » (« utilisateurs » et « investisseurs/traders »).

## D. OBJECTIFS, APPORTS ET ORGANISATION GÉNÉRALE DE LA THÈSE

À la question de savoir si les CM sont des monnaies ayant réussi à s'autonomiser du politique, nous soutenons que, bien qu'elles soient monnaies, l'idéologie qui les entoure est contrefactuelle : les CM, notamment Bitcoin, sont, comme toute monnaie, des artefacts socio-politiques conflictuels qui, au-delà d'une pure gouvernance technique (espace de la règle) relèvent de compromis politiques toujours en (re)construction (espace de la discréption).

Cette thèse générale est structurée autour de problématiques spécifiques répondant aux prétentions libérales technicistes des *coiners\**, rappelées en introduction de notre propos. Ces prétentions prennent la forme d'un syllogisme stipulant que (i) puisque la technique est autonome et neutre vis-à-vis du monde social et que (ii) les CM sont des monnaies purement techniques, alors (iii) elles sont immunisées de la gouvernance humaine et de ses intérêts socio-politiques, ce qui en fait (iv) de « meilleures » monnaies que les formes monétaires antérieures, en particulier que les « fiat monnaies » nationales. Chaque prémissse de ce syllogisme recouvre des problématiques singulières nécessitant un travail de déconstruction.

Nous opposons aux deux premières que la neutralité technique n'est qu'une illusion, en raison de la normativité inhérente à tout objet socio-technique. Avec une CM, architecture et code protocolaire ne sont pas neutres, non seulement parce qu'ils incorporent les vues socio-politiques de leurs concepteurs, mais aussi parce que ces vues idéelles ne font pas un contenu matériel (spécifications protocolaires et logiciel client). Un protocole nu ne fait pas monnaie, laquelle nécessite une infrastructure : des usages, d'autres arrangements socio-techniques pour s'y connecter, une maintenance et des évolutions qui en renégocient formes, contenus et normativité. Cette première étape de la démystification de la neutralité technique des CM permettra d'aborder les prémisses restantes, touchant à leurs prétentions proprement monétaires.

Nous soutenons que les CM font monnaie, à l'aune de notre institutionnalisme monétaire ainsi que de leur usage en compte et en paiement. De notre point de vue, il est impossible d'affirmer en surplomb la supériorité d'une monnaie sur une autre, puisque leur qualité « bonne » ou « mauvaise » relève du jugement des membres de leurs communautés de paiement et est sans cesse rediscutée au gré de la survenue de controverses irréductiblement politiques. Au niveau des acteurs, ces controverses et jugements exprimés sur les propriétés désirées de leur CM dessinent une structure de gouvernance, et non son absence. Pour l'interroger, nous partirons des crises des CM, ou plutôt de leur fabrique par les *coiners*\*. Les étiquettes, catégories, dispositifs de régulation et de contrôle des modifications protocolaires, les moyens de contention, les arènes de débats et les acteurs mis à jour sont les marques d'une gouvernance de crise à deux faces, différentes et complémentaires : une forme routinière *de huis clos*, où prime *a priori* un consensus local entre des acteurs hautement techniciens, ainsi qu'une absence de dissensus global et une forme plus exceptionnelle *publique et ouverte*, où le consensus recherché est d'emblée global en raison de l'existence d'un dissensus réel ou supposé. Bien que la face routinière apparaisse technocratique, l'activité de maintenance des codes protocolaires par un collège de spécialistes s'avère hautement encadrée, ce qui permet d'assurer responsabilité, contrôle et expression de dissensus. C'est l'apparition du dissensus qui conduit la gouvernance à adopter une forme opposée, ouverte et publique, caractérisée par une mobilisation large des parties prenantes communautaires. Ces parties prenantes (dont le périmètre est soumis à discussion) doivent participer aux débats et aux décisions dans une recherche de légitimité communautaire qui prend appui sur des arènes de discussion et des dispositifs de mesure du consensus variés.

Cette thèse vise deux types de contributions. La première contribution est empirique puisque cette thèse documente, cartographie et analyse l'écosystème et la gouvernance, de Bitcoin et d'Ethereum de leurs origines à 2020. Elle repose sur un travail documentaire, d'immersion participante, d'enquête, d'observation participante, qui a permis de documenter et de cartographier la gouvernance des CM étudiées, et d'ébaucher des catégories et concepts dans un contexte académique où les données sont encore parcellaires. La seconde contribution est plus théorique, puisque cette thèse entend également fournir des éléments de caractérisation des CM et des acteurs participant de leur gouvernance. Elle souligne notamment que l'existence de ces nouvelles formes de monnaies ne peut laisser indemnes les représentations monétaires dominantes que partagent d'ailleurs en partie les *coiners*\* et leurs détracteurs. Notre travail s'adresse d'abord aux acteurs académiques s'intéressant au champ monétaire, mais aussi à l'ensemble des praticiens amenés à traiter de questions relatives aux CM, monnaies digitales\* et crypto-actifs\* (qui comprend tous ceux travaillant dans des administrations publiques ou internationales (administration fiscale, ministères, banques centrales, etc.) ou dans le secteur privé (banque, finance, assurance). Enfin, les acteurs de la société civile (ONG, associations, etc.), comme toutes les personnes curieuses des enjeux économiques, sociaux et politiques de ces technologies, y trouveront matière à réflexion.

La thèse est organisée en trois chapitres que nous décrivons maintenant.

**Le premier chapitre** présente Bitcoin et Ethereum et questionne la neutralité et l'autonomie prétendument « techniques » de leur protocole. À contre-pied du « technologisme » d'une partie de la littérature qui insiste sur leur seul protocole, nous les replacerons dans leur contexte socio-historique. Nous montrons que les CM ne sont pas de pures réalisations techniques, neutres, autonomes et stabilisées, mais des infrastructures négociées et hybrides : la technique et le monde social s'influencent mutuellement dans un va-et-vient politique (Akrich 1989 ; Star 1999). Ces

protocoles intègrent des *a priori* sociaux faits d'inspirations théorico-pratiques hétérogènes. Et un protocole seul ne fait pas monnaie : ce statut dépend de son interaction avec des utilisateurs, *via* un développement infrastructurel, principalement hors chaîne, permettant la création de circuits et de raccordements, et l'établissement d'espaces de conversion (portefeuilles\* et passerelles\*). Ce processus est complexe, multi-acteur et multi-niveau, et permet aux CM d'évoluer, de s'adapter, d'étendre leurs usages et de s'intégrer au système monétaire et financier, leur conférant, par monétisation, une valeur d'échange.

Nous examinerons ainsi la conception et les agencements socio-techniques de Bitcoin, en soulignant que chacun des choix architecturaux effectués (en particulier le consensus fondé en PoW\*) est irréductiblement hybride, négocié, reflétant les inspirations et contraintes du projet de Nakamoto, notamment la décentralisation. En décalant l'analyse vers les utilisateurs et usages, Bitcoin apparaîtra comme une infrastructure sans couture, réductible ni aux desseins de son concepteur, ni à ses frontières protocolaires, puisqu'il est toujours renégocié par les acteurs (réintermédiation de certains processus et activités, disputes autour d'évolutions protocolaires supprimant des usages auparavant possibles considérés comme illégitimes, etc.). De même, la présentation d'Ethereum mettra en lumière ses aspects normatifs et son développement infrastructurel propre, influencé par Bitcoin, mais enrichi de ses critiques sur ce qui est perçu comme ses rigidités protocolaires et infrastructurelles. Cette volonté d'émancipation vis-à-vis de Bitcoin explique des arrangements différents, démontrant à nouveau que les CM ne peuvent se prévaloir d'une quelconque neutralité technique.

Le **deuxième chapitre** présentera notre contribution à la controverse entourant le statut monétaire des CM. Nous examinerons les critiques existantes des CM, en les replaçant dans leur contexte théorique et épistémologique. Les CM représentent une épreuve d'explicitation de la monnaie pour les approches monétaires dominantes fondant ces critiques : les CM, comme d'autres innovations monétaires avant elles, mettent en crise la définition que leurs détracteurs ont de la monnaie. Contre l'avis de la majorité des économistes et praticiens de ce domaine (banquiers et banquiers centraux), nous affirmerons le caractère monétaire des CM depuis une approche institutionnaliste et ethnographique. Nous montrerons que, dans leurs usages, les CM possèdent les caractéristiques minimales de toute monnaie (elles se rapportent à la dette, à la confiance et à la souveraineté), et s'intègrent facilement au champ de la monnaie, en tant que monnaies parallèles communautaires, dont elles représentent une forme inédite.

Nous proposerons une recension des différentes critiques formulées à l'encontre de Bitcoin et des CM, distinguant deux familles de fondations théoriques : l'approche instrumentale et l'approche a nominaliste/chartaliste. Nous montrerons que, du point de vue d'un institutionnalisme monétaire non étatique, intéressé aux usages, ni les fonctions canoniques de la monnaie, ni l'exclusivité étatique ne peuvent reléguer les CM hors du champ monétaire : leur usage en compte et en paiement sont indéniables, quand leurs UCN\* sont les seules à pouvoir exprimer et régler les frais d'usage de leurs protocoles. Mais si Bitcoin et Ethereum sont pour nous monnaie, ce n'est ni dans le sens retenu par la majorité des économistes et des praticiens, ni dans celui des *coiners*\* : elles sont monnaies non pas en remplacement des monnaies nationales, mais en complément de celles-ci, avec des usages de niche *malgré* et même *à cause* des imperfections rédhibitoires pointées par leurs critiques (forte volatilité, usage pour des activités illégales). Finalement, contrairement à ce qu'en pensent les *coiners*\* et leurs contemporains, la singularité des CM dans le champ monétaire ne tient pas à l'absence de gouvernance humaine, mais à sa présence. Les CM disposent d'une gouvernance duale et polycentrique qui les place dans une nouvelle catégorie de monnaie, distincte des monnaies privées ou publiques existantes. Adoptant un nominalisme campé dans la thèse de la discréption, il nous sera impossible de conclure sur la qualité « bonne » ou « mauvaise » de Bitcoin ou

d’Ethereum, puisque cette qualité s’apprécie au regard de leur capacité à se reproduire légitimement aux yeux des acteurs, laquelle dépend de la qualité de cette gouvernance polycentrique qui doit assurer la définition, la réalisation d’objectifs collectifs, ainsi que la gestion des conflits que ce chapitre aura introduits.

Le **troisième chapitre** analysera la gouvernance de Bitcoin et d’Ethereum, à travers leurs crises, et principalement la faille « Bitcoin Core CVE 2018 #17144 » pour Bitcoin et le *Hard Fork*\* d’Ethereum consécutif à l’attaque de « The DAO » pour Ethereum. L’enquête sur les crises (de la mise en crise à la remise en ordre) fera apparaître les dimensions normative et politique à la fois de la gouvernance *par*, mais aussi de la gouvernance *sur* l’infrastructure, ainsi que son polycentrisme. Différents types de crises interrogent le fonctionnement normal du système de paiement, reflétant l’existence d’une politique de crise dont les marques prennent la forme de nomenclatures, d’échelles de gravité, de procédures de découverte et de divulgation, de modalités de réactions, d’acteurs et procédures impliqués, d’arènes d’action, de discussions et de dispositifs de mesure du consensus communautaire. Nous identifierons deux familles de crises suivant l’adéquation entre ce que permettent les codes et ce que la communauté attend d’eux - *les crises de vulnérabilité* et celles *d’évolution* -, ainsi que deux formes polaires que peut revêtir cette gouvernance. La gouvernance de crise *de huis clos* semble restreinte à un collège d’experts techniciens et celle *publique et ouverte*, par nature conflictuelle, mobilise l’ensemble des parties prenantes de la communauté. Qu’importe la face de la gouvernance, le consensus du protocole apparaît soumis *in fine* à un consensus communautaire sur ses propriétés désirées, associant plus ou moins directement et largement les membres de la communauté et leurs intérêts différents.

À partir du cas de la crise Bitcoin CVE 2018, nous montrerons qu’une structure de gouvernance *sur* l’infrastructure prend le relais quand la gouvernance *par* est mise en défaut. C’est principalement la production et les coulisses, face routinière d’une gouvernance confinée, qu’il nous a été permis de documenter et d’analyser dans ce cas. Dans sa forme de *huis clos*, la gouvernance *sur* le protocole éclaire les dimensions infra-politiques, fondées en confiance et délégation, de la maintenance des codes de l’implémentation logicielle hégémonique Bitcoin Core, et la centralité qu’y prend le groupe restreint des « core devs », sans pour autant être technocratique. Si la remise en ordre fut réalisée secrètement et sans publicité, selon un consensus local entre des acteurs en réseau\* (« core devs » et opérateurs de « pool de minage »), des régulations et contrôles communautaires existent. Du fait du caractère critique des activités entourant les codes protocolaires et des pouvoirs qu’ont sur eux certains membres de la communauté, la gouvernance offre aux usagers certaines garanties contre les changements de règles discrétionnaires non consensuels. Analyser la gouvernance *sur* l’infrastructure d’une CM ne peut cependant s’arrêter à la face routinière de la gouvernance de crise puisque, sans dissensus franc, le consensus entourant les modifications de codes reste essentiellement local, tacite et sans ambages. Ce n’est pas le cas des crises *d’évolution*, comme dans le cas du *Hard Fork*\* consécutif à l’attaque de « The DAO » pour la communauté Ethereum, qui conduisent inéluctablement à des débats, voire des conflits résolus, eux, sur une « grande scène », en public et à grand bruit. C’est lors de l’expression rare et intermittente de cette seconde face de la gouvernance que l’ensemble des composantes communautaires (utilisateurs finaux, bourses d’échange, opérateurs de services, etc.) se pare des costumes des contre-pouvoirs et que l’ensemble des mécanismes communautaires visant à assurer la production de consensus (et d’expression du dissensus) se trouve mobilisé.

## E. DÉCLARATION D'INTÉRÊTS

Nous détenons au 05 septembre 2024 un portefeuille\* en CM et crypto-actifs\* dont la valeur et la composition changent fréquemment (hors *jeton non fongible* ou « *Non Fungible Token* »<sup>59</sup>). Sa valeur actuelle est comprise entre 150 000 et 190 000 euros ; pour sa composition plus de 50% du portefeuille\* relèvent d'UCN\* Ether (~31%) et Bitcoin (~20%), l'autre moitié recouvre plus de 30 autres différentes CM et crypto-actifs\*, dont une seule a un poids supérieur à 5% (SNX ~10% dans le portefeuille\* total). Cette multiplicité renvoie à la dynamique d'expérimentation première qui est toujours restée présente, même si s'y est mêlée dans un deuxième temps une dynamique d'investissement plus personnelle.

Nos activités économiques rémunérées dans ce champ ne recouvrent que des activités d'enseignement et nous sommes rémunérés en euros.

---

<sup>59</sup> Les NFT collectionnés n'ont pas été intégrés du fait de leur valorisation plus problématique : faible liquidité, actifs de niche, forte concentration : une évaluation grossière, pour ce qu'elle « vaut », voit cette collection avoir une valeur de vente comprise entre 10 000 et 30 000 euros. Elle fut majoritairement constituée lors de nos premières immersions participantes : nos activités de « Beta testeur » pour les jeux « *Spell Of Genesis* », « *Sarutobi* », « *Takara* » et notre participation à la communauté « *Rare Pepe Card* ».

# CHAPITRE I - L'ÉMERGENCE DU PHÉNOMÈNE DES CRYPTOMONNAIES (CM) : BITCOIN ET ETHEREUM COMME INFRASTRUCTURES SOCIOTECHNIQUES

« Le commerce sur Internet en est venu à reposer presque exclusivement sur les institutions financières agissant comme tiers de confiance afin de traiter les paiements électroniques. Alors que le système fonctionne suffisamment bien pour la plupart des transactions\*, il souffre de faiblesses inhérentes au modèle de confiance. Les transactions\* totalement irréversibles ne sont pas réellement possibles, car les institutions financières ne peuvent pas éviter d'être médiateur de conflits. Le coût de la médiation augmente les coûts de transaction\* [...]. Avec la possibilité de réversibilité, la nécessité de la confiance s'étend. [...] Ces coûts et incertitudes dans les paiements peuvent être évités par la présence et l'argent physiques, mais aucun mécanisme n'existe pour faire des paiements à travers un canal de communication sans tiers de confiance. Le besoin est d'avoir un système de paiement électronique basé sur une preuve cryptographique [...] permettant à deux parties volontaires de réaliser entre elles des transactions\* sans avoir besoin d'un tiers de confiance. [...] Dans ce papier, nous proposons une solution [...] utilisant un serveur d'horodatage\* distribué pair-à-pair afin d'engendrer calculatoirement la preuve de la chronologie des transactions\*. Le système est sûr tant que les nœuds\* honnêtes contrôlent collectivement plus de puissance CPU que celle de chacun des groupes de nœuds\* d'attaquants coopérants. »

**Bitcoin : A Peer-to-Peer Electronic Cash System**  
Satoshi Nakamoto, 2008, p. I<sup>60</sup>

« Le développement de Bitcoin par Satoshi Nakamoto en 2009 a souvent été salué comme une évolution radicale de la monnaie, premier exemple d'un actif numérique qui n'est adossé à aucun autre actif ni n'a de « valeur intrinsèque », ni d'entité centralisé ou régulateur. Cependant, une autre partie sans doute plus importante de l'expérimentation Bitcoin est la technologie blockchain sous-jacente en tant qu'outil de consensus distribué et l'attention est rapidement en train de se porter sur cet autre aspect de Bitcoin. D'autres applications de la technologie blockchain fréquemment citées comprennent l'utilisation d'actifs numériques sur la blockchain pour représenter des monnaies personnalisées et des produits financiers (« colored coins »), la propriété d'un bien physique (« smart property »), des actifs non fongibles tels que les noms de domaine (« Namecoin »), de même que des applications plus complexes où des actifs numériques sont directement contrôlés par un bout de code exécutant des règles diverses (« smart contracts\* »), ou même encore des organisations autonomes décentralisées basées sur la blockchain « decentralized autonomous organizations » ou DAOs. Ce qu'Ethereum entend fournir est une blockchain avec un langage de programmation\* intégré, Turing-complet, qui peut être utilisé pour créer des « contrats » susceptibles de coder des fonctions de transition d'état quelconques, permettant aux utilisateurs de créer n'importe lequel des systèmes décrits ci-dessus ainsi que beaucoup d'autres que nous n'avons pas encore imaginés, tout ceci en quelques lignes de code. »

**Ethereum Whitepaper**  
Vitalik Buterin, 2013, p.I<sup>61</sup>

Bitcoin est « une évolution radicale de la monnaie » (Buterin 2013d, p. 1), car « complètement décentralisé », « entièrement peer-to-peer, sans tiers de confiance » qu'il s'agisse d'un serveur, ou d'une autorité centrale (Nakamoto 2008c, 2009b). Par la technique et pour la première fois, l'argent est soustrait au « modèle de confiance » et à ses faiblesses (Nakamoto 2008c). Finis la « violation » de confiance consécutive aux recompositions du consensus politique, les changements de règles du jeu, la réversibilité des paiements ou encore l'intervention d'institutions financières médiatrices (Nakamoto 2008c, 2009a). Bitcoin participe d'une souveraineté individuelle inédite, en opposition aux cadres juridictionnels nationaux et à leurs instances de régulation vis-à-vis desquels chacun

---

<sup>60</sup> Traduction française réalisée par Arnaud-François Fausse @AFFAUSSE que nous avons pu modifier marginalement. Pour la version originale, voir [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_fr.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf) [consultation au 01/06/2022].

<sup>61</sup> Traduction française réalisée par l'Asseth. Pour la version originale, voir <https://ethereum.org/en/whitepaper/> [consultation au 01/06/2022].

pourrait choisir de faire sécession : il s'agit de « *placer [son] argent et [sa] confiance dans un cadre mathématique exempt de politique* » (Tyler Winklevoss, cité par Mullin 2013). Quelle différence radicale distingue Bitcoin des systèmes monétaires hiérarchisés traditionnels ? Sa neutralité politique répondent les *coiners*\* ! Bitcoin se présente comme un présent apolitique, parfait et sans égal, offert par un démiurge anonyme agissant en roi philosophe. Le consensus politique variable et ses « *codes humides* » seraient remplacés tout entiers par un consensus technique, indiscutable et non négociable, car programmatiquement déterministe, produit par un protocole informatique\*, lui codé en « *sec* » (Szabo 2008b)<sup>62</sup>. Ce design parfait et immutable immunise Bitcoin contre la discréption, offrant les conditions d'une monnaie à la fois « *saine* » de par son monnayage *ad hoc* et aussi absolument neutre et apolitique (Keir 2022). Indépendant de tout désir et de toute attente, il se présente comme un standard universel, imperméable aux conflits sociopolitiques qui lui restent extérieurs : Bitcoin n'étant « *pas plus une monnaie libérale qu'une monnaie communiste* », chacun pourra l'adopter quels que soient sa culture, sa langue, sa religion, sa géographie ou son système politique ou économique (Antonopoulos 2013; Keir 2022).

Les ambitions technicistes des *coiners*\* qu'interroge cette thèse peuvent se traduire sous la forme d'un syllogisme que nous qualifions de « libéral-techniciste » postulant que : puisque (i) la technique est autonome et neutre vis-à-vis du monde social, et que (ii) les CM sont des monnaies purement techniques, alors (iii) elles sont immunisées contre toute gouvernance humaine et ses intérêts politiques, ce qui en fait, naturellement, de (iv) « meilleures » monnaies que les monnaies nationales. Ce chapitre s'intéresse principalement aux deux premières prémisses : nous démontrerons que la neutralité technique absolutisée attribuée aux cryptomonnaies\* n'est qu'une illusion. Ce travail de démythification est fondamental pour saisir pleinement la complexité sociotechnique qui caractérise les CM avant d'aborder les questions suivantes de la thèse. La neutralité, par définition, est relative à des normes et valeurs auxquelles elle se rapporte, voire s'oppose. Ce qui est reconnu à demi-mot est que la neutralité de Bitcoin n'est pas une « *absence de principes* », mais un « *principe en soi* » (Antonopoulos 2013) s'opposant à d'autres. Pour nous, le paradoxe est d'affirmer qu'un protocole relevant d'un acte profondément politique puisse être apolitique (Keir 2022). Ce paradoxe est redoublé quand on s'aperçoit que l'absolue neutralité d'un accès universel connaît cependant une exception : Bitcoin « *traite toute transaction\* de n'importe quelle personne et vers n'importe quelle autre [...] indépendamment de tout le reste* », sauf si « *vous n'adhérez pas aux règles du réseau\* ou si vous ne payez pas les frais appropriés* », suivant une logique « *de marché libre* » (Keir 2022). S'exprime ici l'oxymore d'une universalité conditionnée à laquelle le slogan « *Code is Law* » renvoie: si toute loi est politique, un protocole et son code le sont aussi. Qu'importent les visions monétaires et les récits des créateurs(s) et promoteurs, d'ailleurs hétérogènes (cf. Chap. II). Bitcoin renvoie à un projet politique, constitutionnel même, qui, quoique distribué, évolutif et « *sans État, est loin d'être apolitique par nature* » (Jeong 2013, p. 2 et 3). Les déclamations de neutralité précédentes entretiennent une confusion en rabattant une neutralité d'ordre « extrinsèque », sur une autre « intrinsèque ». Extrinsèquement, le protocole n'épouse pas les réglementations nationales. Mais il n'est neutre que relativement aux autres systèmes normatifs, auxquels il oppose sa normativité propre. Intrinsèquement, ses règles faites en code ne sont pas neutres. Elles établissent les conditions du monnayage, la forme reconnue de l'UCN\*, des transactions\* attendues, ou « *comment traiter ceux qui tentent de falsifier le grand livre* » (*Ibid.*, p. 27 et 28). Ce code régule et hiérarchise l'ensemble des interactions possibles *on chain\**, établissant

---

<sup>62</sup> N. Szabo (2008b), chef de file d'une interprétation rigoriste du « *Code is Law* », distingue le « *code humide* » « *interprété par le cerveau* », du « *code sec* » qui l'est lui « *par les ordinateurs* ». Le premier, comme le droit, est par nature conflictuel du fait d'interprétations différentes de la loi entre ceux à qui elle s'impose et ceux qui l'appliquent, à l'inverse du « *code informatique et [des] fichiers lisibles par ordinateur (dans la mesure où un ordinateur les traite de manière cohérente)* » (*Ibid.*). Cf. Chap. III.

des statuts et rôles, des comportements permis, et d'autres incités ou interdits. Dire que Bitcoin n'est pas régulé est vrai et faux, suivant que l'on se place du point de vue de son protocole (auquel cas il l'est) ou des cadres juridictionnels nationaux (auquel cas, il échappe aux régulations).

Dépeindre Bitcoin et toute CM comme une pure réalisation technique, neutre, autonome et stabilisée correspond selon nous à tomber dans l'écueil d'un « technologisme », que l'approche des STS vise à dépasser. Participant de la définition de notre objet, cette démarche nous conduit à apprêhender les CM non comme des objets *déjà constitués*, mais comme des objets *en construction*. Nous chercherons donc à montrer dans ce chapitre de quelle façon les CM incorporent des *a priori* sociaux et politiques dans leurs caractéristiques de conception (Akrich 2010, p. 208). Mais si les *récits maîtres* (Star 1999, p. 384 et 385), les choix architecturaux et les paramètres initiaux de Bitcoin et d'Ethereum ne sauraient être compris sans considérer les inspirations politiques de Nakamoto, nous éviterons l'écueil inverse d'un « sociologisme » tout aussi erroné. Bitcoin, Ethereum et les CM ne doivent pas plus en effet être réduits à l'idéologie de leur concepteur. Filiations idéelles ne font pas contenu matériel. Entre l'idéation d'un protocole et la production des implémentations logicielles qui le supportent gît une multiplicité de problématisations hétérogènes, hybrides et situées. La production logicielle est toujours tendue entre les « *objectifs* » poursuivis et la difficulté de la « *mise en œuvre* », entre le risque de « *l'échec* » et la formulation de « *compromis* [lors desquels] *les objectifs contradictoires et les différences politiques rencontrent les détails techniques.* » (Edwards et al. 2009, p. 366). En second lieu, les CM sont des infrastructures sociotechniques dont les formes et contenus sont renégociés par des usages débordant de tous côtés les desseins du concepteur. Un protocole seul ne fait pas monnaie – « *crypto* » ou non – sans *confrontation* à des utilisateurs participant à part entière de sa production. Outre les rôles prévus au scénario, les acteurs recrutés peuvent en inventer d'autres (Akrich 2010, p. 208). Les CM ne sont pas construites, au sens de délibérément conçues et planifiées. Elles se développent dans un environnement changeant, grâce au travail de petites mains opérant dans l'ombre de « *créateurs* » mythifiés. Faire CM ne se décrète pas. C'est le produit tant matériel qu'idéel d'un ensemble de processus complexes, multi-acteurs et multi-niveaux, qui, par étapes, conduisent ces protocoles à évoluer, à étendre leurs usages et à s'intégrer au système monétaire et financier, les dotant finalement d'une valeur dans l'échange. Faire monnaie se fait au prix d'un processus heurté de *monétisation* (cf. Chap. II). Ce sont ces processus que nous tachons de retracer et d'analyser dans ce chapitre pour les CM. Si « *la technique définit son monde* », ce monde « *redéfinit la technique* » en retour (Akrich 1989, p. 43, 37 et 42) dans un va-et-vient très politique. La CM Bitcoin ne se réduit ni à son protocole, ni aux intentions de son concepteur, mais renvoie à une infrastructure qui, à la manière de la bouteille de Klein, est sans « *limite déchiffrable* », où « *son intérieur est son extérieur* » puisqu'elle doit se connecter à « *d'autres infrastructures* » par le travail d'acteurs dispersés (Kavanagh et Miscione 2017, p. 22). C'est ce processus que nous désignons comme la dynamique carnavalesque du développement infrastructurel des CM, une dynamique caractérisée par son aspect composite, négocié, fait de critiques et d'*« inversions paradoxales »* (*Ibid.*, p. 14). Comme tissu sans couture, Bitcoin est une étoffe au motif arlequin (cf. Chronologie 2), où chaque innovation peut constituer des déguisements non prévus à la parade initiale. Et les acteurs et/ou les UCN\* d'endosser de nouveaux costumes, les uns en différents « *Pierrots* » de l'intermédiation, les autres en autant de reconnaissance de dettes (« *IOU* » d'unités de comptes natives) émises et administrées par les premiers. Ces travestissements variés traduisent des intérêts et des désirs monétaires ou transactionnels diversifiés, démontrant par là qu'une CM est « *multifacette* » et « *politiquement contestée* » (Dodd 2017, p. 4 et 8). Ainsi considérée, une CM, même Bitcoin, n'apparaît pas plus neutre extrinsèquement qu'elle ne l'est intrinsèquement.

Ce chapitre vise aussi à offrir les éléments d'intelligibilité minimaux des caractéristiques et fonctionnements des CM, de Bitcoin et Ethereum en particulier, sans lesquels il nous serait

impossible d'évoquer dans la suite la thèse leur gouvernance. Reconnaissant qu'il est en dehors de nos compétences et peu utile à la démonstration de décrire exhaustivement les éléments et processus techniques de Bitcoin et d'Ethereum, ce premier chapitre présente leur fonctionnement au travers d'éléments simplifiés. Cependant, à contrepied d'une partie de la littérature redoublant le récit de monnaies désincarnées, apolitiques et exemptes de rapports sociaux, notre présentation ne s'arrête pas à leur seul fonctionnement protocolaire. Tout notre effort au contraire dans ce chapitre a consisté à les réinsérer dans le contexte général, tant idéal que matériel, de leur émergence en tant qu'infrastructure monétaire et financière. La nature composite des CM que nous visons à démontrer se retrouve dans les matériaux et sources hétéroclites rassemblées pour cette démonstration (voir encadré n°1 ci-après). Cette nature induit une mise en garde sur le caractère complexe, et parfois très technique, que pourra revêtir ce chapitre. Les nécessités de la démonstration imposent une granularité fine, potentiellement ardue à suivre, malgré des efforts de synthèse et simplification. Car démontrer que le politique, la négociation et le conflit se cachent dans le moindre détail technique nous a imposé de convoquer certains de ces acteurs non humains pour témoigner, là où ils sont trop souvent tenus sous silence. Des annexes, visant à alléger le corps du texte d'éléments techniques génériques, complètent le chapitre en offrant des voies d'approfondissement aux lecteurs curieux.

Traiter des CM comme catégorie générique impose de revenir au pionnier Bitcoin, d'où la place étendue qui lui est octroyée dans ce chapitre. Dans la mesure où il est le premier représentant de la catégorie des CM, son contexte d'émergence et ses arrangements sociotechniques forment de fait le matériau génétique de l'explosion subséquente des CM. Toutes (Ethereum n'y échappe pas) s'y rapportent toujours de près ou de loin. Ceci explique que notre présentation d'Ethereum fasse l'économie des éléments déjà posés pour n'insister que sur son altérité face à Bitcoin. Ce chapitre dense offre encore une vue circonstanciée du champ des CM, de l'émergence de leurs écosystèmes, de leurs acteurs, des ressources et contraintes de leur développement.

Partant du point de vue de l'objet technique et du concepteur, notre **première section (I.1)** présente Bitcoin. Nous restituons comment ses agencements sociotechniques clefs renvoient aux inspirations et contraintes théoriques et pratiques singulières que Nakamoto avait en tête, en soulignant que chacun des choix architecturaux effectués – en particulier le consensus fondé en PoW\* – est irréductiblement hybride, négocié et politique. Le **second temps (I.2)** propose de décaler le point de vue vers celui des utilisateurs réels et leurs usages. Saisi dans l'épaisseur d'un développement porté par une multiplicité d'acteurs, Bitcoin démontre qu'il n'est réductible ni aux desseins de son concepteur, ni à ses frontières protocolaires, puisqu'il est sans cesse renégocié par les improvisations d'acteurs. Une démarche similaire fonde la **dernière section (I.3)**, présentant Ethereum. Celle-ci revient sur les points saillants de sa normativité et de son développement infrastructurel propre. Finalement, la normativité des agencements d'Ethereum permet de souligner en négatif celle de Bitcoin : le design de Bitcoin est nourri des critiques de Nakamoto à l'endroit du système monétaire traditionnel auxquelles le design d'Ethereum ajoute des critiques à l'endroit de Bitcoin et des expériences qui l'ont suivi.

## I.1 QUAND BITCOIN DÉFINIT SON MONDE... : L'ALOI POLITIQUE D'UNE CM PIONNIÈRE

Cette section présente synthétiquement Bitcoin partant de la conception de son concepteur. Le/les créateur(s) de Bitcoin n'ont produit formellement ni cahier des charges, ni notice d'utilisation. Pour seules spécifications protocolaires et notice explicative, Nakamoto dote Bitcoin

du *WP\** (Nakamoto 2008c), de ses écrits en ligne (courant jusqu'en 2010<sup>63</sup>) et des premiers codes sources logiciels. Au-delà du caractère « sacré » qui est attribué<sup>64</sup> à ces productions, elles sont autant de traces renseignant ses desseins originaux. Le design de Bitcoin, comme les *récits maîtres* (Star 1999, p. 384-385) mobilisés par Nakamoto, repose sur des hypothèses, des croyances et des représentations qu'il a du monde social dans lequel Bitcoin doit s'insérer. Les saisir impose de restituer le creuset génétique de Bitcoin, assemblage hétéroclite d'inspirations, de contraintes et d'épreuves que Nakamoto enchevêtre dans son design. Mais attention, ne pas être « *l'otage des acteurs et de l'histoire qu'ils fabriquent* » implique un retour socio-historique, à partir duquel peut s'éclairer la façon dont les catégories mobilisées « *ont été localement construites et déconstruites [et] comment ont été éliminés certains acteurs et certains problèmes* » (Callon, 2006, p. 24).

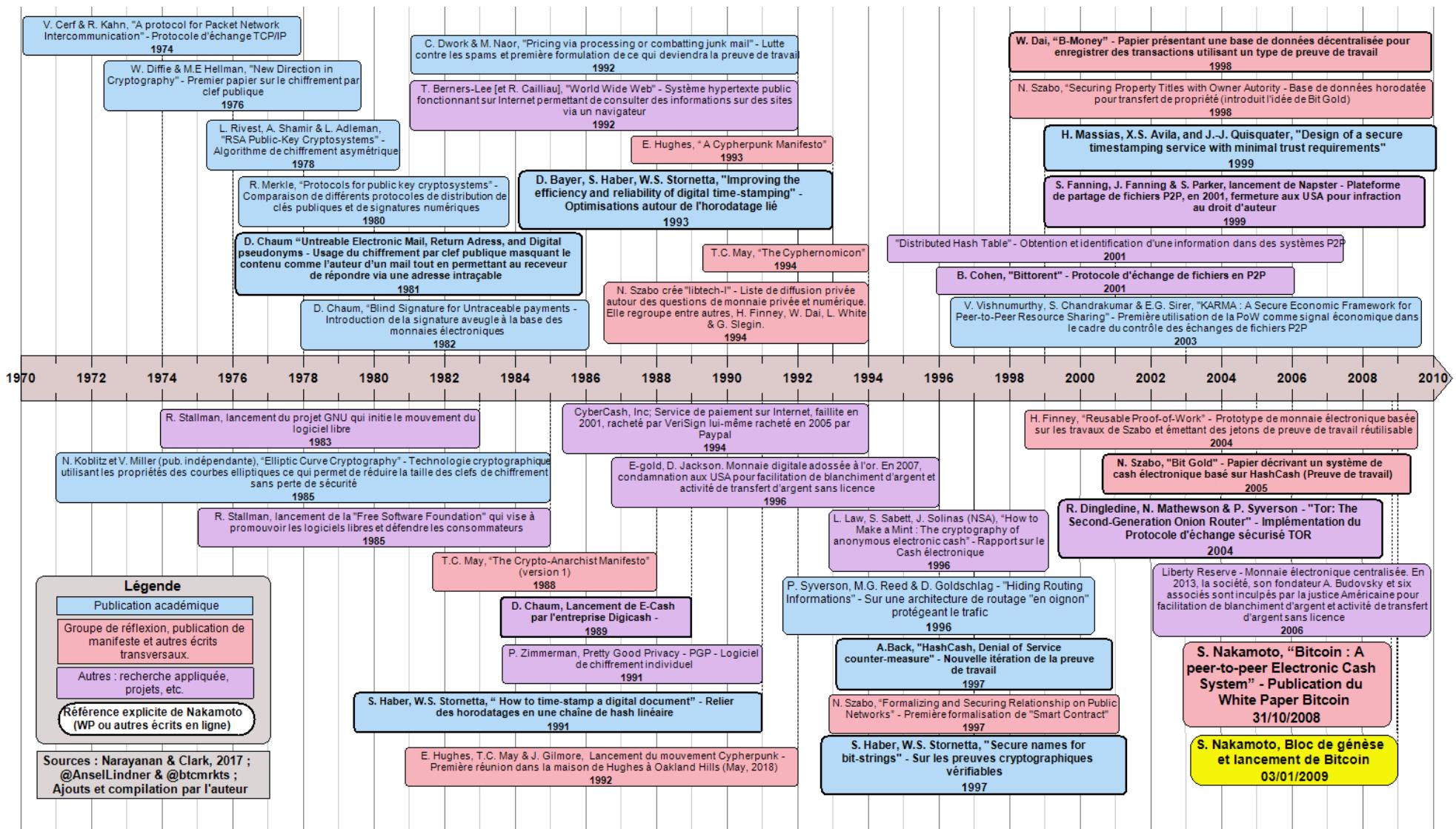
Nous allons le voir, l'éviction des « intermédiaires » et de leur consubstantielle « confiance », ainsi que la défiance envers les administrations étatiques et leurs régulations ne se comprend qu'à l'aune d'un certain substrat idéologique et des épreuves théoriques et pratiques que Bitcoin est censé dépasser. Restituer ce substrat idéologique de Bitcoin et le réinsérer dans l'histoire plus large des recherches sur les protocoles de registre\* distribué est une condition nécessaire, seule à même de mettre en perspective les alliances que Nakamoto cherche à produire par ces attachements sociotechniques (sect. I.1.1). Nécessaire mais non suffisante, car l'architecture et les paramètres initiaux de Bitcoin renvoient à des contraintes hybrides et négociées, aussi théoriques que pratiques, impliquant de trancher des arbitrages : ce que démontre l'analyse de l'algorithme de consensus\* fondé sur l'usage, radicalement innovant, d'une PoW\* (sect. I.1.2). Enfin, nous présenterons le fonctionnement de Bitcoin au travers de l'exemple idéal typique du traitement d'une transaction\* suivant le script original de Nakamoto (sect. I.1.3).

---

<sup>63</sup> L'ensemble de ses écrits sont disponibles sur le site <https://satoshi.nakamotoinstitute.org/> et un condensé a été réalisé dans « The Book of Satoshi » (Champagne 2014).

<sup>64</sup> Au sein des pratiques de type religieux qui se sont développées dans certaines franges de la communauté Bitcoin, le *WP\** occupe une place à part en tant que « *texte sacré* » écrit de la main du « *prophète : Satoshi* ». F. Ersham, [https://twitter.com/FEhrsam/status/933521744429686784?s=20&t=wQcy0w0tHCe8Ed\\_Odmm\\_Kw](https://twitter.com/FEhrsam/status/933521744429686784?s=20&t=wQcy0w0tHCe8Ed_Odmm_Kw) [consultation au 01/09/2022]. Si le *WP\** n'est en rien définitif, « *des fanatiques* » l'interprètent comme « *une Écriture sainte* » (Mow 2018).

## Chronologie 1 : Bitcoin, un objet sociotechnique aux inspirations hétérogènes



Source : Rolland Maël

### I.1.1 Du terreau matériel et idéal aux racines de Bitcoin

Dans le champ des CM, l'impression que Bitcoin naît *ex nihilo* de la cuisse d'un démiurge révolutionnaire peut prévaloir : « *imprévisible* », il aurait « *émergé de nulle part* » (Pouliot 2018). Nakamoto serait « *un outsider académique, et [...] Bitcoin ne porte[rait] aucune ressemblance avec des propositions universitaires antérieures* » (Narayanan et Clark, 2017, p. 1). Son émergence relèverait d'une « *Immaculée Conception* » (Held et McCormack 2018; Lars 2021; Favier 2021; Huegli 2022). Non seulement « *le fruit d'une incroyable intelligence [et] d'un coup de chance* » (Held et McCormack 2018), mais aussi d'« *un ensemble de circonstances extrêmement rares* » (N. Carter cité par Huegli 2022), le singularisant par nature des autres CM<sup>65</sup>. Son développement est « *organique : il a été ouvert à tous dès ses débuts, a lentement attiré les plus intéressés puis s'est développé progressivement, sans précipitation.* » (Lars 2021). Il « *est apparu... sans autre forme de procès* » (Favier 2021), comme « *la première forme de vie* » (Held et McCormack 2018). Bitcoin « *n'a pas fait l'objet d'un préminage*<sup>66</sup>, *d'une ICO ou d'une levée de fonds réservée à des investisseurs accrédités ; tout le monde pouvait en miner, en acheter ou en vendre* » et « *l'amorçage de sa valeur* » [a] *constitué un processus incertain* » (Lars 2021) : ces UCN\* n'eurent « *pas de prix durant leurs premiers mois d'existence* » (*Ibid.*), plongées « *dans un monde où les espèces numériques n'avaient pas de valeur établie, elles circulaient librement* » (N. Carter cité par Huegli 2022).

Paradoxalement, les thuriféraires de Bitcoin nous disent qu'il vient de « *nulle part* » et, en même temps, qu'il est « *l'aboutissement d'un processus itératif au cours duquel des individus motivés par leur idéologie ont continuellement innové sur le travail des autres, guidés par les principes organisationnels fondamentaux des logiciels libres et de l'idéologie cypherpunk.* » (Pouliot 2018). Les deux n'étant pas tenables, laissons les pratiques et références de Nakamoto trancher la question (cf. Chronologie 1<sup>67</sup>). Son travail s'inscrit tout à la fois dans un certain académisme (Rykwalder 2014; Bonneau et al. 2015; Qureshi 2019; Narayanan et Clark 2017; Bano; et al. 2017; Chanut 2019, en bleu dans la chronologie) et dans des philosophies politiques (*Cypherpunk* et *Cryptoanarchisme* et libertarienisme, en rouge). Il s'appuie aussi sur des recherches appliquées et des expérimentations singulières (logiciels libres, réseaux\* P2P et monnaies privées numériques dont Bitcoin est plus ou moins explicitement inspiré, en violet ; Narayanan et Clark 2017; Bano; et al. 2017; Pouliot 2018; Van Wirdum 2018; Jean-Luc 2018; McCormack et Szabo 2019; McCormack et Van Wirdum 2020; Cuen 2020; McCormack et Van Wirdum 2020). L'histoire intellectuelle de Bitcoin est un cas exemplaire d'entremêlement de « *relations entre le monde universitaire, les chercheurs extérieurs et les praticiens* »(Narayanan et Clark 2017, p. 1). D'où sa

---

<sup>65</sup> Cela touche à une controverse entre les *bitcoiners* et les autres *coiners*, ayant trait aux questions de gouvernance que nous aborderons plus avant dans notre chapitre III.

<sup>66</sup> Une « *prémine* » est un terme indigène qui qualifie le mécanisme de création de tout ou partie des UCN d'un protocole de registre\* distribué avant même le lancement d'un protocole. Nous y reviendrons en section I.3.

<sup>67</sup> Ce document est d'abord construit sur la généalogie du pedigree académique de Bitcoin de Narayanan et Clark (2017, p.2). En complément, afin de réinscrire Bitcoin au-delà de ses seules inspirations académiques, nous y ajoutons des sources grises ; au premier chef, la chronologie « *Bitcoin pre-history* » d'Ansel Linder et btcmrkts (2018) qui ajoute aux inspirations académiques de Bitcoin, d'autres plus sociopolitiques. Cherchant moins à être exhaustif qu'illustratif, nous avons retenu à chaque fois les références séminales au détriment de celles secondaires (sur les consensus classiques, par exemple) et écarté certains éléments événementiels, voire discutables (chez Ansel Linder et btcmrkts (2018), comme la référence à M. Rothbard, entre autres). En guise de vérifications, de compréhension et de complément, nous avons pris connaissance des références primaires et enrichi l'ensemble d'éléments tirés d'autres lectures (références au logiciel libre, par exemple). Ces éléments sont distingués par un code couleur selon qu'ils s'inscrivent dans le champ académique (bleu), dans le mouvement *cypherpunk* et *crypto-anarchiste* (rouge) ou dans d'autres types de champs (violet), afin de visibiliser la nature chimérique de la création de Nakamoto, dont les références explicites sont finalement pointées en gras.

capacité à éclairer la dimension construite de ces « mondes » aux frontières poreuses puisqu'on y trouve des personnalités reconnues du monde académique, simultanément engagées dans des activités militantes et professionnelles. Dans le sillage d'Akrich (1989), la restitution de ces éléments génétiques permet d'éclairer la « trame principale », mais aussi les contraintes de « réalisation » et de « montage » afin de rendre intelligibles les intrigues du « scénario », le « script » et le casting des « personnages » - les statuts et rôles afférents – au cœur de la conception Bitcoin suivant les desseins de son concepteur. Car, si Bitcoin est une monnaie, l'éviction principielle des solutions centralisées qui en est la marque est frappée au coin de philosophies politiques et d'expériences pratiques qu'il nous faut expliciter.

## Une monnaie frappée au coin de philosophies politiques et d'expériences pratiques

Le/les créateur(s) anonyme(s) de Bitcoin renseigne(nt) leurs inspirations critiques. Le papier séminal - « *Bitcoin : Un système de cash électronique pair-à-pair* »<sup>68</sup> - prend la forme d'un court WP\*, publié le 31 octobre 2008 sous le pseudonyme de Nakamoto (Nakamoto 2008c), d'abord diffusé dans un cercle d'initiés via la *Cryptography Mailing List*<sup>69</sup>. En janvier 2009, le même Nakamoto publie les codes informatiques de la première version logicielle (Bitcoin-Qt, aujourd'hui Bitcoin Core), génère l'*enregistrement de genèse*\*, enregistre le nom de domaine Bitcoin.org<sup>70</sup> et fonde le forum *Bitcointalk*<sup>71</sup>, sur lequel il reste actif jusqu'au 12 décembre 2010 (Champagne 2014). L'introduction du WP\* est déjà l'occasion pour lui de critiquer les monnaies existantes (voir épigraphe du chapitre), mais les contraintes formelles de l'exercice lui imposent la parcimonie. Nakamoto est plus acerbe en ligne, ce qui permet de préciser ses critiques et leurs références. Sa défiance à l'encontre des autorités monétaires et des tiers de confiance est centrale puisqu'aux coûts de transaction\* induits (Nakamoto 2008c) s'ajoutent selon lui des risques et abus rédhibitoires : pour lui, en effet, le système fractionnaire repose structurellement sur des coercitions asymétriques dangereuses (censure de transaction\*, saisie de compte, etc.) et du monitoring (surveillance des informations financières) qui, instrumentés politiquement, conduiraient inéluctablement à une émission monétaire excessive (prêt en dernier ressort, Quantitative Easing...) et de l'inflation « *avilissant la monnaie* » (Nakamoto 2009b).

Déjà, Nakamoto reconnaît une « *conception et [un] codage [...] commencés en 2007* » (Champagne 2014, p. 125), soulignant comment la crise financière de 2007-2008 joue le rôle d'événement déclencheur : insatisfait des actions menées, c'est avec ironie qu'il inscrit dans

---

<sup>68</sup> Le message originel est consultable ici : <https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html> [consultation au 05/06/2022].

<sup>69</sup> Cette liste, « *consacrée à la technologie cryptographique et à son impact politique* », nécessite une inscription, et ses membres doivent rester « dans le sujet » : elle comprend « *les aspects techniques des cryptosystèmes, [leurs] répercussions sociales [...] et la politique de la cryptographie*\*, comme le contrôle des exportations ou les lois limitant la cryptographie\*. Les discussions sans rapport avec la cryptographie\* sont considérées comme hors sujet. » Voir <https://www.metzdowd.com/mailman/listinfo/cryptography> [consultation au 05/06/2022].

<sup>70</sup> « Il a utilisé ses adresses électroniques provenant de serveurs de messagerie hautement confidentiels et a trouvé le moyen d'enregistrer anonymement le domaine bitcoin.org [...] le 18 août 2008 » (voir <https://www.whois.com/whois/bitcoin.org>, cité par Ducrée 2022, p. 4 [consultation au 06/06/2022]).

<sup>71</sup> Le profil de Nakamoto est encore en ligne (<https://bitcointalk.org/index.php?action=profile;u=3>) comme son premier billet (<https://bitcointalk.org/index.php?topic=5>). Il y annonce la création de ce nouveau forum dédié en remplacement de l'ancien, lancé en mai 2009 et hébergé sur sourceforge.net (<http://bitcoin.sourceforge.net/boards/index.php>, site aujourd'hui inaccessible, l'archive est consultable ici <https://web.archive.org/web/20090511173000/http://bitcoin.sourceforge.net/> [consultation au 05/06/2022]).

l'enregistrement de genèse<sup>72</sup> le message : « *The Times 03/Jan/2009 Le Chancelier est sur le point de lancer un deuxième plan de sauvetage pour les banques* »<sup>73</sup>. Nakamoto fait coup double, puisqu'à l'ironie il ajoute l'affirmation pratique de la crédibilité des principes de transparence et d'ouverture à tous qu'il promeut : cette référence à la une d'un grand média, prouve la date effective du lancement du Bitcoin à la suite duquel et « *à partir de son deuxième bloc* », tout « *intéressé* » peut prendre part à Bitcoin dans les mêmes conditions que son créateur (Huegli 2022)<sup>74</sup>. Face aux gouvernements, Nakamoto vise modestement<sup>75</sup> à gagner « *une bataille importante dans la course aux armements et [à] accéder à un nouvel espace de liberté pour plusieurs années* » (Champagne 2014, p. 44). Cette bataille des racines anciennes reflète les filiations théoriques et pratiques de ces critiques. En raison de notre formation, nous connaissons certaines critiques économiques (monétarisme, *Free banking* ; cf. Chap. II). Cependant, en travaillant sur le sujet, nous en avons découvert d'autres. Nakamoto s'inspire, plus ou moins explicitement des idées et pratiques développées, à partir de 1980-90, par des groupes autoproclamés *Crypto-anarchistes*, *Cypherpunk* ou *Extropians*<sup>76</sup>. Ils se sont constitués autour d'organisations de chercheurs en sciences informatiques et en *cryptographie*\*, par exemple *l'International Association for Cryptologic Research*, créée en 1981 (Castor 2017; McCormack et Van Wirdum 2020), et d'espaces de discussion, soit physiques<sup>77</sup> soit numériques, avec la création de la liste de diffusion « *cypherpunk*

---

<sup>72</sup> Le bloc de genèse est un « *fait du prince* », codé dans le protocole. Il est le premier enregistrement émis et diffusé au sein du réseau. Son statut est particulier, suivant qu'il ne fait pas référence à d'autres enregistrements et les UCN émises en récompense de sa production sont protocolairement inutilisables. Cet enregistrement 0 est consultable via un explorateur

Bitcoin

(<https://live.blockcypher.com/btc/block/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f/>)

Ces services d'explorateurs sont accessibles en ligne pour chaque CM. Pour Bitcoin, voir par exemple <https://live.blockcypher.com/btc>; <https://blockstream.info/>. Ces services permettent de suivre le traitement des transactions\*, de consulter les enregistrements et les transactions passées depuis le lancement de la chaîne de blocs\* et d'accéder à d'autres données (sur le minage ou la répartition des UCN par adresses, par exemple), contribuant ainsi à la transparence de ces systèmes de paiements.

<sup>73</sup> Titre à la une du Times du 3 janvier 2009. [https://en.bitcoin.it/wiki/Genesis\\_block](https://en.bitcoin.it/wiki/Genesis_block) [consultation au 24/09/2015].

<sup>74</sup> Cette affirmation récurrente est contrefactuelle puisqu'il faut attendre le 9 janvier pour que soit publié le premier logiciel.

<sup>75</sup> Nakamoto sait la victoire temporaire, reconnaissant qu'il « *ne [trouve] pas de solution aux problèmes politiques dans la cryptographie*\* » seule (Champagne 2014, p. 44).

<sup>76</sup> Ces groupes différents connaissent des chevauchements. Pour le premiers, les principaux fondateurs sont David Chaum ; John Gilmore ; Timothy C. May et Eric Hughes, voir <https://en.wikipedia.org/wiki/Cypherpunk> [consultation au 02/10/2017]. Cette appellation, établie par T.C. May dans « *Crypto-anarchist Manifesto* » (May 1988), est conçue comme « *une idéologie plutôt [qu'un] plan* » et l'une « *des rares contributions réelles à l'idéologie dans la mémoire récente.* » (May 1994, p. 294). Pour ce qui est des *Extropians*, « *pas aussi souvent discuté [, ils] ont commencé dans les années 80, il s'agissait d'un groupe de futuristes californiens super optimistes [...] intéressés par la nanotechnologie, la technologie de prolongation de la vie, l'exploration spatiale et ils voyaient la science progresser à un rythme croissant, exponentiel même, et ils ont commencé à philosopher sur ce que cela pourrait apporter à la société [...] c'était une idée très libertarienne et très influencée par l'économie autrichienne. [...] May était l'un de ces extropiens [...] Szabo l'était [...] Wei Dai l'était [...] Hal Finney était là et beaucoup de ces extropiens sont allés à la réunion Cypherpunk, qui ne s'appelait pas encore les Cypherpunks [ : c'est] une sorte de blague qu'ils ont inventée [,] c'était un jeu de mots sur cypherpunk. » (McCormack et Van Wirdum 2020). La paternité de cette appellation est attribuée à Judith Milhon, qui l'a construite sur le modèle du genre littéraire « *Cyberpunk* » (Manne 2011). Elle entre dans le dictionnaire Oxford en 2006 : correspondant à un nom donné à une « *personne qui utilise le chiffrement lorsqu'elle accède à un réseau informatique dans le but d'assurer la confidentialité et de se protéger, en particulier des autorités gouvernementales* ».*

<sup>77</sup> La première rencontre physique réunit les fondateurs, *extropians* et *cryptoanarchiste*, dans la maison de Hughes à Oakland Hills et donne lieu par la suite à des rencontres mensuelles (Jean-Luc 2018; McCormack et Van Wirdum 2020). La *cypherpunk mailing liste* hébergée par J. Gilmore et H. Daniel May, 2018; <http://mailing-list-archive.cryptoanarchy.wiki/> est accessible uniquement par cooptation. On retrouve dans cette liste de diffusion des « *grands noms* », par exemple : A. Back, B. Cohen, E. Hughes, H. Finney, I. Griggs, J. Gilmore, J. P. Barlow, J. Assange, M. Hellman, W. Diffie, Bryce “Zooko” Wilcox, W. Dai, M. Blaze, N. Szabo, P.E. Metzer, P. Zimmerman, T.C. May, voir <http://mailing-list-archive.cryptoanarchy.wiki/authors/notable/> [consultation au 15/08/2020].

*mailing list* » aujourd’hui disparue, et dont Nakamoto utilise 20 ans après l’héritière (*Ibid.*). Au travers de courts textes et manifestes sont forgées des philosophies politiques singulières autour des questions de nouvelle technologie de l’information et de la communication<sup>78</sup>. Hétérogènes, les « *inclinaisons philosophiques* » des membres de ces groupes vont du très « *radical [...] Tim May à celles, plus modérées, d’Éric Hughes* » (Jeong 2013, p. 9-10). Le premier, « *libertarian* » auto-déclaré, s’identifie aux courants libertariens anarcho-capitalistes<sup>79</sup>. Postulant une primauté « naturelle » d’individus libres, coordonnés spontanément par des mécanismes marchands, il dit participer à « *la propagation de la crypto-anarchie* », une révolution technique qui permettra, hors de tout contrôle, de tout échanger sur des marchés parfaits : « *un marché informatisé anonyme rendra même possibles des marchés odieux d’assassinats* » (May 1992). Hughes, plus modéré, développe une vision en termes de « *contrat social* » et de « *bien commun* » : si tant est que la « *vie privée [est] nécessaire à une société ouverte à l’ère électronique* », son extension nécessite, au-delà de la seule concurrence, de la « *coopération* » (Hughes 1993).

Restent entre ces idéologues des dénominateurs communs. Ils partagent la volonté de remettre en cause le monopole de l’usage des techniques cryptographiques par les administrations publiques et militaires (Castor 2017; McCormack et Van Wirdum 2020). Ils défendent le droit cardinal de chacun à la vie privée et à l’anonymat (qui n'est pas le secret, Hughes 1993) contre des gouvernements et des firmes abusant de leur emprise sur l’information et les canaux de sa circulation. Dans leur volonté de rendre impotentes toutes les entités à prétention orwellienne<sup>80</sup> (Chaum 1985), la technologie prend une place centrale. L’interface des réseaux\* et de nos écrans permettrait de dissocier, radicalement et comme jamais, nos corps et nos esprits. La cryptographie\* et le cyberspace, « *nouvelle partie de l’esprit* » (Perry Barlow 2000, p. 50), ouvrent des voies d’émancipation inédites : il deviendrait possible d’assurer de manière efficace et sécurisée la négociation comme l’exécution de contrats électroniques privés entre des parties ne connaissant ni leurs noms, ni leurs identités juridiques (May, 1992). Est ainsi proclamée une souveraineté « individuelle » inédite, opposée aux cadres collectifs de l’État-Nation. De celle-ci peut émerger des communautés constituées librement, sans aucun recours à la « *menace de la violence* », car « [leurs] participants ne peuvent pas être identifiés par leurs vrais noms ou leurs adresses » (Dai 1998). Suivant un développement technologique inéluctable, l’État et ses capacités d’action sont remis en cause<sup>81</sup> : le gouvernement ne serait « *pas temporairement détruit, mais [deviendra] inutile et interdit de manière permanente* » (May 1992). Face aux États et « *gouvernements du monde industriel, [...]*

<sup>78</sup> Notons Timothy C. May avec « *The Crypto Anarchist Manifesto* » (1992) et « *Cyphernomicon* » (1994) ; Eric Hughes avec « *A Cypherpunk’s Manifesto* » (1993) ; ou encore « *A Declaration of Independence of Cyberspace* » de J. Perry Barlow ([1996], 2000).

<sup>79</sup> Malgré la polysémie en langue anglaise, May assume s’opposer aux courants libertaires, déclarant qu’il est « *venu à l’appeler "cryptoanarchie" et [qu’] en 1988, [il a] écrit "le Manifeste Crypto Anarchiste", dont la forme est vaguement inspirée d’un autre manifeste célèbre [le manifeste du Parti Communiste de Marx et Engel, NdL]. Il est basé sur "l’anarcho-capitalisme", une variante bien connue de l’anarchisme. (Rien à voir avec les anarchistes ou les syndicalistes russes, juste avec le libre-échange et les transactions volontaires)* » (May 2018). La revendication est étayée dans *Cyphernomicon* (1994) où Ayn Rand est érigée en inspiration primordiale du crypto-anarchisme (p. 294) ; Friedrich Von Hayek est convoqué (p.283) pour son concept d’ « *ordre spontané* » et dans lequel May s’enorgueillit que le fils libertarien de Milton (David Friedman, auteur de « *The Machinery of Freedom* » à ne pas confondre à son frère Benjamin, économiste d’obédience néo-keynésienne), soit « *converti à ces idées [...] suffisamment pour donner une conférence [...] intitulée "Crypto Anarchie et l’État"* » (May 1994, p. 294).

<sup>80</sup> Tiré du titre de D. Chaum (1985, p. 1), « *Security without identification: transaction systems to make big brother obsolete* ».

<sup>81</sup> « *Un spectre hante le monde moderne, le spectre de la crypto-anarchie. La technologie informatique est sur le point de donner aux individus et aux groupes la possibilité de communiquer et d’interagir entre eux de manière totalement anonyme [...] Ces développements vont complètement modifier la nature de la réglementation gouvernementale, la capacité de taxer et de contrôler les interactions économiques[...]* » (T. May, 1992).

*géants de chair et d'acier fatigués* » appartenant au passé, un « *moi virtuel immunisé contre [leur] souveraineté* » émerge du « *cyberespace* » (Perry Barlow 2000). Au « *nom de l'avenir* » et malgré le fait qu'il faille encore « *consentir à [leur] domination sur [les] corps* », il est désormais possible de se « *disperser sur la planète* » afin d'établir « *une civilisation de l'esprit dans le cyberespace* » que « *personne ne [pourra] arrêter. Puisse-t-elle être plus humaine et plus juste que [ce que les] gouvernements ont créé auparavant.* » (*Ibid.*). Pour que ces communautés plus justes et démocratiques émergent, il est nécessaire de disposer de protocoles informatiques sécurisés et durables, avec des architectures permettant une coopération efficace entre individus, hors identification *intuitu personæ*. Il reste à développer les éléments essentiels à l'existence de ces communautés virtuelles autonomes, y compris la monnaie, cruciale pour leur coordination. Dans ces réseaux\* décentralisés pair-à-pair, une participation égalitaire de chacun est attendue. La transparence et l'auditabilité des codes sont indispensables, tout comme l'*holoptisme*, propriété essentielle permettant à chacun de vérifier l'ensemble des activités qui s'y déroulent. Si l'argent, comme « *moyen de faire respecter les contrats* » a « *traditionnellement [été] fourni par le gouvernement ou des institutions parrainées* » (Dai 1998), les *cypherpunks* travailleront à l'émergence d'alternatives. Pour cela, ils doivent lever certains obstacles les privant encore d'une « *monnaie numérique plus robuste et plus fiable* » (May 1994, p. 8)<sup>82</sup>.

Le contexte dans lequel les *Cypherpunk* et *Crypto-anarchisme* ont émergé explique pourquoi leurs membres en sont venus à détester toute forme de centralisation, en particulier étatique, et à créer des systèmes sociotechniques pour s'en affranchir. Ils ont eu à faire face, pour certains personnellement, aux gouvernements et à leurs coercitions... particulièrement leurs expérimentations monétaires. Leur « *lutte anti-gouvernementale et individualiste* » fut pratique avant d'être théorique et s'est « *manifestée le plus clairement dans le procès intenté par le ministère de la Justice américaine à Philip Zimmermann*<sup>83</sup> », créateur du protocole de chiffrement *PGP*, considéré comme une « *réalisation historique* » du mouvement pour la vie privée (Jeong 2013, p. 10). Dans un monde octroyant au numérique une place toujours plus grande, P. Zimmerman et ceux qui le défendent sont persuadés que le droit à la vie privée « nécessite » un accès de tous, plein et entier, aux technologies de chiffrement. Ce procès prouverait, selon eux, que rien n'est à « attendre » de la « *bienveillance* » « *des gouvernements, des entreprises ou d'autres grandes organisations sans visage* » quant à la garantie d'un droit à la « *confidentialité* » (Hughes 1993). D'autres batailles suivront, comme autour de la loi de « *réforme des télécommunications de 1996* » aux USA, tentant de « *soumettre le cyberespace à des contraintes plus sévères que celles actuellement en vigueur à la cafétéria du Sénat* » (Barlow 2016, p. 48). Ces disputes s'inscrivent dans les luttes apparues, courant 1990, contre ce qui est considéré comme un « *second mouvement des enclosures* » via la montée *irrésistible* de la propriété intellectuelle (Coriat et Broca 2015, p. 272). Dans les années 1970-80, suivant un affaiblissement compétitif, les USA ont en effet amorcé un renforcement draconien de la propriété intellectuelle dans les domaines du logiciel et du vivant (Coriat 2010, p. 5). L'extension de l'*« idéologie propriétaire »* passe par une instrumentation du droit. Les partisans des enclosures avancent que l'efficience économique commande que les formes « *de "droits partagés"* » soient remplacées par des droits de propriété privée « *entiers, c'est-*

---

<sup>82</sup> May reconnaît des systèmes de communication encore « *fragiles* », connaissant les « *problèmes habituels* » de montée en charge (« *Scaling* »), comme ceux rencontrés par la liste de diffusion Cypherpunk (« *surcharge, manque d'espace disque, mise à jour des logiciels, etc.* ») qu'il voit comme un « *avertissement* », une leçon sur ce qu'il est encore nécessaire de construire (May 1994, p. 8).

<sup>83</sup> En 1994, P. Zimmermann est soumis à un « *long interrogatoire concernant l'éventuelle exportation illégale de munitions dangereuses* » (Stay 1997, p. 581). La justice américaine lui reproche la diffusion libre de son logiciel qui, qualifiée d'*« exportation cryptographique »*, viole « *la réglementation sur le trafic international des armes (ITAR)* » (Jeong 2013, p. 10). Bien qu'abandonnée, l'enquête du grand jury suscite « *l'indignation publique* » et s'érige en « *événement catalyseur* » de ces groupes (*Ibid.*).

*à-dire exclusifs* » (*Ibid.*, p. 1). Voilà qu’aux demandes d’un droit d’accès de tous, plein et entier, au code logiciel, les législateurs répondaient par la fermeture, l’exclusivité et l’interdit propriétaire. Face à ce qu’ils considèrent comme une déclaration de « *guerre au cyberspace* » du gouvernement, les *Cypherpunks* vont chercher à démontrer « *combien [ils peuvent] être astucieux, déroutants et puissants pour [se] défendre* » et prendre « *congé d’eux* » (Perry Barlow, 2000, p. 50). Par le droit, les usagers étaient dépossédés « *des libertés d’utiliser, de copier, de modifier et de distribuer les logiciels* » (Mangolte 2013b, p. 9) et la société, des bénéfices sociaux de l’informatique ouverte. Par le droit s’effectue la contre-offensive avec des chercheurs en informatique qui s’allient stratégiquement à des juristes<sup>84</sup>. Aux licences *copyright* et au contrôle exclusif octroyé au propriétaire est opposée une diversité de licences libres, depuis les plus intransigeantes *copyleft*s à d’autres plus *permissives*<sup>85</sup> (*Ibid.*, p. 1). La liberté logicielle est érigée comme pierre angulaire de cette « *défense active et militante des libertés sur Internet* » (L. Lessig, à qui les *coiners*\* empruntent le slogan « *Code is Law* », cf. Chap. III – cité par Coriat et Broca 2015, p. 274). Bitcoin et ses codes sources publiés sous licence MIT<sup>86</sup> doivent s’analyser à l’aune de ces combats et de leurs enjeux.

Nakamoto voit des enseignements similaires dans d’autres expérimentations numériques qui ont eu à faire face à la loi et à son application. Citons déjà les expériences de monnaies numériques privées : que ce soit de l’ « *eCash* », reconnu comme le premier système de paiement basé sur la cryptographie\* du début 1990 par D. Chaum (Jeong 2013; Van Wirdum 2018; McCormack et Van

---

<sup>84</sup> La critique « *de la privatisation croissante du patrimoine intellectuel et culturel de l’humanité* » dans le champ juridique émerge d’un groupe d’acteurs académiques dont les têtes de file sont J.Litman, Y.Benkler, L.Lessig, J.Boyle (Coriat et Broca 2015, p. 273).

<sup>85</sup> La notion de logiciel libre (« *free software* ») émerge début 1980 grâce à Richard Stallman qui crée la *Free Software Fondation* et le projet GNU sous la première licence libre, dès 1983. Le premier standard de « *définition du free software (logiciel libre)* » (Mangolte 2013, p. 9) attendra l’ « *emblématique* » licence « *GPL* », de Stallman et Eben Moglen en 1989 (*Ibid.*, p. 277). Cet engagement fait suite à l’abandon par Stallman de son poste de chercheur au MIT, marquant son refus de l’évolution des règles en matière logicielle, marquant l’obligation de « *rejoindre le monde du logiciel propriétaire* » et ses « *accords de non-divulgation* » qui empêchent d’ « *aider les autres programmeurs* » et de contribuer à l’avènement d’ « *un monde où toute communauté coopérative serait interdite, un monde où des murs de plus en plus hauts, ceux des différentes firmes, sépareraient les différents programmeurs (ou programmeurs-utilisateurs), les isolant les uns des autres* » (Stallman cité par Mangolte 2013b, p. 8). Le projet sous licence libre, GNU (pour « *GNU’s Not Unix* », un système d’exploitation compatible Unix) voit son acronyme affirmer un peu plus son opposition « *éthique et politique* » à « *l’évolution en cours dans la communauté d’UNIX, avec la fermeture d’une partie des codes, la division de la communauté et l’apparition de différents UNIX propriétaires* ». Le « *free software* » a deux objectifs et renvoie à un ensemble de libertés : d’abord, constituer un « *stock de ressources logicielles* » réutilisable par tous librement, ensuite fixer des règles explicites de leur mise en commun, par la définition des droits et obligations des usagers « *en matière de modification, de transformation et de redistribution des programmes* » (*Ibid.*, p. 9). La liberté logicielle se définit à l’aune de quatre libertés irrévocables : celle d’exécuter le programme qu’importe l’usage, celle d’en étudier le fonctionnement et de le modifier à sa guise et l’améliorer, celle d’en redistribuer (donner et vendre) des copies en distribuant ces améliorations au public (Moreau 2019, p. 2). Les licences dites *copyleft* sont héréditaires, elles imposent que toute redistribution se fasse sous la même licence ; ce faisant, elles sont incompatibles avec les codes propriétaires. En 1998, afin de prendre ses distances avec l’ « *idéologie* » de Stallman et de la *Free Software Fondation*, l’ « *Open Source Initiative* » voit Bruce Perens établir une nouvelle définition en dix critères (Mangolte 2013, p. 11), qui conduit à la création de licences plus « *permissives* », permettant que des modifications soient rendues propriétaires (Moreau 2019, p. 4). Aujourd’hui, l’éventail de licences libres disponibles est large et à chacune sont attachés des droits et des obligations différents en termes d’usage, de réutilisation et redistribution (voir Coriat 2010; Mangolte 2013; Coriat et Broca 2015; Moreau 2019)

<sup>86</sup> Licence de logiciel libre dite « *permissive* » et ouverte aux entreprises, qui limite les restrictions de réutilisation, particulièrement l’absence d’ « *héritage* » pour les ré-usages, qui rend les changements de licence possibles.

Wirdum 2020)<sup>87</sup>, ou les diverses expériences qui lui succèderont : le « *CyberCash* » lancé en 1994 (CNET News 1997; Trombly 2001), l'*E-Gold* en 1996 (Lars 2020b), le *Liberty Dollars* en 1998 (Lach 2011) ou le *Liberty Reserve* en 2006 (Seibt 2013). Ces systèmes reposent encore sur des architectures centralisées, condition nécessaire aux paiements et règlements, ce qui constitue aussi leur talon d'Achille : le centre concentrant tous les pouvoirs est aussi en dernière instance un « *point unique d'échec* » (Nakamoto cité dans Champagne 2014, p. 101) : l'atteindre lui, c'est atteindre l'ensemble du réseau\*. Ces expériences se sont toutes soldées, à plus ou moins courte échéance, par des échecs : faillites – pour *Digicash* et *CyberCash* - ou fermetures judiciaires. On ne badine pas avec les régulations monétaires et financières, et leurs instigateurs se verront inculpés de blanchiment d'argent et d'exploitation illégale d'entreprise de transfert de fonds – pour *E-Gold*, *Liberty Dollars*, et *Liberty reserve* (Lars 2020b; Lach 2011; Seibt 2013). Ensuite, c'est un même problème qu'a révélé crûment la fermeture de Napster (1999-2001), la première plateforme centralisée d'échange de fichiers : c'est le centre qui fut fermé afin de censurer le service offert permettant de contrevenir éventuellement à la propriété intellectuelle<sup>88</sup>. Ces échecs incitent certains acteurs, comme B. Cohen, fondateur de *BitTorrent*, à développer des protocoles pair-à-pair (P2P) plus résilients et difficiles à atteindre. Ces expériences convainquent Nakamoto de l'inanité intrinsèque des designs centralisés<sup>89</sup> : si les « *gouvernements sont bons pour couper les têtes d'un réseau\* contrôlé centralement comme Napster, [...] les réseaux\* P2P purs comme Gnutella et Tor semblent tenir le coup* » (Nakamoto 2008a). D'ailleurs, des *cypherpunks* et *cryptoanarchistes* notoires, d'obédience libérale/libertarienne assumée, avaient pensé avant lui à la création de monnaies numériques décentralisées via des architectures P2P. Dès 1998, Wai Dai, « fasciné » par la crypto-anarchie de May, présente le concept de « *b-money* », reposant sur un système distribué en P2P et intraçable, utilisant des clefs cryptographiques ; la création monétaire y serait liée à la diffusion d'une « *solution à un problème de calcul* » au sein d'un réseau\* où « *chaque participant tient une base de données (distincte) sur la somme d'argent appartenant* » à chacun, les règles protocolaires définissant « *la manière dont ces comptes sont mis à jour* » (Dai 1998). Plus tard, Nick Szabo, figure *Cypherpunk* à qui est attribué le concept de « *Smart contract\** » (Narayanan et Clark 2017, p. 20-21) développe de 1998 à 2005 une idée proche avec « *Bit gold* » : à l'architecture P2P s'ajoute explicitement une PoW\* comme solution à opposer au *problème de double dépense\** (le système HashCash de A. Back étant cité, Szabo 2005; Szabo 2008; Van Wirdum 2018). Ces deux propositions auraient été nourries des échanges entre des CypherPunks et des économistes réputés

<sup>87</sup> D. Chaum, co-fondateur de l'*International Association for Cryptologic Research*, est cité comme le « *père de l'argent numérique* » : ses recherches ont contribué aux questions « d'anonymat » (D. Chaum 1981, cité par Narayanan et Clark 2017, p. 18; Castor 2017; McCormack et Van Wirdum 2020) et, dès 1985, il endosse la casquette d'entrepreneur innovateur pour lancer l'entreprise *DigiCash*. Celle-ci émettait pour le compte de ses clients des unités monétaires anonymes - les *CyberBucks* - permettant des règlements (Chaum 1994; Chaum 1996; Van Wirdum 2018; Lars 2020c). Le système nécessite que l'entreprise dispose de passerelles avec le système bancaire traditionnel et, en 1995, l'entreprise obtient une première licence - avec la *Mark Twain Bank* de St Louis - , en 1996, c'est la Deutsche Bank qui se joint au projet, suivi du *Crédit Suisse*, puis de l'*Australian Advance Bank*, de la *Norske Bank* de Norvège et de la *Bank Austria*. L'entreprise *DigiCash* s'est même vu négocier - sans succès - des accords avec ING et ABN Amro, Visa, Netscape et Microsoft (voir Van Wirdum 2018). Malgré cet intérêt de la part de grandes banques, l'entreprise fera faillite en 1998. Nakamoto y fait référence ici : <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493> (Nakamoto 2009c) [consultation au 25/09/2020].

<sup>88</sup> En juin 1999, S. Fanning, étudiant américain de 18 ans, lançait sur son site download.com le premier programme d'échange de fichiers intitulé *Napster*. Le site, comptant 60 millions d'utilisateurs dans le monde est fermé en juillet 2001, suite à une plainte de l'association américaine des artistes (la RIAA).

<sup>89</sup> Pour Nakamoto, « *toutes les entreprises qui ont fait faillite depuis les années 1990* » autour des monnaies électroniques étaient condamnées par une centralisation qu'il vise à dépasser : si l'*« ancienne mint centrale chaumienne [...] était la seule chose disponible [...] ]. J'espère qu'il est évident que seule la nature centralisée de ces systèmes les a condamnés. Je pense que c'est la première fois que nous essayons un système décentralisé, non basé sur la confiance.* » (Nakamoto 2009b) Voir le post original : <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493> [consultation au 25/09/2020]

pour leurs positions libérales (G. Selgin et L. White), au sein d'une liste de diffusion *ad hoc*, créée par Szabo en 1994 ("Libtech-1", en rouge dans la chronologie, McCormack et Szabo 2019; Lars 2020a). Mais pour autant, *B-money* et *Bitgold*, dont Nakamoto reconnaît explicitement l'inspiration (Nakamoto 2010d<sup>90</sup>), restent des propositions sans implémentation.

En leur temps, ces propositions manquent des ressources qui les rendront possibles. Les années 2000 changent la donne avec des avancées dans le domaine logiciel (avec *Bittorrent*, *Tor*, *Gnutella*) et matériel (augmentation des puissances de calcul et des capacités de traitement). L'ubiquité et l'ouverture à tous, d'abord limitées aux codes sources, s'étendent aux réseaux\* et à leurs données endogènes\*. Cette sédimentation composite au long cours explique pourquoi « *Bitcoin a mis si longtemps à être inventé* » : pour s'étayer, il attendait des fondations faites de recherches fondamentales et appliquées, dont Nakamoto a une connaissance fine (Narayanan et Clark 2017, p. 3).

### Une création hétérodoxe, entre recherche académique et recherche appliquée

Le substrat idéologique et les expériences pratiques précédentes sont essentiels pour comprendre l'éviction principielle des « intermédiaires », des centres et points de « contrôle », comme la défiance envers les États et leurs régulations, au cœur du design de Bitcoin. Pour autant que pointer les inspirations politiques de son créateur assoit la démonstration d'une nature politique de Bitcoin, on ne peut retenir ce terreau idéologique comme unique (comme le fait Gerd 2017, Chap. 2; ou Columbia 2015). Bitcoin ne peut être réduit aux « *déterminations sociales* » et à l'idéologie de son créateur (impossibles à établir parfaitement par ailleurs) sans quoi, cela nous priverait de la capacité « *de rendre compte des destins différenciés* » (Akrich 1989, p. 31-32) que, en tant qu'objet sociotechnique, il a pu et pourrait connaître. Ses filiations idéelles ne suffisent pas à expliquer son contenu matériel, qui dépend aussi de recherches fondamentales et appliquées. Nous rappellerons ces inspirations scientifiques, sans pour autant verser dans la tentation inverse de rabattre Bitcoin sur un creuset techno-scientifique, garantie de sa légitimité, de son indépendance et de sa neutralité. Car le cas Bitcoin permet d'éclairer singulièrement une thèse centrale des études de STS, un « *mélange d'intérêts sociopolitiques et cognitifs* » se trouvant au cœur de la « *recherche scientifique* » : les CM représentent une nouvelle occasion d'étudier la façon dont ces intérêts hybrides influencent « *jusqu'au sein de l'arène scientifique et [de créer] un rapport de force favorable à certaines des thèses ou des interprétations proposées* » (Callon 2006a, p. 37, 59).

Le second lignage de Nakamoto, qui complète son lignage *Cypherpunk*, le situe encore « *sur les épaules de géants* » puisque « *presque tous les composants techniques du Bitcoin sont issus de la littérature universitaire des années 1980 et 1990* » (Narayanan et Clark 2017, p. 1). Pour preuve, sur les 8 références bibliographiques du WP\*, seule la référence à « *b-money* » de Dai 1998 n'est pas académique. Les 7 autres traitent de serveur d'*horodatage*\* (pour trois d'entre-elles), de chaîne de bit (*bit string*), de *fonction de hachage*\* et de leurs usages potentiels et de probabilité appliquée

---

<sup>90</sup> Il y écrit que « *Bitcoin est une mise en œuvre de la proposition b-money de Wei Dai* », <http://weidai.com/bmoney.txt> sur les Cypherpunks; <http://en.wikipedia.org/wiki/Cypherpunks> en 1998 et de la proposition *Bitgold* de Nick Szabo <http://unenumerated.blogspot.com/2005/12/bit-gold.html> (Nakamoto 2010d) [consultation au 27/09/2020].

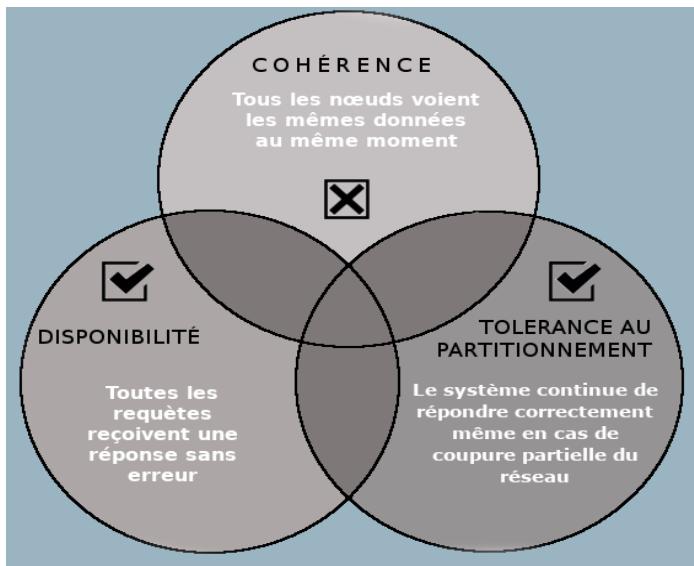
(Nakamoto 2008c, p. 9)<sup>91</sup>. Ces papiers travaillent sur des problématiques spécifiques aux réseaux\*, particulièrement distribués, et contribueront à l'émergence des solutions de consensus distribué des protocoles dits « classiques » (Bano; et al. p. 3). Le champ des protocoles distribués et le champ monétaire rencontre des problématiques similaires. L'érection séculaire des systèmes hiérarchisés modernes répond en grande partie aux problèmes multidimensionnels que sont l'unicité et la stabilité du système de paiement, dont le faux monnayage est une des manifestations (Blanc et Desmedt 2010; Gilbert et Helleiner 1999). L'identification certifiée des parties au système monétaire (des utilisateurs finaux aux entités d'émissions autorisées) et le contrôle donné à une autorité centrale unique sont des réponses à ces problèmes. Comme le fut, dès le VIII<sup>e</sup> siècle avant J.-C., la première monnaie frappée et étalonnée au poids attribuée, suivant Hérodote, au Roi de Lydie (Galbraith 1976, Chap. 2)<sup>92</sup>. Les monnaies numériques n'y dérogent pas : cela s'inscrit dans des problématiques anciennes en science informatique. Nakamoto est informé des recherches précédentes et des risques qu'encourent les systèmes de protocoles de registre\* distribué P2P (*sybille attaque* et *double dépense*, cf. *infra*). Et c'est autour de ces problèmes qu'il réarticule des composants sociotechniques existants afin d'élaborer une solution radicalement différente des précédentes (Nakamoto 2008c). Constituer un réseau\* distribué ouvert et fonctionnel d'*archivage partagé\** renvoie à un problème posé dès 1970, sous le nom de « *tolérance aux fautes byzantines* », une version globale du « *problème des deux généraux* » (Champagne 2014, dit aussi « *problème des généraux byzantins* », théorisé par Lamport & al, 1982, cité par Narayanan et Clark 2017, p. 9 et Rauchs et al. 2018, p. 15). Celui-ci est simple : « *deux personnes (ou plus) ont besoin de partager des informations dans un environnement communicationnel peu fiable, où les messages envoyés peuvent être perdus ou falsifiés* » (Champagne 2014, p. 67). Cet environnement est dit « *hostile* » (*adversarial environnement*) au sens où des parties prenantes « *inconnues* » peuvent y prendre part librement, induisant de manière malveillante ou non, des comportements imprévus (déconnexions d'une partie des nœuds\*, envoi de message invalide, détournement du protocole et des voies de consensus).

---

<sup>91</sup>En l'occurrence : H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements" In 20th Symposium on Information Theory in the Benelux, May 1999 ; S. Haber, W.S. Stornetta, "How to time-stamp a digital document" In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991; et D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping" In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993; S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997; A. Back, "Hashcash - a denial of service counter-measure" <http://www.hashcash.org/papers/hashcash.pdf>, 2002 ; R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980 ; W. Feller, "An introduction to probability theory and its applications," 1957. (Nakamoto 2008c, p. 9)

<sup>92</sup>Pour Galbraith (1976, Chap.2), cette lutte contre la dépréciation monétaire consécutive aux fraudes est au cœur même de l'histoire de la banque, comme avec les premières banques publiques qui offraient des garanties collectives (précisément municipale) : toute monnaie était acceptée à sa valeur métallique intrinsèque et, par suite, transformée en « bonne monnaie » de titre et poids légal, suivant le paiement de frais (de brassage et de monnayage) à cet émetteur.

**Figure 2 : Le théorème d'impossibilité de CAP**



Source : Rolland Maël

Ces systèmes font face au théorème d'impossibilité de CAP (pour « Coherence, Availability and Partition tolerance » ou théorème de Brewer, cf. Figure 2) stipulant que tout système de calcul distribué ne peut, à un instant t, garantir simultanément les trois propriétés que sont : (1) la disponibilité\*, qui permet que chaque demande soit toujours traitée par le système ; (2) la *tolérance à la partition*\*, c'est-à-dire que le service fonctionne toujours même si quelques nœuds\* échouent ou trichent ; et (3) la cohérence permettant que tout nœud\* du système accède aux mêmes données au même moment (Teruzzi 2016b; Kernfeld 2016). Cela induit deux risques centraux pour un protocole de registre\* distribué voué à tenir le rôle de système monétaire et de paiement.

À la *double dépense* qui permettra à une partie de payer plusieurs fois avec les mêmes UCN\* – jouant sur la partition et la cohérence du système (Bano; et al. 2017, p. 2) -, s'ajoutent les *attaques sybilles*, où une même entité crée une multitude de nœuds\* au sein d'un système afin de « contourner les garanties de consensus » en obtenant la majorité (Narayanan et Clark 2017, p. 11; Bano; et al. 2017, p. 12). Comment les systèmes de registre\* distribué font-ils face à des informations contradictoires en restant viables et fonctionnels ? Comment des machines distribuées s'entendent-elles sur un historique transactionnel commun ? Comment évitent-elles la tricherie ? Pour que toute requête soit authentique, valide et prise en compte par tous les participants du système et que soit ainsi garantie l'unicité de ses informations endogènes, il faut que l'ensemble des nœuds\* suive des règles similaires les forçant à réaliser « *les mêmes transitions d'état dans le même ordre* » sachant que, pour une CM, « *les transactions*\* sont des transitions d'état » et « *l'état à répliquer est l'ensemble des soldes* » (Narayanan et Clark 2017, p. 9-10).

Historiquement, ces problèmes ont engendré une littérature prolifique et des solutions diverses de consensus ont été développées, comme le protocole Paxos tolérant à la partition (Lamport 1989), ou les protocoles dits « PBFT » (« Practical Byzantine Fault Tolerance », suivant M. Castro et B. Liskov 1999) intégrant des risques plus étendus (Narayanan et Clark 2017; Bano; et al. 2017; Rauchs et al. 2018). Ces solutions de consensus « classique » reposent toutes sur une logique similaire : le réseau\* est constitué statiquement en « groupes fermés », et chaque participant à ce comité est authentifié et accrédité *a priori* (d'où l'appellation « permissioned », Bano et al. 2017, p. 9). Cette architecture prévient contre les risques d'attaque sybille et la double dépense\*, puisque le protocole spécifie l'« accord de plusieurs nœuds\* sur une valeur » à « ajouter à la blockchain », généralement via l'élection par roulement, parmi les nœuds\* de ce comité, d'un « leader » produisant les données que répliqueront les autres (Rauchs et al. 2018, p. 62). Ainsi, les droits d'écriture sur le livre comptable sont réservés à des membres de confiance, sanctionnables en cas d'abus, qui traitent les demandes de changement d'état du registre\* et produisent de nouvelles versions des données canoniques. Pour Nakamoto, ces « *solutions habituelles* » de consensus « classique », consistant « à confier à une société de confiance disposant d'une base de données centrale le soin de vérifier les doubles dépenses », ne sont pas acceptables (Nakamoto 2009c).

Malgré sa connaissance fine du champ de la cryptographie\*, de la science informatique et des réseaux\*, « *Nakamoto ne s'est pas soucié de l'examen par les pairs universitaires* ». Et son rejet des solutions de consensus « classique » fondées sur le « *modèle de confiance* » (*Ibid.*) qu'il honnit, le conduit à produire un WP\* qui, « *malgré le pedigree de beaucoup de ses idées, était plus nouveau que la plupart des recherches universitaires* » (Narayanan et Clark 2017, p. 23). Du côté des universitaires, ils ont en retour majoritairement « *ignoré le Bitcoin* » (*Ibid.*). D'où un statut d'« *outsider académique* » hétérodoxe : vers août 2008, il « *a contacté des acteurs clés [A. Back, W.Dei, que nous présenterons ci-après] au sujet des antériorités et de leur citation correcte [...], dont il n'était pas (pleinement) conscient à l'époque [et] l'accueil initial sur ce forum de cryptographes en novembre 2008 a été extrêmement sceptique ; seule une poignée d'adeptes de la première heure [H. Finney, M. Malmi, entre autres ] ont réagi [...] ; encore moins de programmeurs ont rejoint Satoshi Nakamoto dans le développement de Bitcoin* » (Ducrée 2022, p. 4). De fait, Nakamoto propose aux problèmes précédents une solution controversée : quelques-uns soulignent qu'elle fonctionne en pratique, mais une majorité de chercheurs fait valoir qu'elle ne peut « *fonctionner, en se basant sur des modèles théoriques ou des expériences avec les systèmes antérieurs* » (Narayanan et Clark 2017, p. 23-24). D'où une relégation hors du champ scientifique de Bitcoin par nombre d'académiques. Certains parlent même de fraude<sup>93</sup>. Ainsi, comme innovation, Bitcoin est un objet controversé qui rend « *visibles les territoires où les techniques et les sciences ne sont pas constituées, où l'on débat pour savoir ce qui est acquis et ce qui ne l'est pas, pour délimiter les frontières entre recherche fondamentale et recherche appliquée, où l'on se bat pour définir et articuler logiques socio-économiques et logiques techniques, où l'on définit l'identité des acteurs impliqués, où l'on négocie les intérêts, les problèmes légitimes, la répartition des tâches et où, même partiellement, les divisions et catégories imposées sont remises en cause sous la poussée de nouveaux acteurs.* » (Callon 2006a, p. 25). La controverse autour de la solution de Bitcoin aux problèmes posés aux monnaies numériques fait ainsi « *éclater l'illusion d'une pure nécessité technique* » et rend visible l'existence de divergences au sein de la communauté des chercheurs et techniciens (*Ibid.*), démontrant comment problèmes et solutions « *techniques* » renvoient à des visions du monde irréconciliables, socio-politiquement fondées.

### I.1.2 Bitcoin : une chimère théorico-pratique très politique

Bitcoin s'inscrit dans une histoire longue des idées et des techniques. Mais, comme tout innovateur, Nakamoto affronte un « *labyrinthe* » fait de contraintes diverses : gît, entre lui « *et ses buts, une multitude d'objets, de souffrances, d'apprentissages* », l'obligeant « *à ralentir, prendre un détour, puis l'autre, à perdre de vue le but initial, à revenir, à tâtonner* » (Latour 2000, p. 46). Pour inspirante que soit cette histoire, elle n'offre encore à Nakamoto ni design architectural, ni code logiciel prêt à l'emploi<sup>94</sup>. Pour l'un et l'autre, l'inventeur va devoir opérer des compromis et arbitrages et fixer des choix technologiques (*langage de programmation\**, bibliothèques logicielles, etc.), des paramètres et variables suivant des contraintes *ad hoc* – théoriques, mais aussi empiriques. Le design de Bitcoin suppose la fixation de statuts et de rôles d'acteurs, tout comme les modalités de leurs interactions *on chain\**. Ces arrangements sociotechniques sont autant de régulations définissant ce qui, *on chain\**, est possible et impossible, honnête ou non<sup>95</sup>, incité ou sanctionné.

<sup>93</sup> Le chercheur en informatique J. Stolfi pour qui « *tout chercheur en science informatique devrait être capable de voir que les cryptomonnaies sont des systèmes de paiement totalement dysfonctionnels et que la "technologie blockchain\*" (y compris les "contrats intelligents") est une fraude technologique* » (Colomé 2022).

<sup>94</sup> Notre enquête fait ressortir que la conception d'un système et l'implémentation des codes logiciels correspondent à des activités, compétences et acteurs distincts (cf. V. Zamfir, chercheur en conception qui reconnaît ne pas savoir coder, annexe n°5).

<sup>95</sup> Nakamoto utilise ce terme dans le WP\* (16 occurrences au total, soit deux par page en moyenne).

Impossible de reconnaître le caractère « révolutionnaire » de Bitcoin en détournant l'attention de ce qui fait le *saut qualitatif* de Nakamoto.

## Des composants sociotechniques anciens singulièrement recomposés

Les dispositifs au cœur du protocole Bitcoin renvoient aux mathématiques et à une de leurs sous-disciplines appliquées, la cryptographie\*. Cette dernière recouvre un ensemble de techniques et d'algorithmes, permettant de chiffrer/déchiffrer des informations et pouvant être mobilisés pour des applications variées (que d'ailleurs, les CM aident encore à découvrir<sup>96</sup>). Loin de ne faire que « *cacher* »<sup>97</sup>, ces fonctions cryptographiques peuvent être instrumentées à des fins d'authentification et de certification, mais aussi de structurations des données comme de mécanismes désincitatifs. Il est significatif que, historiquement, la cryptographie\* ait d'abord « *été monopolisée par les gouvernements à des fins d'espionnage et de protection des secrets d'État* » (Jeong 2013, p. 9) avant son extension au secteur privé, en partie grâce au travail des *Cypherpunks* précédents (Castor 2017; McCormack et Van Wirdum 2020). La place centrale que prennent ces technologies dans Bitcoin explique l'appellation même de CM, que nous reprenons à notre compte : c'est la cryptographie\* qui garantit les propriétés individuelles et collectives visées. Pour composer Bitcoin, Nakamoto infère de sa contrainte originelle de décentralisation une série de propriétés qu'il doit porter, et sélectionne les composants sociotechniques dont il dispose grâce aux travaux des précurseurs évoqués.

Un protocole, même ouvert à tous, se doit d'identifier ses membres, même lâchement. À la place des arrangements impliquant des tiers de confiance qui résolvent habituellement les problématiques d'authentification et d'identité des acteurs, Bitcoin et les CM s'appuient sur l'usage *individuel* d'outils d'authentification cryptographique\*. L'authentification cryptographique\* renvoie à un ensemble de techniques anciennes, permettant de prouver l'identité des contreparties comme l'intégrité des données échangées. L'utilisation de la cryptographie asymétrique, à couples de clefs publiques/privées<sup>98</sup>, est exposée par Diffie-Hellman dès 1976 (le chiffrement RSA, pour « Rivest, Shamir et Adleman », fut la première mise en œuvre officielle, Castor 2017). Ces clefs sont « inverses fonctionnelles » : les informations chiffrées par la clef publique ne peuvent être déchiffrées que par la clef privée et inversement (Qureshi 2019, Annexe n°V.2). C'est précisément la diffusion de ce type de chiffrement en protection de la confidentialité des mails qui a valu à P. Zimmermann les déboires exposés précédemment. L'usage de cette cryptographie\* asymétrique comme « *pseudonyme numérique* » et « *formes d'expression de l'identité* » était déjà proposé par D. Chaum<sup>99</sup>. Ces technologies étaient préalablement mobilisées par des systèmes centralisés, comme l'*E cash* et son système de « signatures aveugles » (Chaum 1982), et ne sont donc pas propres aux systèmes décentralisés. Les acteurs bancaires et financiers s'en servent eux-mêmes, mais, dans ce cas, les tiers de confiance en conservent la maîtrise pour le compte de client dépendant. Or, Nakamoto enjoint chaque utilisateur à rejeter cette dépendance : « *Be your own Bank* » clament

---

<sup>96</sup> Bitcoin et les CM ont revitalisé le domaine des systèmes distribués et conduisent à des nouvelles conceptions et à des avancées en cryptographie\* : les technologies dites de preuves à divulgation nulle (« *Zero Knowledge proof* ») sont exemplaires puisque, avant les CM, elles n'avaient « *aucun déploiement dans le monde réel* » (Bonneau et al. 2015, p. 118; Bano; et al. 2017, p. 1 et 13).

<sup>97</sup> Étymologiquement, le terme dérive de du grec “*kruptos*” (κρυπτός) signifiant « *caché* » et “*graphein*” (γράφειν) signifiant « *écrire* ».

<sup>98</sup> Le chiffrement asymétrique diffère du chiffrement symétrique en ce que les co-échangistes disposent d'une seule et même clef servant à la fois pour chiffrer et déchiffrer les messages (Qureshi 2019). L'unique façon de communiquer cette clef « *en toute sécurité était donc de se rencontrer physiquement* », ce qui change « *avec la cryptographie\* à clef publique, qui, pour la première fois, [permet] de communiquer en toute sécurité, [sans jamais s'être] rencontrées* » (McCormack et Van Wirdum 2020)

<sup>99</sup> May en faisait la clef d'une souveneté individuelle hors État (May 1994, p. 294).

les *coiners*<sup>\*</sup>, « *not your key, not your coin* » ! La souveraineté individuelle suppose que les individus atomisés administrent, chacun de leurs côtés, leurs identités et leurs fonds. Comme pour May, l'authentification cryptographique devient clef d'une souveraineté individuelle hors État (May 1994, p. 294), où chacun est responsable en propre, avec les risques que cela comporte.

La chose fondamentale ici est que, dans les paiements, l'identité « réelle » des coéchangistes brille par son absence (Narayanan et Clark 2017, p. 19). Cette identité est « *exogène* » (Rauchs et al. 2018, p. 59) au protocole qui, de manière endogène, ne reconnaît formellement que des clefs cryptographiques et des adresses qui en dérivent, occultant les protagonistes réels. La circulation monétaire *on chain*<sup>\*</sup> relève de ces clefs uniquement : elles seules *agissent* lors des transactions<sup>\*</sup> via la production des signatures d'ordre de cession d'UCN<sup>\*100</sup> (Bonneau et al. 2015, p. 3). Ces clefs cryptographiques sont pour l'utilisateur un identifiant unique : il diffuse sa clef publique à qui de droit et elle sert à déchiffrer/authentifier les messages qu'il transmet, signe / chiffre avec la clef privée correspondante. Attention, si la clef publique peut être partagée, la clef privée doit au contraire être conservée secrètement et de manière sécurisée. En cas de divulgation, toute personne en sa possession a la maîtrise des fonds. Bitcoin utilise différentes solutions de chiffrement pour créer des couples de clefs privées / publiques et en dériver des adresses publiques suivant les propriétés de sécurité et de lisibilité désirées par Nakamoto<sup>101</sup>. Un portefeuille<sup>\*</sup> de CM – quelle que soit sa forme - n'est ainsi pas autre chose qu'un logiciel capable de générer, de stocker et d'administrer des couples de clefs publiques /privées pour transférer ses actifs digitaux suivant les règles protocolaires considérées.

Le protocole dispose ainsi de quoi identifier ses membres. Il faut encore trouver des solutions pour établir une structure de données répondant aux questions ouvertes par la production collective d'un registre<sup>\*</sup> de transactions<sup>\*</sup> canonique commun. Là encore, en ce qui concerne les propriétés désirables que le « *livre comptable* » doit avoir en environnement adverse, Nakamoto les infère de la contrainte de décentralisation. Sa base de données transactionnelles doit être « *immutable ou, plus précisément en ajout seulement* [« *append only* »] ». Elle doit ne permettre que d' « *ajouter de nouvelles transactions*<sup>\*</sup>, mais pas supprimer, modifier ou réorganiser les transactions<sup>\*</sup> existantes » (Narayanan et Clark 2017, p. 4). Simultanément, elle doit permettre aux utilisateurs « *d'obtenir à tout moment un condensé cryptographique succinct de l'état du grand livre* », évitant qu'ils aient à en « *stocker l'intégralité* », tout en garantissant que, en cas d'altération maligne, la manipulation serait détectée (*Ibid.*). Pour obtenir ces propriétés, Nakamoto part des fonctions de hachage<sup>\*</sup> (voir Annexe n°8) et des travaux concernant leurs applications et usages. Bitcoin y puise de quoi authentifier et certifier l'intégrité de données endogènes<sup>\*</sup>, les structurer (fonctions de *hash*<sup>\*</sup>, horodatage<sup>\*</sup> lié et *arbre de Merkle*<sup>\*</sup>), mais aussi désinciter certains comportements numériques (du

---

<sup>100</sup> Une transaction spécifie un « *hachage d'une clef publique* » qui est vérifié suivant « *une routine de validation*<sup>\*</sup> de signature ». Il s'agit en général du script « *scriptPubKey* » d' « *une transaction "pay-to-pub-key-hash"* [où] la totalité de la transaction de rachat doit être signée à l'aide d'une clef avec le hachage spécifié » (Bonneau et al. 2015, p. 3). Si la majorité des transactions Bitcoin sont de ce type, d'autres types plus complexes existent, permettant des usages applicatifs diversifiés (cf. portefeuilles<sup>\*</sup> multisignatures ou protocoles de seconde couche, traités ci-après).

<sup>101</sup> Bitcoin utilise le chiffrement asymétrique ECDSA (*Elliptic Curve Digital Signature Algorithm*) pour la création de couples de clefs privées-publiques : ces couples sont réputés uniques, car le risque de « collision », c'est-à-dire qu'un même couple de clefs soit généré par un autre utilisateur, est infinitésimal compte tenu des propriétés mathématiques des algorithmes utilisés et de l'état des connaissances. Dans un second temps, Bitcoin utilise conséutivement deux fonctions de hachage (*ripemd-160* et *Base58Check*) pour la dérivation d'adresse : en plus de leur rôle de compression des données, offrant une meilleure lisibilité (comme l'explique Nakamoto dans les codes sources de la première version client, [https://en.bitcoin.it/wiki/Base58Check\\_encoding](https://en.bitcoin.it/wiki/Base58Check_encoding)), ce traitement offrirait une résistance aux ordinateurs quantiques dont Nakamoto anticipe le développement et qui, en l'état des connaissances, compromettaient la sécurité de nombreux outils cryptographiques (Rykwalder 2014; Qureshi 2019, voir Annexe n°7).

fait des coûts computationnels que leur usage induit pratiquement, comme la « preuve de travail\* » ou PoW\*).

En soi, une fonction de hachage\* ne fait que chiffrer, en sens unique, des données brutes entrantes (un document, une image, des codes logiciels, etc.) sous la forme d'une *empreinte numérique\** de taille fixe prédéterminée (exemple de la fonction SHA 256 en Annexe n°8). Ce simple usage permet déjà à toute personne disposant des données entrantes de vérifier leur intégrité (le hash\* transmis doit correspondre à celui que la personne réalise). L'arbre de Merkle\* renvoie à un usage similaire, mais plus complexe, de ce type de fonction : il permet de structurer un ensemble de données, potentiellement volumineux, en les réduisant en un hash\* unique appelé « hash\* sommet » (ou “*Merkle root*”, voir Annexe n°9) qui permet là encore d'en vérifier l'intégrité. Cette technique, proposée par R. Merkle (pionnier de la cryptographie\* dont dérive le nom de l' « arbre ») en 1980, visait à faciliter la production de « *répertoire public de certificats numériques* » de sites Internet (*Ibid.*, p. 8). Pour son modèle, Nakamoto choisit une structure de données dite d'« Horodatage\* lié », empruntée aux chercheurs Haber et Stornetta<sup>102</sup> (Nakamoto 2008c, p. 9). Les données transactionnelles y sont liées entre elles par « *des hachages plutôt que des signatures [...] plus simples et plus rapides à calculer* » ; au lieu d'être chaînées « *individuellement* », ce qui peut être inefficace, elles sont « *regroupées [...] en blocs* », ce qui les dote toutes du « *même horodatage\** » ; enfin « *à l'intérieur de chaque bloc, les données [sont] reliées entre elles par un [...] arbre de Merkle\**, plutôt que par une chaîne linéaire »<sup>103</sup> (Bano; et al. 2017, p. 2). La répétition d'un tel schéma « *dans chaque bloc* » produit « *une chaîne de hachage dans laquelle chaque bloc vérifie implicitement l'intégrité de la chaîne entière qui le précède, et la falsification des données précédentes est détectable* » (*Ibid.*). Cette structure offre des « *propriétés importantes* » : le hachage du dernier bloc – l'*en-tête d'enregistrement\** – est un condensé unique où toute modification de l'une des transactions\* (« feuille ») modifie « *jusqu'à la racine du bloc et [les] racines de tous les blocs suivants* » ; ainsi, avec simplement la connaissance du dernier hachage valide, tout acteur peut « *télécharger le reste du grand livre depuis une source non fiable et vérifier qu'il n'a pas changé* » (Narayanan et Clark 2017, p. 7). Dans le même sens, il est facile de « *prouver qu'une transaction\* particulière est incluse dans le grand livre* » sans avoir à divulguer beaucoup d'informations (*Ibid.*).

Enfin, ces fonctions de hachage voient avec Bitcoin leurs usages instrumentés pour désinciter des comportements non souhaités : c'est ce que recouvre l'appellation Preuve de travail\* (*PoW\**), qui implique un travail computationnel coûteux pour produire une empreinte cryptographique. À puissance de calcul donnée, la nature probabiliste des fonctions permet de déterminer l'occurrence d'un hash\* dont les propriétés particulières servent de cible (cf. le hash\* sommet d'un enregistrement doit débuter par un certain nombre de 0, qui renvoie à un niveau de difficulté<sup>104</sup>). L'obtention d'un hash\* cible requérant (en moyenne) un temps de traitement donné, cela permet

---

<sup>102</sup> Leurs travaux portaient sur les questions d'horodatage\* et de « *notariat numérique* » de documents (brevets, contrats commerciaux) nécessitant une certification chronologique. Dans leur *proposition* : « *des documents sont constamment créés et diffusés. Le créateur de chaque document établit une heure de création et signe le document, son horodatage\* et le document précédemment diffusé. Ce document précédent a signé son prédecesseur, de sorte que les documents forment une longue chaîne [...]. Un utilisateur extérieur ne peut pas modifier un message horodaté puisqu'il est signé par le créateur, et le créateur ne peut pas modifier le message sans modifier également toute la chaîne de messages qui suit. Ainsi, si une source de confiance (par exemple, un autre utilisateur ou un service d'horodatage\* spécialisé) vous donne un seul élément de la chaîne, toute la chaîne jusqu'à ce point est verrouillée, immutable et ordonnée dans le temps* ». (Narayanan et Clark 2017, p. 4-5)

<sup>103</sup> Nakamoto suit les optimisations proposées par Haber et Stornetta, qui ont été introduites indépendamment par J.Benaloh et M. de Mare en 1991 (Narayanan et Clark 2017, p. 6).

<sup>104</sup> La difficulté mesure le degré de difficulté pour "miner" un entête valide, elle correspond au nombre estimé de hachages nécessaires pour trouver un hash inférieur ou égal à une cible donnée. Ainsi, la PoW\* « *consiste à rechercher une valeur qui [...] hachée [...] commence par un nombre de zéro bits.* » (Nakamoto 2008c).

d'établir le temps de chaque cycle de mise à jour du registre\* avec une époque de traitement des transactions\*, fixée à dix minutes en moyenne pour Bitcoin. L'usage de la PoW\* fut proposé à l'origine comme protection des boîtes mail contre les *spams*. Dans ce cas, chaque destinataire de courriels demande à l'envoyeur la transmission d'un *hash*\* cible (c'est-à-dire ayant demandé un certain niveau d'effort) avant de l'accepter (Dwork & Noar 1992, Back 1997, cité dans (*Ibid.*, p. 11-12). Ce type d'arrangement est aussi mobilisé contre les attaques par déni de service\* (DOS). Celles-ci saturent un serveur par l'envoi d'un très grand nombre de requêtes. À chaque fois, l'usage de la PoW\* permet de filtrer les comportements jugés souhaitables : pour l'utilisateur « normal », il sera simple et rapide de réaliser cette PoW\*, mais un attaquant, avec ses millions de courriels ou requêtes, devra mettre en œuvre une grande quantité de ressources.

Nakamoto trouve donc dans la cryptographie\* de quoi identifier les membres du réseau\* et une structure de données distribuée potentiellement utilisable. Mais son innovation radicale réside moins là que dans l'usage qu'il fait de la PoW\*, qui résout, sans passer par les solutions de consensus « classique », les problèmes précédemment évoqués (double dépense et sybille attaque). Les signatures numériques « *constituent l'une des composantes fondamentales* » de Bitcoin, permettant que « *n'importe qui [puisse] vérifier les signatures pour vérifier la chaîne de propriété* », mais reste le « *problème non résolu [de] la double dépense* », puisque « *tout propriétaire pourrait essayer de dépenser à nouveau une pièce déjà dépensée.* »<sup>105</sup> (Nakamoto 2009). Nakamoto y répondra par la réorganisation radicale des « *propriétés de sécurité* [de son système] *en ajoutant le schéma de preuve de travail\** » (Narayanan et Clark 2017, p. 5).

---

<sup>105</sup> Voir citation originale <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source> [consultation au 01/10/2020]

## L'usage de la PoW : un « jeu » d'incitations très politique

Nous l'avons vu, le bon fonctionnement de tout protocole distribué tolérant à la partition « suppose qu'une stricte majorité ou super majorité (par exemple, plus de la moitié ou des deux tiers) des nœuds\* du système soient à la fois honnêtes et fiables » (*Ibid.*, p. 11). Cela nécessite que chaque participant y trouve son compte *via* un partage des gains escomptés et coûts supportés alignant leurs intérêts à tous. Au sein des protocoles fermés à consensus « classique », cela est garanti par la centralisation. Une entité établit *a priori* une liste de participants *ad hoc*, disposant du droit exclusif en écriture dans la base de données. Ces derniers supportent les coûts opérationnels en échange d'une rétribution. À chaque cycle de mise à jour du registre, c'est parmi eux que le protocole conduit au tirage au sort d'un nœud\* *leader* unique, en charge de produire une mise à jour canonique du registre\* que les autres suivront. Nakamoto a cherché lui aussi à aligner des intérêts potentiellement contradictoires, mais en univers décentralisé. Il fait pour cela un usage inédit de la PoW\*, ce qui est sans conteste son véritable coup de « génie » (*Ibid.*, p. 15). La PoW\* lie ensemble, d'un même « coût » (computational) et suivant un rythme qu'elle sert à définir, le traitement « honnête » des transactions\* et la création monétaire, tout en assurant un archivage partagé\* à participation ouverte et une convergence consensuelle de toutes les parties prenantes sur un registre\* de compte valide, cohérent et sécurisé (c'est-à-dire protégé des *attaques sybilles* et de la *double dépense*)<sup>106</sup>. Si un tel usage de la PoW\* avait été suggéré par Dai ou Szabo, Nakamoto doit en fixer des contours précis suivant les hypothèses qui étaient les siennes. Il manie avec la PoW\* « la carotte et le bâton ». Clef angulaire du consensus de Nakamoto, la PoW\* est le cœur du système, car il fabrique un jeu d'incitations devant assurer la persuasion et l'enrôlement des opérateurs de nœuds\* et, finalement, la viabilité et la soutenabilité de Bitcoin.

La participation à Bitcoin ne repose pas sur une liste préétablie de nœuds\* au sein de laquelle est tiré au sort, par roulement, celui auquel est octroyé le droit de traiter les transactions\* et de produire le prochain *enregistrement canonique*\* pour l'ensemble des autres. En soi, une liste de participants est disponible, mais elle est dynamique et non statique, évoluant au gré des entrées et sorties de mineurs. Et si la résilience du réseau\* dépend d'une participation ouverte attirant un grand nombre de participants, cela expose en retour le protocole au risque spécifique d'attaque sybille\*. De lui découle une série d'autres risques dévoyant les propriétés du protocole.

Le premier problème concerne l'établissement des modalités « équitables » d'un tirage au sort du nœud\* *leader* pour chaque nouvel enregistrement parmi cette masse : comment garantir que le tirage soit protégé contre les *attaques sybilles* s'apparentant à une fraude ? Cela renvoie au « problème de la détermination de la représentation dans les processus de décision majoritaire. [Car] si la majorité était basée sur une adresse IP - une voix, elle pourrait être subvertie par toute personne capable d'attribuer plusieurs IP. » (Nakamoto 2008c, p. 3). En effet, s'il suffit de maintenir un nœud\* pour participer au tirage au sort et que le coût induit est faible, pourquoi ne pas accroître ses chances en multipliant les nœuds\* afin d'en opérer un nombre relativement plus grand que les autres ? Un acteur ou un groupe pourrait ainsi obtenir plus de 51% des chances, soit une majorité dans le consensus leur permettant « d'initier puis d'inverser des transactions\* et donc de dépenser deux fois, d'empêcher certaines transactions\* d'être confirmées ou d'empêcher certains ou tous les autres mineurs de miner des blocs valides » (Champagne 2014, p. 39). C'est là l'attaque dite des 51%, centrale dans le WP\* de Nakamoto (2008, explicité en Annexe n°10). Pour rendre difficilement praticable ce type d'action, Nakamoto choisit que l'élection d'un leader relève d'une course computationnelle où la PoW\* est censée incarner « essentiellement un CPU - une voix » au

---

<sup>106</sup> La façon dont ces différentes propriétés s'agencent sera clarifiée, nous l'espérons, à la fin de notre exposé. Nous ne pouvons pas déployer en une fois l'ensemble du dispositif.

tirage (Nakamoto 2008 p. 3) : c'est l'activité de « minage ». L'obtention d'un consensus sur le prochain nœud\* *leader* relève de ce processus concurrentiel intensif en calcul : « *tous les nœuds\* tentent de trouver la solution à une énigme de hachage et le nœud\* qui gagne ajoute le bloc suivant à la blockchain.* » (Bano; et al. 2017, p. 1). Dans ces conditions, la chance d'un opérateur d'être tiré au sort comme *leader*, dépend de la part de la puissance de calcul qu'il consacre à l'activité de minage, relativement à l'ensemble de celle déployée dans le réseau\* par tous les nœuds\*. Dès lors, la stratégie dominante est de concentrer toute la puissance dans un seul et même nœud, car multiplier les nœuds\* est contreproductif, diluant la puissance de calcul, donc les chances de l'opérateur.

Toutefois, l'élection d'un nœud\* *leader* ne suffit pas. Cette course à la PoW\* renvoie à un processus probabiliste qui, couplé aux performances hétérogènes du réseau\* distribué, implique une « *faible cohérence : différents nœuds\* peuvent finir par avoir des vues différentes de la blockchain, ce qui entraîne des Forks\** » (*Ibid.*), suivant que plusieurs opérateurs peuvent, dans un laps de temps court, trouver une empreinte cible valide. On retrouve là le théorème de CAP. Ainsi, Bitcoin ne garantit disponibilité\* et tolérance à la partition\* qu'au détriment de la cohérence\* : ses nœuds\* ne sont jamais cohérents à un instant t, chacun peut recevoir des transactions\* nouvelles et commencer à les traiter alors que d'autres ne les ont pas encore reçues. D'où l'apparition possible de deux enregistrements candidats valides, mais concurrents, qu'il faut départager (voir la section suivante sur les réorganisations et les « blocs orphelins »<sup>107</sup>). Les protocoles de consensus centralisés n'ont pas ce problème : un seul *leader* est élu à chaque époque/cycle et l'enregistrement qu'il produit est par définition canonique. Nakamoto va mobiliser ingénieusement la PoW\* afin de lever l'ambiguïté. Si deux nouveaux enregistrements candidats valides sont trouvés par des nœuds\* mineurs sur un laps de temps relativement proche, la règle de consensus concernant l'enregistrement à considérer comme canonique est simple et non négociable. Le protocole stipule en effet que les nœuds\* doivent toujours se tourner vers l'enregistrement le plus long (en nombre de blocs empilés) correspondant au plus lourd (en puissance de calcul accumulé), ce que le protocole établit pour chaque enregistrement sous forme d'une « *hauteur de block* » ou « *Block Height* » ; Nakamoto 2008 p. 3) : cette règle, « *incarnation de la décision majoritaire* »<sup>108</sup>, « *doit avoir le dernier mot* » puisque « *croire que la chaîne la plus longue est toujours la plus valide, quoi qu'il arrive* » est l'unique façon permettant que les participants restent « *sur la même longueur d'onde* » (Nakamoto cité par Champagne 2014, p. 50). C'est cette règle qui réconcilie le réseau\* sur un registre\* unitaire et rend les éventuelles incohérences transitoires, garantissant que les données endogènes\* restent cohérentes\* pour l'ensemble du système (cf. illustration section I.1.3). En définitive, la PoW\* sert tout à la fois à produire un consensus entre l'ensemble des nœuds\* et à le mesurer (en terme de « *hauteur de block* ») pour que tous le suivent sans ambiguïté. Cela offre « *une solution au problème des généraux byzantins, [...] la façon dont tous les problèmes de synchronisation, de base de données distribuée et de vue globale [...] sont résolus.* » (Nakamoto 2008b<sup>109</sup>). De même, la double dépense\* est empêchée, si tant est que les nœuds\* « honnêtes » détiennent plus de 51% de la puissance de calcul totale engagée dans le réseau\*. Le terme d'algorithme de consensus\* qui s'est imposé renvoie moins à l'algorithme utilisé (la fonction de hachage\* demandée, pour Bitcoin, le

<sup>107</sup>

Le

site

<https://forkmonitor.info/blocks/btc/0000000000000000004b8adbe583584f0e2370c0b752ede243535f8cf3f354>, de l'entreprise « BitMEX Research », a été mis en place afin de suivre en temps réel et de signaler l'occurrence de ce type de situation (Bier 2018; <https://twitter.com/bitmexresearch/status/1270413012260786177>) [consultation au 03/10/2020].

<sup>108</sup> « *La décision majoritaire est représentée par la chaîne la plus longue, celle qui a investi le plus d'efforts en matière de [PoW\*]. Les nœuds\* considèrent toujours que la chaîne la plus longue est la bonne et continueront à travailler pour l'allonger.* » (Nakamoto 2008c, p. 3).

<sup>109</sup> Voir le message original ici <https://satoshi.nakamotoinstitute.org/emails/cryptography/11/#selection-5.0-15.23> [consultation au 03/10/2020].

SHA 256) qu'à l'ensemble des règles et processus suivis par les nœuds\* afin d'assurer leur convergence sur un enregistrement canonique\*.

En plus de servir à conduire « équitablement » l'élection d'un nœud\* *leader* et à établir le caractère canonique des enregistrements produits, l'autre avantage est que le chaînage par PoW\* des enregistrements permet de sécuriser le contenu à travers le temps. Plus le temps passe, plus il devient difficile d'altérer les données transactionnelles passées : « *si une majorité de la puissance est contrôlée par des nœuds\* honnêtes, la chaîne honnête connaîtra la croissance la plus rapide [aussi,] pour modifier un bloc passé, un attaquant devrait refaire la PoW\* du bloc et de tous les blocs suivants, puis rattraper et dépasser le travail des nœuds\* honnêtes.* » (Nakamoto 2008c, p.3). Dans sa course à la construction d'un historique canonique de transactions\* frauduleux, la probabilité de réussite de l'attaquant diminue « *exponentiellement à mesure que le nombre de blocs que l'attaquant doit rattraper augmente* » (Nakamoto 2008c, p. 7). Ainsi, comme pour les spams et les attaques DOS\*, Nakamoto use de la PoW\* contre les *attaques sybilles* et la double dépense comme d'une désincitation. Cependant, dans sa recherche d'équilibre, les seuls coûts ne peuvent suffire. Désinciter les comportements malhonnêtes est une chose, inciter en retour ceux *honnêtes*, dont le réseau\* a un besoin vital, en est une autre.

Par son importance, Nakamoto fait le choix radicalement innovant d'attacher à l'activité de minage (spécifiquement à la production d'une PoW\* valide devenue canonique), l'émission monétaire de Bitcoin. Ce faisant, au désintéressement / sanction induit par la PoW\*, Nakamoto attache un intérêssement plus positif : la création monétaire des UCN\* offerte en récompense au nœud\* *leader*, pour chaque cycle de mise à jour du registre. De ce fait, l'établissement des modalités d'émission endogène des UCN\* (son monnayage) est une incitation politique essentielle à la soutenabilité de Bitcoin. Pour Nakamoto, le « *choix du nombre de pièces et du calendrier de distribution* » est « *un choix difficile* » (Nakamoto et Hearn 2009) qui, au-delà des références monétaires situées (cf. Chap. II), n'est pas sans conséquence pratique. Pour le rythme d'émission, Nakamoto définit un échéancier *ad hoc* suivant une logique d'émission explosive bien que décroissante (Nakamoto 2009b) au rythme d'une temporalité propre, dont l'unité est les enregistrements (voir l'échéancier anticipé et effectif, Annexe n°II.2) : à son lancement et durant les trois premières années, 50 bitcoins sont créés par nouveau bloc émis, ce qui, rapporté aux UCN\* en circulation, donne un « *taux d'inflation de la monnaie bitcoin [...] stupéfiant* » avoisinant les 35% (Champagne 2014, p. 45). Ces UCN\* sont émises et assignées par le protocole de manière endogène via l'émission d'une transaction\* de récompense (ou « *coinbase transaction\** ») incluse protocolairement lors des opérations de production d'un *enregistrement candidat*\*<sup>110</sup>. À la suite de l'enregistrement de genèse\* du 3 janvier 2009<sup>111</sup>, chaque nouveau bloc qui devient canonique donne lieu au versement de la récompense d'émission prévue à l'adresse du nœud\* vainqueur de la course à la PoW\* l'ayant produit. Une fois émise sous forme d'une *sortie de transaction*\* non dépensée\* (ou « UTXO\* ») liée à la transaction\* *coinbase* de récompense, les UCN\* pourront, après un laps de temps coder dans le protocole (voir section I.1.3), être échangées et circuler. La récompense de création monétaire est programmatiquement divisée par deux tous les 210 000 enregistrements (phénomène dit de « Halving » Sedgwick 2020b), cf. lignes verticales Annexe n°II.2) jusqu'à

---

<sup>110</sup> La transaction « *coinbase* » est une transaction de type spécifique liée à l'activité de traitement des transactions\* (minage) : première dans l'ordre d'un enregistrement, elle contient la récompense de création monétaire et les frais de transaction collectés.

<sup>111</sup> Nakamoto a doté ce premier enregistrement d'un statut particulier, et cette première récompense de 50 bitcoins à l'endroit d'une adresse contrôlée par Nakamoto n'est pas utilisable : « *Au niveau technique, le premier « coinbase » est spécial. On ne peut pas dépenser ni faire changer d'adresse ces 50 btc. La toute première transaction (coinbase) du bloc Genesis n'est pas une transaction valable. Elle ne fait pas partie de l'ensemble des transactions.* » A. Feron, voir <https://bitcoin.fr/bloc-genesis/> [consultation au 04/10/2020].

atteindre sa quantité maximum de 21 000 000 d'unités en circulation, vers l'année 2140 (Decrypt 2020, courbe bleue, premier graphique). Ce rythme d'émission dépend de la capacité de calcul totale participant à la réalisation de PoW\* et peut varier à court terme, ceci expliquant les différences entre l'émission anticipée et l'émission effectivement réalisée (graphique 2.1 et 2.2, Annexe n° II.2). Comme pour les matériaux d'une automobile, la fixation de cette quantité et de ce rythme d'émission renvoie à une « *composition de forces dont la nature est des plus diverses* » (Akrich 2010, p. 2) : Nakamoto l'aurait assise sur une « *supposition éclairée* » (Nakamoto et Hearn 2009) et des références (plus ou moins farfelues)<sup>112</sup>. Reste qu'elles sont aussi importantes qu'arbitraires, puisqu'une multiplicité de paramètres pouvait être implémentée, suivant des considérations sociotechniques différentes<sup>113</sup>. Si « *les pièces* » devaient bien « *être distribuées initialement d'une manière ou d'une autre* » et qu'un « *taux constant* » semble à Nakamoto « *être la meilleure formule* » (Nakamoto in Champagne 2014, p. 47), il est impossible de dire si cette répartition est plus « *pure* », « *immaculée* », ou efficace qu'une autre<sup>114</sup>. Autre conséquence pratique de ces choix : l'intéressement ayant une fin programmée, Bitcoin devra trouver d'autres subsides à distribuer aux opérateurs pour qu'ils continuent à supporter ses coûts de fonctionnement et de sécurisation à long terme : si Nakamoto et certains *bitcoiners*\* postulent que les frais de transaction\* en sus des récompenses de création monétaire prendront le relais, cela n'a rien d'automatique et fait débat (cf. « *Scaling Debate* », Chap. III).

Ces choix reposent sur une série de présupposés et problématiques non uniquement techniques. Cette émission, Nakamoto la fait « *stupéfiante* », afin d'inciter les premiers acteurs à sécuriser le réseau\* naissant, par définition fragile : pour atteindre un nombre de noeuds\* suffisant dans un temps court, il faut que les opérateurs aient à y gagner<sup>115</sup>. Optimiste, Nakamoto fait l'hypothèse que les UCN\* bitcoins rencontreront une demande et comme « *on sait à l'avance combien de nouveaux bitcoins seront créés chaque année [et que] la masse monétaire augmente d'un montant prévu, [cela] n'entraîne pas nécessairement une inflation* », car, « *si l'offre de monnaie augmente au même rythme que le nombre de personnes qui l'utilisent, les prix restent stables. Si elle n'augmente pas aussi vite que la demande, il y a déflation et les premiers détenteurs de monnaie*

<sup>112</sup> Dans une correspondance, Nakamoto mentionne que « *les 21 millions de BTC ont été déduits de la masse monétaire (mondiale M1) [...] qui s'élevait (apparemment) à 21 000 milliards USD [lors] de la publication du Bitcoin White Paper\** », et d'autre travaux indiquent qu'une telle offre « *de BTC permettrait de minimiser les erreurs d'arrondi dans le cadre d'une arithmétique à virgule flottante de 64 bits* » (Ducrée 2022, p. 19). Reste que « *dans un autre courriel [...] Nakamoto a révélé avoir joué un peu avec ce nombre, envisageant initialement 42 [...] mais 42 millions semblaient élevés* » [ce qui] *n'a pas beaucoup de sens.* » (*Ibid.*). Enfin, Ducrée (2022, p. 24 à 31) fait un inventaire des références entourant potentiellement le choix du chiffre 21, allant des plus techniques (les opérateurs binaires ou autres systèmes numériques), à d'autres plus ésotériques (le symbolisme géométrique, mais aussi des références médiatiques, cinématographiques ou sportives).

<sup>113</sup> « *Mon choix du nombre de pièces et du calendrier de distribution était une supposition éclairée. C'était un choix difficile, car une fois que le réseau est en place, il est verrouillé et nous sommes coincés avec lui. Je voulais choisir quelque chose qui rendrait les prix similaires à ceux des monnaies existantes, mais sans connaître l'avenir, c'est très difficile. J'ai fini par choisir quelque chose d'intermédiaire. Si le bitcoin reste une petite niche, sa valeur unitaire sera inférieure à celle des monnaies existantes. Si vous imaginez qu'il est utilisé pour une fraction du commerce mondial, alors il n'y aura que 21 millions de pièces pour le monde entier, et il vaudra donc beaucoup plus par unité. Les valeurs sont des entiers de 64 bits avec 8 décimales, de sorte qu'une pièce est représentée en interne par 100000000. Il y a beaucoup de granularité si les prix typiques deviennent petits. Par exemple, si 0,001 vaut 1 euro, il peut être plus facile de changer l'emplacement du point décimal, de sorte que si vous avez 1 bitcoin, il est maintenant affiché comme 1000, et 0,001 est affiché comme 1* » (Nakamoto et Hearn 2009).

<sup>114</sup> À l'aune du concept d'optimum de Pareto, au fondement de la mesure de l'efficacité économique, cela est impossible : chaque situation de dotations initiales possible est optimum au sens de Pareto (Harribey 1997).

<sup>115</sup> « *L'un des aspects essentiels du bitcoin est que la sécurité du réseau augmente en fonction de sa taille et du montant de la valeur à protéger. L'inconvénient est qu'il est vulnérable au début, lorsqu'il est petit, bien que la valeur qui pourrait être volée devrait toujours être inférieure à la quantité d'effort nécessaire pour la voler* » (Nakamoto et Hearn 2009).

*voient leur valeur augmenter.* » (Nakamoto cité par Champagne 2014 p.46-47) ». En outre, la valeur d'échange dérivée de cette demande, couplée à l'hypothèse d'une rationalité individuelle maximisatrice, garantirait que les opérateurs de nœuds\* aient intérêt à l'honnêteté. Un « *attaquant avide [...] capable de rassembler plus de puissance de calcul que tous les nœuds\* honnêtes* » devra « *choisir entre l'utiliser pour escroquer les gens [...] ou l'utiliser pour générer de nouvelles pièces* ». En bon homo œconomicus, il conclura qu'il est « *plus profitable de respecter les règles* » lui donnant droit à beaucoup de récompenses « *que de saper le système et la validité de sa propre richesse* » (Nakamoto 2008c, p. 4). En outre, ceci est en parfaite adéquation avec l'image d'un « jeu de bouteille de Klein », sans frontières claires et où l'intérieur et l'extérieur se confondent (Kavanagh et Miscione 2017, p. 12). À l'image des rapports coûts / bénéfices entrevus, qui ne sont ni stables, ni définis de manière endogène. Les coûts de la PoW\* recouvrent des biens et services (électricité, machines) réglés en monnaie nationale. La valorisation des UCN\* est, elle, renvoyée à une concurrence marchande entre monnaies, qu'il faut organiser, et dépend d'une demande qu'il faut développer. Les coûts de production comme la valorisation des UCN\*, qui déterminent *in fine* leurs revenus, relèvent d'acteurs et de processus largement exogènes au protocole (cf. section III).

De ce fait, la profitabilité des opérateurs dépend d'une valorisation volatile, laquelle peut entraîner des mouvements brusques et massifs d'entrées et sorties de capacité de calculs, auxquels le protocole doit s'adapter. Pour faire face au changement d'intérêt des mineurs (à technologie constante) et pour encadrer les effets des avancées technologiques, Nakamoto choisit une *cible de difficulté\** dynamique qui, à puissance donnée, lui permet d'établir la découverte d'une PoW\* en SHA 256, valide toutes les dix minutes environ (Nakamoto 2008c, p. 4). Pour maintenir stable le rythme d'émission, Bitcoin compense « *l'augmentation de la vitesse du matériel et la variation de l'intérêt pour l'exécution des nœuds\** » suivant que la cible de difficulté\* de la PoW\* « *est déterminée par une moyenne mobile visant un nombre moyen de blocs par heure. S'ils sont générés trop rapidement, la difficulté augmente* » et inversement (Nakamoto cité par Champagne 2014, p.46-47). Ce processus permet en dynamique de conserver un *temps d'enregistrement\** d'environ 10 minutes et de respecter l'échéancier d'émission prévu, malgré des variations importantes de la puissance de calcul déployée, particulièrement dans les premiers temps du réseau\* (comme illustré par l'Annexe n°II.2<sup>116</sup>). Cette règle est assise sur la loi de Moore (Nakamoto 2008c, p. 4 ; Champagne 2014, p. 157 et 319) et les évolutions technologiques anticipées. Celles-ci lui apparaissent aussi exogènes qu'ambivalentes. D'un côté, elles portent un risque d'obsolescence, Nakamoto le sait. La fonction de hachage\* SHA 256 de sa PoW\* pourrait être brisée, non par les « *améliorations informatiques de la loi de Moore* », mais « *par une méthode de craquage révolutionnaire* » (Nakamoto cité par Champagne 2014, p. 157, c'est-à-dire par le développement d'ordinateurs quantiques). Dans cette situation, Nakamoto pensait qu'il suffirait au protocole d'implémenter « *une nouvelle fonction de hachage\* [...]. Tout le monde devra mettre à jour son logiciel [qui] conserverait un nouveau hachage de tous les anciens blocs pour s'assurer qu'ils ne sont pas remplacés par un autre bloc avec le même ancien hachage.* » (Nakamoto cité par *Ibid.*, p. 157-158). Nakamoto use prudemment du conditionnel, quand d'autres au contraire voient cette situation comme une « *bombe à retardement* » (E. Z. Yang cité par Jeong 2013, p. 32), qui ne manque de poser problème et d'ouvrir des débats conflictuels : Nakamoto ne le sait pas encore, mais on ne change pas si facilement un rouage aussi essentiel de Bitcoin (cf. Chap. III). D'un autre côté, le progrès technique est chez lui nécessaire à la dynamique de soutenabilité à long terme de Bitcoin. La base de données Bitcoin a un poids croissant (suivant l'augmentation du nombre de transactions\*)

---

<sup>116</sup> C'est cette cible de difficulté\*, recalculée tous les 2016 enregistrements, qui explique que les écarts entre les émissions quotidiennes effectives (la courbe rouge du graphique 2.2) et celles attendues (représentées dans le graphique 2.1) ne sont que momentanés, permettant que, en moyenne, l'émission suive l'échéancier programmé (hors *crise de faux monnayage*, cf. Chap. III).

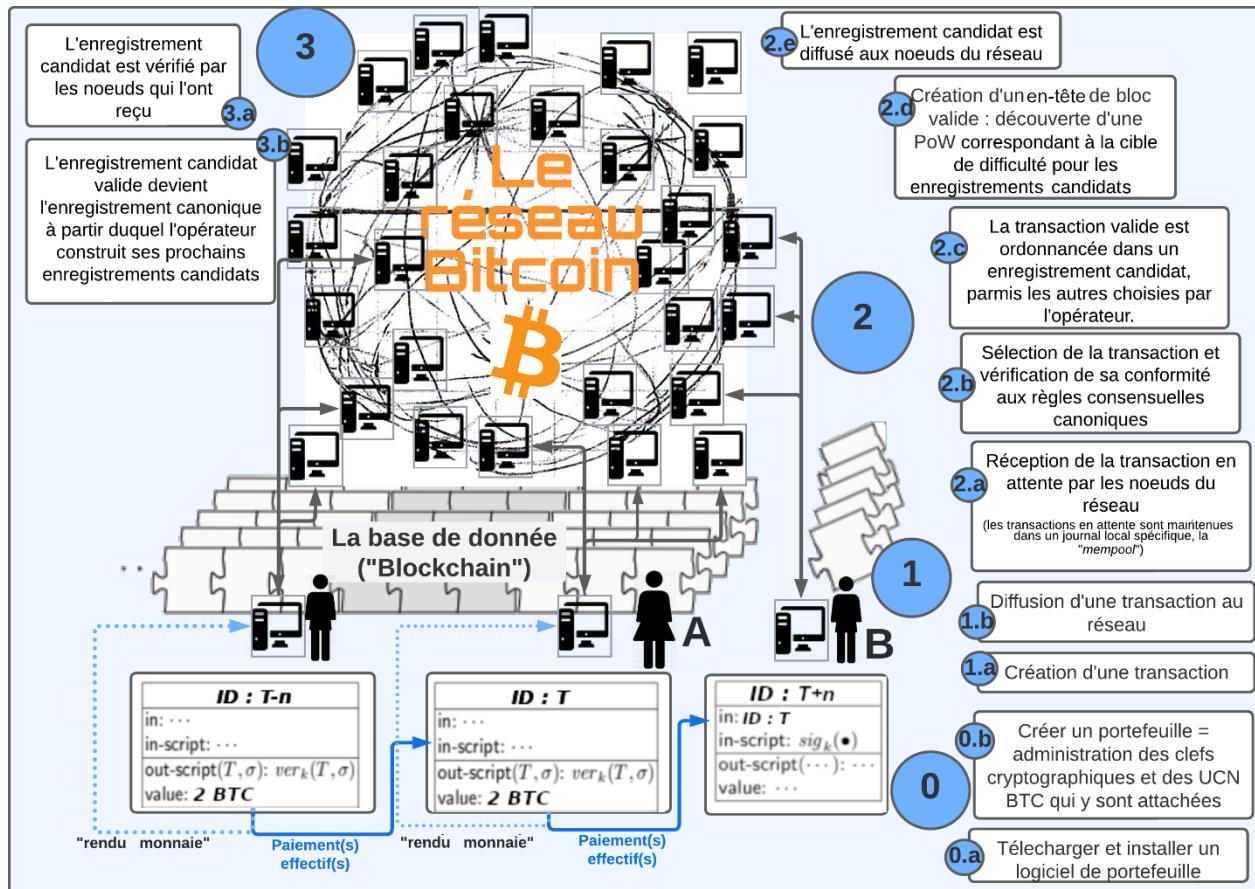
qui y est consigné), ce qui, à coût de stockage donné, conduira à terme à des coûts croissants, qui induiront en retour une centralisation des opérateurs du fait d'économie d'échelles. Nakamoto, là encore, évacue ce problème, postulant que « *les systèmes informatiques étant généralement vendus avec 2 Go de RAM à partir de 2008, et la loi de Moore prévoyant une croissance actuelle de 1,2 Go par an* » (Nakamoto cité par Champagne 2014, p.46-47), l'évolution à la baisse du coût de stockage attendue compense l'augmentation du poids de la base de données (ce qui est en débat, cf. « *Scaling Debate* », Chap. III).

Le consensus de Nakamoto par PoW\* est un arrangement sociotechnique essentiel à la sécurité et à la soutenabilité de Bitcoin, servant tout à la fois : au tirage au sort équitable d'un leader, à mesurer le caractère canonique des enregistrements, à sécuriser ces enregistrements et à créer de la monnaie de manière endogène. De ce fait, Bitcoin est comparable à une « bouteille de Klein », puisque les effets du jeu d'incitations dépendent de variables à la fois endogènes (fixation du monnayage), mais aussi et surtout exogènes, sur lesquelles ni Nakamoto, ni le protocole n'ont de prise. En définitive, les fonctions et sens de ce jeu d'incitations sont irréductiblement politiques. En outre, les choix architecturaux présentés relèvent de négociations jamais closes : de nouveaux compromis pourront et/ou devront émerger, car Bitcoin doit s'adapter à un environnement changeant pour survivre. Reste encore à présenter le fonctionnement de Bitcoin, ses acteurs et dispositifs sociotechniques suivant le script entrevu par Nakamoto.

### I.1.3 Le fonctionnement de Bitcoin suivant le script original de Nakamoto

Nous voilà familiarisés avec les composants et mécanismes clefs de Bitcoin. Mais, pour l'heure, nous n'avons entrevu la pièce de Nakamoto qu'au travers de ses didascalies et mises en contexte éclairant les grandes lignes d'un scénario qui entremèle un *récit maître* (créer une monnaie numérique distribuée) et des trames secondaires, fait de cas limites et d'intrigues (*double dépense*, *attaque sybille*, convergence en cas de *Fork*\* de chaîne, etc.). Les acteurs (humains ou non) du casting de Nakamoto ont été introduits liminairement, sans tenir compte de l'ordre de passage et des costumes de scène. Il est temps de présenter la répétition générale et sa mise en œuvre afin d'éclairer la façon dont les éléments cités sont censés s'articuler. Nous partons du déroulé séquentiel d'une transaction\* Bitcoin exposé dans le WP\* de Nakamoto (2008b; synthétisé dans la Figure 3), de la production d'une transaction\* individuelle T (processus 0 à 1) à son règlement final dont le traitement distribué permet d'aboutir à la construction collective, abstraite et latente, d'un registre\* de comptes canonique, par synchronisation des copies individuelles de chaque nœud\* (processus 2 à 3).

**Figure 3 : Le fonctionnement synthétique de Bitcoin à travers la réalisation d'une transaction**



Source : Rolland Maël

L'ensemble des composants et mécanismes précédents participent à structurer Bitcoin en trois couches interdépendantes : une couche protocolaire, une couche réseau\* P2P et une couche de base de données publiques, contenant l'état du système. Ces couches forment la scène Bitcoin. Sur ces planches, c'est une histoire sans fin que met en scène Nakamoto et sa saynète originale se rejoue à chaque bloc, suivant le temps d'un cycle de mise à jour du registre. Le casting est sommaire, Bitcoin comme protocole informatique\* pair-à-pair\* voit ses nœuds\* communiquer sur un pied d'égalité et, pour autant qu'un grand nombre d'acteurs est au générique – condition de résilience d'un réseau\* P2P -, les statuts et rôles offerts ne sont ni nombreux, ni singuliers ou personnels. À l'origine, chaque nœud\* est volontairement interchangeable. Le fonctionnement du protocole Bitcoin mobilise un ensemble varié de rôles et de fonctions impliquées dans la production, la vérification et le traitement des transactions\* et des enregistrements (relevant d'une division du travail en recomposition, cf. section I.2.1). Être un pair figurant nécessite d'être connecté au protocole, d'être identifié en son sein et capable de vérifier l'ensemble des données endogènes\* transitant dans le réseau\*. Soit d'être en capacité d'exécuter l'ensemble des fonctions protocolaires canoniques, de la gestion de portefeuille\* à la vérification et au traitement des transactions\*, et à la mise à jour du registre\* par l'activité de minage. Cela passe par la maintenance d'un client « complet » (disposant de l'entièreté de la chaîne de blocs\*) et « mineur » (disposant des capacités de minage).

## Production individuelle d'une transaction\* Bitcoin

Réaliser une transaction\* nécessite de disposer d'un compte Bitcoin approvisionné (0) et donc d'un client logiciel. Ces prérequis sont sous-tendus dans le WP\* de Nakamoto qui, à la suite de son introduction critique, débute par la définition d'une transaction\* Bitcoin, renseignant la forme que revêtent les actrices de premier rôle que sont les UCN\* et les modalités de leur circulation. Pour qu'elles circulent, il faut produire et publier un ordre de cession valide *via* un client Bitcoin.

### (0) *Les Préalables : disposer d'un portefeuille et d'UCN*

Sans possession préalable d'UCN\*, pas de dépense possible. Le protocole ne fait pas crédit. Pour en recevoir, il faut disposer d'une adresse, dérivée d'un couple de clefs cryptographiques étant les seules identités des coéchangistes A et B au sein du protocole. Aucune connexion Internet n'est nécessaire, hormis pour télécharger le logiciel client, qu'il suffit ensuite d'installer sur l'ordinateur utilisateur (étape 0.a dans le schéma). Au sein du client, ne sont mobilisés ici que ses composants liés aux fonctions de portefeuille\* : la création et l'administration des clefs cryptographiques comme la dérivation d'adresses (étape 0.b).

Suivant leurs conditions d'émission, le costume des UCN\* bitcoin est scriptural : une « *pièce* » de monnaie bitcoin n'est autre qu' « *une chaîne de signatures numériques. Chaque propriétaire transfère la pièce au suivant en signant numériquement un hachage de la transaction\* précédente et la clef publique du propriétaire suivant et en les ajoutant à la fin de la pièce.* » (*Ibid.*, p. 2). Sa forme comptable prend la forme d'une liste de sortie de transaction\* non dépensée\* (ou UTXO\*) correspondant aux unités reçues non encore dépensées : l'ensemble des UTXO\* représente la masse monétaire en circulation (Lars 2018b). En cela, chaque transaction\* est chaînée aux transactions\* passées et ce jeu d'entrées / sorties permet de suivre leur circulation du moment de leur émission (leur « *transaction\* coinbase* » d'origine) jusqu'à leur dernier propriétaire, à la manière d'une lettre au porteur à endossement : dans le schéma, l'individu A possède déjà 2 BTC issus d'une transaction\* reçue en T-n<sup>117</sup>. Cette UTXO\* est attachée à l'adresse de A, qui est le seul, *via* sa clef privée, à pouvoir signer légitimement les transactions\* sortantes l'impliquant. Si contribuer à l'activité de minage fut la première manière d'obtenir des UCN\*, il est aujourd'hui possible d'en obtenir en don ou en paiement, en échange de biens, de services ou d'autres devises... mais, pour cela, il aura fallu que de nombreux acteurs y travaillent (cf. section suivante).

### (1) *Créer et diffuser une transaction\* Bitcoin*

Une transaction\* est une demande en écriture sur le registre\* des comptes, un ordre de cession d'UTXO\* qui définit un/de nouveau(x) propriétaire(s). Sa rédaction relève d'un langage spécifique, très simple et sécurisé, établissant une syntaxe et une liste d'instructions possibles : le « Bitcoin

---

<sup>117</sup> Pour simplifier, nous dotons cette transaction d'une identification fantaisiste (ID : T-n), plus lisible que la forme réelle : « d1ec044d66a62778e87aab8e0f06a666eb3c7bfb32f0a324a62f12dc636aa737 ».

script » et ses « OP\_CODE »<sup>118</sup> (Lars 2018a ; Lars 2018b). Un client portefeuille\* approvisionné peut créer *via* ce langage une transaction\* Bitcoin valide (étape 1.a). Le script de transaction\* créé (ID : T) stipule, par le jeu d’instructions du standard utilisé<sup>119</sup>, les modalités par lesquelles le destinataire pourra y accéder à l’avenir. Généralement, la prochaine transaction\* doit fournir la clef publique légitime - son *hash*\* correspond à l’adresse de destination qui était intégrée au script de la transaction\* précédente (ID : T-n), ainsi qu’une signature de la clef privée associée à la clef publique fournie. La transaction\* produite (ID : T) ordonne la dépense de l’UTXO\* de 2BTC reçue par la transaction\* précédente (ID : T-n) qu’elle prend en entrée. Les ou les UTXO\*(s) prises en entrée seront dépensées en entier *via* la production de nouvelles UTXO\*s en sortie : cette transaction\* (ID : T) en contient 3, l’une correspondant au paiement de A à B (de 1 BTC), l’autre aux frais de transaction\* octroyés à l’adresse de l’opérateur qui la traite (de 0,005 BTC), et la dernière au rendu monnaie, renvoyé à A (de 0.0095BTC).

L’ordre de cession est signé par la clef privée ( $\text{sig}_k$  représente la signature) avant d’être diffusé au réseau\* (opération 1.b) ; contrairement aux actions précédentes réalisées hors ligne, celle-ci est liée au réseau\* P2P et des connexions à Internet et au réseau\* Bitcoin sont nécessaires.

## Production collective d’un consensus sur un registre transactionnel commun

La nouvelle transaction\* (ID : T) n’est qu’une proposition de modification du registre, visant à dépenser l’UTXO\* de 2 BTC de A par la création desdites 3 UTXO\*s. Sa conformité doit être vérifiée avant toute modification du registre\* canonique (étapes 2 et 3). Produire un consensus collectif autour de la validité des transactions\* individuelles émises renvoie à différentes opérations : cela va du traitement des transactions\* (étapes 2.a, b, c et d), à la production d’enregistrements candidats (étapes 2.d et e ; l’activité de minage en langage indigène) en passant par leur canonisation, concomitante à leur vérification/acceptation par l’ensemble des nœuds\* (étapes 3.a et b). Ces opérations mobilisent des composants et des fonctions plus intensives en ressources que celles impliquées dans la tenue d’un portefeuille\* : sans quoi, impossible de « vérifier les signatures pour vérifier la chaîne de propriété » (Nakamoto 2008c, p. 2). D’où l’obligation de maintenir un registre\* transactionnel à jour permettant de vérifier, à chaque cycle de mise à jour, la validité des transactions\* et des enregistrements présents et passés.

---

<sup>118</sup> Pour une CM, le concept de transaction renvoie à un programme informatique. Sa rédaction peut être réalisée dans des langages de programmation aux propriétés différentes : diverses syntaxes et jeux d’instructions, appelés « OP\_CODE », sont disponibles. C’est en eux que sont codifiées les demandes d’écritures à exécuter lors du traitement des transactions\*. Ils déterminent le périmètre applicatif du protocole, rendant possibles ou impossibles formellement certains types d’interaction, renvoyant à des qualités dites d’« expressivité ». Le Bitcoin script est considéré comme peu expressif : c’est un langage de programmation\* à pile, très simple et non Turing complet, sans boucles, ni pointeurs, « rien que des mathématiques et de la cryptographie\* »(Champagne 2014, p. 160-161) : « les « données » sont placées sur la pile et des « codes opératoires » (opcodes) agissent sur ces données. » (Lars 2018b). Pour « riche » que soit Bitcoin script, avec sa centaine de codes opératoires, les actions possibles sont relativement restreintes par rapport à d’autres CM (*Ibid.*). Un langage dit « Turing-complet » (comme « Solidity » d’Ethereum) possède un haut degré d’expressivité en ce qu’il permet la réalisation de boucles – cf. exécuter une portion de code plusieurs fois de suite jusqu’à qu’une condition de sortie soit rencontrée. La faible « expressivité » n’apparaît pas que comme un défaut, puisqu’elle est économique et relativement sécuritaire – les boucles accroissent les risques de bogue et/ou d’utilisation malveillante (Lars 2018a ; Lars 2018b). L’ensemble des instructions du langage script Bitcoin est consultable ici : <https://en.bitcoin.it/wiki/Script> [consultation au 06/10/2020].

<sup>119</sup> Pour l’heure, nous avons rencontré le script « *scriptPubKey* », format général majoritairement utilisé. Mais d’autres standards existent ouvrant des usages différenciés comme le « *pay-to-script-hash* » mobilisé pour les transactions multisignatures ou les “ *Hashed Timelock Contract* ” permettant la création des réseaux de paiement de secondes couches (cf. section suivante).

## (2) Le traitement distribué des transactions\* par « minage » : vérification, ordonnancement, production et diffusion d'un enregistrement candidat\* valide

La nouvelle transaction\* publiée (ID : T) prend d'abord la forme d'une transaction\* en attente. Elle est réceptionnée par les nœuds\* dans un *journal local*\* dédié : « *la mempool* » (étape 2.a). La vitesse de propagation et de réception dépend de variables diverses (propriétés matérielles et logicielles des conditions d'accès à Internet, topologie du réseau\*, etc.) qui affectent la bande passante entre émetteurs et récepteurs. De son côté, chaque nœud\* choisit les transactions\* en attente qu'il désire traiter. Puis il établit leur validité : est vérifié d'abord que la quantité d'UCN\* en sortie existe en entrée<sup>120</sup> et que la signature produite ( $sig_k$ ) est valide (étape 2.b). S'il y a plus d'UCN\* en sortie qu'en entrée, ou qu'une même UTXO\* est dépensée plusieurs fois, ou si la signature est mauvaise, la transaction\* est « logiquement » rejetée<sup>121</sup>. Les transactions\* valides, elles, sont ensuite agencées dans un arbre de Merkle\* : elles sont passées deux par deux dans une fonction de hachage\* suivant l'ordre défini par l'opérateur, jusqu'à obtenir un *hash*\* unique appelé le « *merkle root* » (opération 2.c). Ce dernier est intégré, avec d'autres informations (la version logicielle utilisée ; l'horodatage\*, le *hash*\* de l'enregistrement précédent et un nombre arbitraire dit « *nonce*\* »), dans un en-tête d'enregistrement\* candidat\* (le « *block header* » ou « *Block hash*\* ») (Nakamoto 2008c, p.3), qui doit encore être scellé par réalisation d'une PoW\* valide (opération 2.d). C'est cette étape qui est intensive en capacités CPU. Pour fabriquer un en-tête de bloc valide, un nœud\* va en *hacher* le contenu (*via* la fonction SHA256) duquel il ne modifie que le *nonce*\* et ce, jusqu'à trouver une empreinte respectant la difficulté cible. Cet en-tête de bloc valide obtenu, l'opérateur diffuse au réseau\* son enregistrement valide qui n'est encore que candidat (opération 2.e).

## (3) Vérification et intégration d'un bloc candidat valide dans le registre canonique commun

La validité de l'enregistrement candidat\* (et des transactions\* intégrées en son sein) soumis au réseau\* ne se décrète pas. Elle est vérifiée par l'ensemble des nœuds\* avant d'être ou non intégrée dans leurs journaux transactionnels, l'érigéant en registre\* canonique (étape 3). L'enregistrement candidat\* valide est diffusé de proche en proche, du nœud\* émetteur à ceux qui lui sont connectés et ainsi de suite. Dès réception, chaque nœud\* va en vérifier la conformité à l'ensemble des règles protocolaires canoniques (étape 3.a). Comme pour l'étape précédente, le client doit encore être complet (disposer d'un registre\* à jour<sup>122</sup>), mais ici, les fonctions mobilisées nécessitent surtout la capacité mémoire et non de calcul : fabriquer une PoW\* valide est difficile, mais sa vérification ne l'est pas, puisqu'elle nécessite seulement l'exécution d'« *un seul hachage* » (Nakamoto 2008c, p. 3). Un enregistrement candidat\* invalide est « logiquement »<sup>123</sup> refusé et un avertissement est diffusé. Si la vérification est concluante, l'opérateur réplique l'enregistrement dans son journal, mettant ainsi à jour sa copie du registre\* canonique de transaction\*. Il dispose d'une nouvelle liste d'UTXO\*, qui servira de point de départ du prochain cycle de mise à jour du registre. Cette séquence

---

<sup>120</sup> En l'espèce, que l'UTXO prise en entrée (liée à la transaction ID : T-n) est suffisante pour couvrir la valeur de sortie, ce qui est le cas ici (la nouvelle transaction de A consume 1,005 BTC, ce qui est inférieur aux 2 BTC de la transaction précédente).

<sup>121</sup> Ces guillemets soulignent que ces règles transactionnelles canoniques peuvent être rendues caduques, cf. la crise CVE 2018 #17144, cas d'étude traité dans le chapitre III.

<sup>122</sup> Pour être valide, « *chaque transaction dans le bloc doit fournir une transition d'état valide vers un nouvel état à partir de ce qui était l'état canonique avant que la transaction n'ait été exécutée*. [Cet état] ne peut être calculé (en toute sécurité) pour tout bloc qu'en partant de l'état d'origine et en y appliquant séquentiellement chaque transaction dans chaque bloc.

<sup>123</sup> Nous expliciterons ces guillemets dans notre chapitre V, puisque ces règles transactionnelles canoniques sont théoriquement rendues caduques par le bogue CVE 2018 #17144 que nous y analyserons.

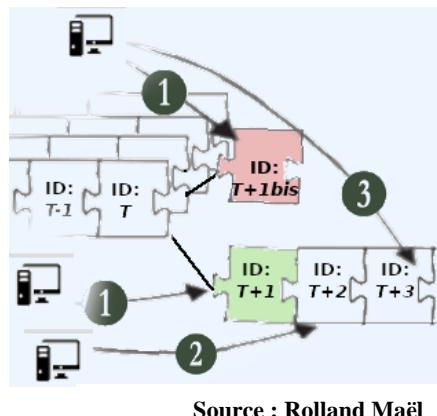
conclusive du scénario décrit par Nakamoto se reproduit à l'infini, les nœuds\* restant en scène pour une nouvelle séquence identique.

À cette étape s'opère la rémunération de l'opérateur dont l'enregistrement candidat\* devient canonique, puisque, ce faisant, il contient des UTXO\* qui lui échoient : celles liées aux frais de transaction\* versés en contrepartie de leur traitement et celle de la transaction\* *coinbase*, la récompense d'émission monétaire. Cette transaction\* et l'UTXO\* de création monétaire qui lui est attachée sont particulières : l'UTXO\* n'est pas directement dépensable par l'opérateur qui les reçoit, contrairement à celles perçues comme frais de transaction\*. Protocolairement, l'UTXO\* créée par une transaction\* *coinbase* ne devient dépensable qu'après que 100 enregistrements ont été produits au-dessus de celui qui la contient (Walker, Greg 2017). Il s'agit là d'une mesure de protection dans le cas où un bloc reconnu canonique un temps devienne « orphelin », suite à une réorganisation de l'historique consécutive à un *Fork\** de chaîne, que le consensus de Nakamoto vise à réguler.

### (3 bis) Réorganisation de l'historique, Fork de chain et bloc orphelin

À un instant t, des milliers de nœuds\* concourent aux étapes 2 et 3 précédentes et, comme le réseau\* est faiblement cohérent, ils n'ont jamais accès aux mêmes informations. Chacun dans son coin, ils traitent des transactions\*, tentent de découvrir des PoW\* valides et vérifient la validité des enregistrements candidats reçus. Cela conduit au risque que, dans la course au prochain enregistrement candidat\*, plusieurs opérateurs traitent de transactions\* différentes et fabriquent un enregistrement candidat\* valide, qu'ils diffusent dans un laps de temps court<sup>124</sup> (situation illustrée par l'étape 1 de la Figure 4 suivante).

**Figure 4 : Réorganisation et « bloc orphelin »**



Les nœuds\* qui leur sont connectés reçoivent des enregistrements candidats différents (ID : T+1 et ID : T+1bis), construits sur le bloc canonique (ID : T). Puisqu'ils sont valides et de même hauteur, la règle de convergence sur l'enregistrement le plus long/lourd échoue à les départager. Chacun devient canonique pour le nœud\* qui l'a reçu faisant apparaître deux ensembles d'UTXO\* différents, incarnant deux historiques de transaction\* en compétition. Le réseau\* se sépare alors en deux branches (d'où le terme *Fork\** de chaîne) : l'une constituée des nœuds\* partageant l'historique (ID : T+1), l'autre considérant le canonique (ID : T+1bis). Grâce au consensus de Nakamoto, l'indétermination est levée rapidement : la probabilité que deux PoW\* valides soient découvertes presque simultanément est mince, la reproduction consécutive d'une telle occurrence l'est encore plus... Dans les dix minutes suivantes, un nouvel enregistrement candidat\* valide se produit et est diffusé (étape 2 de la Figure 4). Suivant la version de l'historique (ID : T+1 ou ID : T+1bis) sur laquelle il est construit, le départage se réalise, l'une étant dès lors plus lourde/longue que l'autre (l'enregistrement ID : T+2, Figure 4). Dès que « *la prochaine PoW\* sera trouvée et qu'une branche deviendra plus longue ; les nœuds\* qui travaillaient sur l'autre branche passeront alors à la branche la plus longue.* » (Nakamoto 2008c, p. 3) : ce nouveau bloc après vérification sera alors et sans ambiguïté considéré par tous comme canonique.

<sup>124</sup> Dans cette situation « *certaines nœuds\* peuvent recevoir l'un ou l'autre en premier. [Bien qu'] ils travaillent sur le premier [...] reçu, [ils] conservent l'autre branche au cas où elle deviendrait plus longue.* » (Nakamoto 2008, p. 3).

L'enregistrement (ID :T+1bis) devient « orphelin » et l'ensemble des transactions\* qu'il contenait, bien qu'ayant pu apparaître un temps confirmées au sein de la chaîne, ne le sont plus... c'est ce mécanisme qu'exploite l'attaque 51% permettant une double dépense *off chain*\* (cf. Annexe n°9). Ce mécanisme de réorganisation explique pourquoi, pour l'usager, si le paiement est validé à l'étape 3-b (apparaissant *on chain*\* comme « confirmé » à la place de « en attente »), il doit généralement attendre six confirmations\*, soit que six nouveaux enregistrements canoniques soient produits au-dessus de celui de la transaction\* en question, pour que le paiement soit considéré comme réglé et finalisé avec le marchand (cf. *finalité de paiement*\*).

Cette section fut l'occasion de présenter Bitcoin du point de vue de son concepteur, de revenir sur le contexte général de sa construction et de son fonctionnement. Il était nécessaire de restituer le substrat idéologique hétéroclite, les emprunts théoriques et les contraintes pratiques, hybrides et négociées, de sa conception (en particulier le consensus en PoW\*). Cette mise en avant des alliances et des attachements sociotechniques radicaux qu'oppose Nakamoto aux systèmes centralisés sert de fondation à notre démonstration de la nature sociotechnique de Bitcoin. Mais pour nécessaires qu'ils soient, ces éléments ne sont pas suffisants pour en éclairer toute l'épaisseur sociotechnique, redoublée par des improvisations d'acteurs renégociant pratiquement les formes et contenus établis par Nakamoto.

## I.2 QUAND LE « MONDE REDÉFINIT » BITCOIN DE MANIÈRE CARNAVALESQUE

Précédemment, nous avons présenté l'objet Bitcoin à partir de son design initial en démontrant comment chacun des choix techniques est une cristallisation de compromis sociopolitiques. Mais le scénario de Nakamoto et les « *mises en scène que les utilisateurs sont appelés à imaginer à partir du dispositif technique et des prescriptions* » ne sont rien sans les acteurs qui en incarnent les rôles ou en inventent d'autres (Akrich 2010, p. 208). Un protocole seul ne fait pas CM : le statut de CM tient pratiquement à sa confrontation avec des utilisateurs, acteurs à part entière de sa « production » par *monétisation* (cf. Chap. II). Cette confrontation se situe par-delà les activités de conception. Nakamoto est conscient que la prétention à faire CM suppose des propriétés extrinsèques et relationnelles, absentes à l'origine. Son Bitcoin « *doit se développer progressivement* » afin que son logiciel et sa « *petite communauté bêta* », encore balbutiants, se renforcent « *en cours de route* » (Nakamoto 2010f). Son plein potentiel – être utilisé au sein d'une multiplicité de services, après des débuts modestes au sein de « *niches étroites* » - se projette dans le temps long, à « *10 ans* » (Nakamoto dans Champagne 2014, p. 94). Cette période est nécessaire à l'*amorçage* d'« *une boucle de rétroaction positive* » qui, suivant une dynamique de « *prophétie auto-réalisatrice* », verra émerger « *tellement d'applications* » que, « *à mesure que le nombre d'utilisateurs augmente[ra], la valeur augmente[ra]* » attirant, par effet réseau\*, de nouveaux utilisateurs, de nouveaux usages, etc. (Nakamoto dans *Ibid.*, p. 106). En cela, Bitcoin et les CM sont moins des objets que des infrastructures sociotechniques, et il est ardu de restituer le travail théorique et pratique complexe concourant à leur développement (Bowker 1996, p. 1). Les infrastructures ne se limitent pas à « *des briques, des tuyaux ou des câbles* », mais « *inclus[en]t également des entités plus abstraites, telles*

*que les protocoles (humains et informatiques), les standards et la mémoire»* (Bowker et al., 2010, p. 97). » et, au-delà de leur diversité, elles se définissent par 9 propriétés (Star 1999, p. 380-382)<sup>125</sup> :

- i. *D'encastrement* : elles sont plongées dans et à côté d'autres arrangements sociotechniques.
- ii. *De transparence pour l'usager* : elles supportent tacitement l'exécution de leurs tâches sans nécessité de réinvention, ou réassemblage pour les réaliser.
- iii. *De portée* : spatiale et temporelle, qui voit leur étendue excéder l'événement et la pratique isolée.
- iv. *D'apprentissage comme bénéfice de l'appartenance* : leurs artefacts et arrangements sociaux sont pris pour acquis suivant l'adhésion des acteurs à une communauté de pratique.
- v. *De liaison à des conventions de pratiques* : elles sont façonnées comme elles façonnent les conventions de leur communauté de pratiques.
- vi. *D'incorporation de standards et normes* : l'extension de leur portée impose de s'intégrer à d'autres infrastructures et outils de manière normalisée.
- vii. *Construites sur une base installée* : elles n'émergent pas *ex nihilo* et doivent lutter avec l'inertie d'une base installée, dont elles héritent des forces et des limites.
- viii. *Deviennent visibles lors de la panne* : leur qualité d'invisibilité aux usagers disparaît lors de panne ;
- ix. *Sont fixées par incrément modulaires* : leur évolution ne se fait pas d'en haut, elle prend du temps et se négocie avec l'ensemble des systèmes impliqués.

Au commencement, Bitcoin n'a encore aucune de ces caractéristiques. Relationnelles, les infrastructures nécessitent temps et travail. Comme pour le téléphone, l'Internet ou les divers systèmes d'information, leur développement se fait par étapes, suivant un travail continu largement réalisé « "en coulisse" par des communautés de pirates et d'ingénieurs » (Bowker 1996, p. 50; rejoint par Star 1999; Edwards et al. 2009). Tout développement infrastructurel renvoie à 3 étapes successives - une *phase de construction / lancement*, une *phase de développement / succès*, et une *phase de sédimentation / stabilisation* - et à chaque nouvelle étape se posent des problématiques d'intégration à un existant constitué d'artefacts, d'habitudes, de normes et de rôles humains (Edwards et al. 2009, p. 366-367). Le développement infrastructurel de Bitcoin n'y déroge pas, il se fait même exemplaire. S'y déploient des enjeux de passerelles\* et de standardisation (vecteurs problématiques d'interopérabilité), d'alignement d'intérêts entre parties prenantes pour lesquelles stabilité, durabilité et innovation (et les risques afférents) n'ont pas le même attrait suivant ce qu'elles attendent de l'infrastructure (*Ibid.*). Finalement, puisqu'agence et pouvoir contenu dans les arrangements évoluent au gré de recompositions « *puissamment (re)distributives* » (en matière de ressources et de possibilités d'action), une infrastructure est mue par l'existence de tensions jamais résolues entre une multiplicité d'acteurs situés, dont les stratégies potentiellement contradictoires en font un objet de conflits et de négociations constantes (*Ibid.* rejoint par Bowker 1996; Star 1999). Si toute CM, au premier chef desquelles Bitcoin, font face à ces problématiques, leur importance est redoublée par une spécificité propre à leur prétention monétaire. Au-delà de dispositifs techniques inédits, les processus d'innovation nécessitent « *l'émergence de nouvelles formes de coopération et la construction de significations partagées entre les acteurs impliqués* » et, dans le cas de la monnaie, cela croise la question de la valeur (Mallard, Méadel et Musiani 2014, p. 1). La valeur (propre à l'argent) et la liquidité des moyens de paiement qui l'incarne, découlent moins de propriétés intrinsèques qu'extrinsèques et relationnelles. Supposant des liens construits « *entre les*

---

<sup>125</sup> La granularité la plus fine a été retenue, leur nombre varie suivant les textes au gré de redécoupages : Star & Ruheleder (1996) cités par Bowker (1996, p. 1) compte les cinq premiers ; Leigh Star et Ruhleider 2010, p. 118-119, s'arrêtent à la 8<sup>ème</sup>.

*dispositifs impliqués dans son usage, et les conceptions de la valeur qu'elle incarne* », confiance et légitimité se jouent dans les modalités d'établissement d'un réseau\* hétérogène d'acteurs et de dispositifs plus ou moins capables de faire émerger de la valeur et d'en « *mettre en œuvre la circulation* » (*Ibid.*). Une CM est ainsi à la fois un agencement sociotechnique et un « *agencement économique* », résultant d'un processus d'*« économisation* » (Fabian Muniesa, Millo et Callon 2007, p. 3) sans lequel il n'est pas de *monétisation* (cf. Chap. II section 2).

L'émergence de Bitcoin, si elle n'est pas immaculée, n'en est pas moins exemplaire puisque, en tant que pionnier, il y avait tout à faire. Ce qui se construit pour lui bénéficie aux autres CM et réciproquement (cf. section I.3). Déjà, il fut nécessaire que certains assurent sa maintenance, sa sécurité, et l'adaptent à un environnement changeant. Dans le même temps, il fallut d'autres acteurs pour créer des passerelles\*, des usages et des marchés, établir des mécanismes de découverte de prix et des modèles de valorisation, éduquer et populariser des récits (« *narrative* »), forger des croyances, des représentations et un sens partagé. Par-delà la conception de Bitcoin et son contexte, le comprendre comme CM nécessite d'en restituer le développement infrastructurel dans sa sociohistoire, afin de saisir les processus ayant concouru à son institutionnalisation comme monnaie. En outre, cette conception des CM, considérée non pas comme objet *déjà* constitué mais comme objet *en construction* (à laquelle nous participons), ouvre sur un problème méthodologique quant à la façon d'en raconter l'histoire complexe. Produites de la même inversion primordiale, où la démarche d'analyse se mue en son objet, les prochaines sections et la chronologie suivante, sur laquelle elles s'étayent, se singularisent de la littérature tant par le périmètre large d'éléments couverts que par la manière dont nous les articulons. Forte est la probabilité que le lecteur ait déjà connaissance d'éléments que nous mobiliserons, qu'ils aient fait l'actualité ou aient été traités par la littérature académique. La probabilité qu'ils les aient rencontrés restitués dans l'historicité proposée est plus faible. Habituellement traités chacun comme objet d'analyse (des « cas »), ces éléments joueront pour nous le rôle de matériaux constituant un objet plus grand, que nous appelons CM et que nous concevons comme infrastructure monétaire. En outre, notre approche plus relationnelle et englobante encourage à dépasser tant certaines dichotomies arbitraires (*on chain\** ou *off chain\**, par exemple) que l'intérêt exclusif porté à des sous-composantes communautaires (« Core Dev », par exemple cf. Chap. III) ou des usages spécifiques (blanchissement, trafics, etc.).

Cette chronologie est construite sur l'analyse *on chain\** de Tasca et Liu (2018) qui, par technique de « clustering » appliqué aux données *on chain\**, ont, entre début 2009 et mai 2015, circonstancié pour Bitcoin trois régimes transactionnels successifs, relevant d'acteurs et d'usages différents : une phase dite de « preuve de concept », suivie d'une de « péché » aboutissant à celle de « maturation ». Nous reprenons à ces auteurs la structure générale de ces régimes, ainsi que leurs dénominations. D'un côté, car cette structure, dont les phases de lancement et de maturation ont été étendues (pour couvrir les premières traces *off chain\** de Nakamoto et du fait que notre analyse courait jusqu'au début 2020), dessine en les épousant les phases de développement infrastructurelles cernées par la littérature des *infrastructural studies* (*phase de construction / lancement, phase de développement / succès*, et *phase de sédimentation / stabilisation*). De l'autre, car ces dénominations choisies, moins abstraites et génériques, caractérisent les évolutions idiosyncratiques de Bitcoin que nous visons à restituer (en cohérence avec nos propres choix méthodologiques et narratifs). En complément, afin de saisir le pendant *off chain\** de ce développement, nous y avons adjoint l'évolution de l'écosystème Bitcoin représenté en domaines de développement infrastructurel, auxquels est appliqué un code couleur. Pour ce faire, nous sommes partis du travail de Rauchs (2016), couvrant l'évolution des segments et acteurs de l'écosystème Bitcoin entre 2009 et 2015. La chronologie a été enrichie d'éléments absents des analyses précédentes (évolutions protocolaires, émergence d'autres CM dont Ethereum, crises, etc.) en mobilisant de la littérature grise (la chronologie du site Bitcoin.fr et diverses autres, égrainées dans les sections suivantes). Sur ces

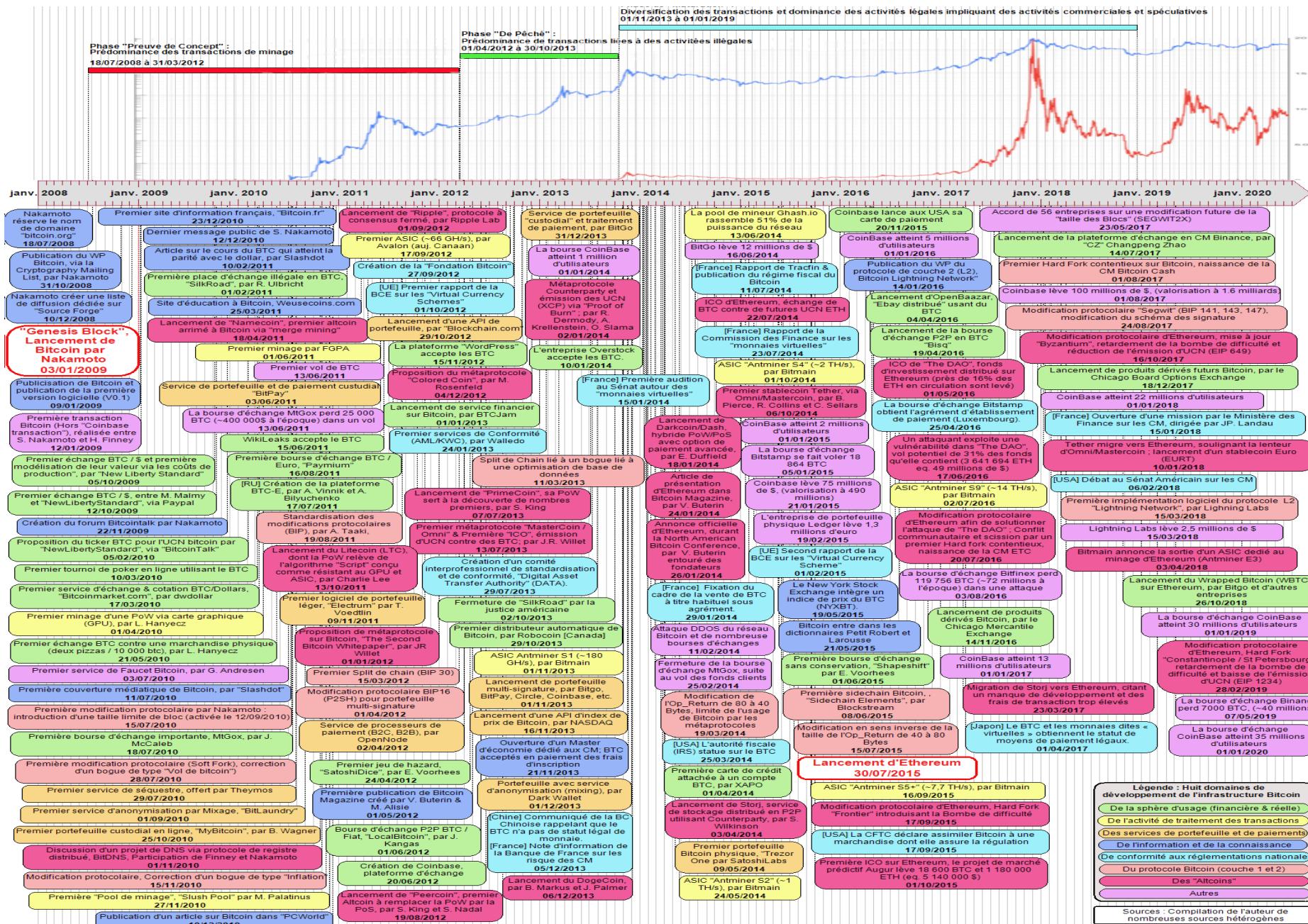
bases, nous constituons 8 domaines de développement infrastructurel de Bitcoin, dont les cinq premiers recomposent les 22 segments de Rauchs (2016, p. 118-119) comme suit : le domaine (i) de la sphère d'usage réelle et financière (en vert) contient les segments « jeux », « place de marché », « service de courtage », « service de notarisation », « innovations blockchain », « bourse d'échange », « plateforme de trading », « services d'investissement », « services de courtage », « processeur de paiement », « services financiers », « distributeur de bitcoin », « micropaiement », « plateforme de transfert de fonds » ; celui (ii) du traitement des transactions\* (en jaune) contient le segment « minage » ; celui (iii) des portefeuilles\* et des paiements (en orange) contient ceux de « portefeuille\* » et « mixage » ; celui (iv) de l'information et de la connaissance (en bleu foncé), « médias », « services de données » et « outils de développement » ; et le domaine (v) de conformité aux réglementations nationales (en bleu clair<sup>126</sup>) contient « services de conformité » et « autres services » ; nous y ajoutons un domaine (vi) du protocole Bitcoin (en rouge), relatif au développement protocolaire et logiciel ; un (vii) des « Altcoins\* » (en rose) et (viii) « autres » (en violet), pour des éléments plus événementiels, non couverts par les domaines précédents. Le tout est rapporté aux évolutions du cours du BTC/USD, avec la capitalisation de marché (en bleu, échelle logarithmique pour saisir la tendance) et le prix de marché (en rouge, échelle linéaire, soulignant l'erratisme, voir Annexe n°II.3).

Cette chronologie est constituée d'évènements structurants du développement infrastructurel de Bitcoin et de celui de la constellation de systèmes alternatifs créés autour *de* et s'articulant *à* lui (dont Ethereum), formant ensemble une infrastructure de périmètre supérieur. Que l'œil du lecteur ne s'y trompe pas, comme avec une peinture pointilliste, il est moins incité à regarder le détail (ce qu'il peut faire) que la figure d'ensemble : la surcharge est volontaire et vise à restituer dynamique crypto-carnavalesque multidimensionnelle, multi-niveaux et multi-acteurs de ce développement infrastructurel (Kavanagh et Miscione 2017). Détails et figures seront explicités lors des deux sections suivantes, mais l'analyse relative au développement infrastructurel de Bitcoin (traitée dans cette section I.2) bénéficie d'une granularité plus fine que celle dévolue aux Altcoins\* et à Ethereum (section I.3) : l'éclairage fourni pour Bitcoin et la valorisation de ces UCN\* vise à être suffisant pour en comprendre les ressorts essentiels et les transposer à d'autres CM.

---

<sup>126</sup> Pour des raisons d'accès aux sources, les informations concernant les juridictions européenne et américaine ont été privilégiés. La Chine, acteur important de l'écosystème Bitcoin, en particulier pour les activités liées au minage, va provoquer des secousses régulières dans l'écosystème par ces va et viens réglementaire sous forme de « China BAN » nombreux (Sergeenkov 2021)

## Chronologie 2 : L'institutionnalisation carnavalesque de l'infrastructure Bitcoin



Source : Rolland Maël

Cette chronologie, dévoilant l'invisible carnavalesque de l'infrastructure Bitcoin et de son développement, en saisit le caractère irréductiblement composite et négocié. Elle illustre à quel point, en tant qu'infrastructure sociotechnique, elle n'est réductible ni à son protocole, ni au dessein de son concepteur. Pour autant qu'elle est un « tissu sans couture », c'est une étoffe au motif arlequin (saisi par notre code couleur), dont la confection renvoie à l'entrecroisement du travail d'une multiplicité de tisserands et de navettes. Bitcoin « *forme “une infrastructure” sans frontière absolue ni définition a priori* » (Leigh Star et Ruhleder 2010, p. 119), puisqu'il est constitué d'une multiplicité de « mondes sociaux » et d'arrangements sociotechniques dont l'articulation repose sur des secteurs, des acteurs et des « *objets-frontières* »<sup>127</sup> (Leigh Star et Ruhleder 2010; Trompette et Vinck 2009, p. 8), encore à créer et qui ne cessent de se recomposer. Nous présenterons d'abord chacune des phases du développement infrastructurel de Bitcoin, en présentant certaines compositions d'arrangements, de pratiques, de secteurs et d'acteurs qui s'y développent (I.2.1). Nous reviendrons ensuite sur quelques « inversions paradoxales clefs » que ce développement carnavalesque a produites : les inversions Cypherpunk et crypto-anarchistes originales, qui faisaient de Bitcoin un « *site où les normes et les structures sont temporairement suspendues, où l'autorité conventionnelle est contestée et où l'autonomie est privilégiée par rapport à l'hétéronomie* », conduisent à d'autres, sous forme de re-intermédiation (I.2.2, Kavanagh et Miscione 2017, p. 18).

### I.2.1 Un développement infrastructurel au-delà du protocole Bitcoin

Si Bitcoin porte quelque fonction monétaire et financière, encore doit-il être autre chose qu'une curiosité technique, toucher des publics plus larges que ses cénacles originaux et être arrimé au monde réel afin que ses transactions\* participent d'échanges, le chargeant en valeurs du même nom. C'est un processus qui a commencé avant le lancement du protocole, et s'est développé par étape.

#### La phase de « preuve de concept » (de juillet 2008 à mars 2012)

Dans sa phase de « preuve de concept<sup>128</sup> », connaissance et pratique de Bitcoin restent confidentielles ; l'activité de minage prédomine et « *sans véritable activité commerciale* », le bitcoin n'est qu'une monnaie de « Monopoly » échangée entre des joueurs peu nombreux (Tasca et Liu 2018, p. 35). S'y retrouvent les caractéristiques de relatif isolement d'un système confiné à un cercle d'initiés, au centre duquel le concepteur Nakamoto jouit de pouvoirs importants (Edwards et al. 2009, p. 367). À l'image de cette période, les enregistrements restent vides jusqu'au 12 janvier 2009, date de la première transaction\* de 10 BTC, réalisée entre Nakamoto et le cypherpunk reconnu H. Finney<sup>129</sup> (Popper 2014; Sedgwick 2018f). Mais avant d'être lancé *on chain\**, Bitcoin a dû être annoncé *off chain\**. Il fallait recruter en amont les acteurs qui prendraient part à la constitution de son réseau\*. La date du 18 juillet 2008, retenue par notre chronologie, correspond à celle choisie par Nakamoto pour déposer le nom de

<sup>127</sup> Définis par Star et Griesemer (1989), les « *Objets-frontières* » sont des « *objets, abstraits ou concrets, dont la structure est suffisamment commune à plusieurs mondes sociaux pour qu'elle assure un minimum d'identité au niveau de l'intersection tout en étant suffisamment souple pour s'adapter aux besoins et contraintes spécifiques de chacun de ces mondes.* ». Constitués « *d'objets et de pratiques partagés* » (Leigh Star et Ruhleder 2010, p. 152), ils assurent « *à la fois l'autonomie de ces mondes sociaux et la communication entre eux* », permettant à des acteurs hétérogènes de travailler chacun de leur côté.

<sup>128</sup> De l'anglais « *Proof of Concept* », en français « Validation\* de principe » ou « Démonstration de faisabilité » : cela correspond à une réalisation simple et épurée visant à faire la démonstration de la faisabilité d'un procédé ou d'une innovation.

<sup>129</sup> Il prend part au réseau dès le 11 janvier 2009, voir <https://twitter.com/halfin/status/1110302988?s=20> [consultation au 07/10/2020].

domaine bitcoin.org, dont il se sert pour sa campagne de mobilisation ciblée. Et pour autant que les acteurs nécessaires à faire tourner des noeuds\* sont censés être indifférenciés, les appelés volontaires sont loin d'être des figurants aux qualités interchangeables, à l'image dudit Hal Finney, mais aussi de Gavin Andresen, Martti Malmi (« Sirius »), Jeff Garzik et d'autres acteurs sous pseudonyme qui, par affinités électives, se joignent tôt à Nakamoto pour assurer la maintenance d'une machinerie tout sauf autonome.

C'est autour et par ce qui n'est qu'un petit noyau dur d'acteurs que le développement de l'écosystème s'amorce<sup>130</sup>. Ce sont eux qui épaulent quotidiennement Nakamoto dans le développement du protocole et l'aideront à l'élaboration des actions correctives (en rouge) à mettre en œuvre lors de la survenue inévitable de bogues (dont les premiers très critiques surviennent rapidement, comme avec le bogue d' « inflation » du 15 novembre 2010, ou celui de « split de chain », du 15 mars 2011 ; cf. Chap. III). Par là même, ils participent activement à la standardisation de leur activité. Si, à l'origine, le code source Bitcoin était « *simplement un fichier .rar hébergé sur SourceForge [forçant] les premiers développeurs\* [à échanger] des correctifs de code avec Satoshi par courrier électronique* », dès le « *30 octobre 2009, Sirius (Martti Malmi) [...] crée un dépôt subversion pour le projet Bitcoin sur SourceForge* », permettant une gestion plus ouverte ; la migration vers la forge logicielle\* Github attendra 2011 (Lopp 2018). Et le fait de travailler sur les codes et de proposer des modifications protocolaires est tôt encadré, avec la mise en place en 2011 des « *Bitcoin Improvement Proposals* », ou « *BIP* »<sup>131</sup>, par exemple (cf. Chap. III). Ce sont eux aussi qui assurent la gestion des canaux d'information servant tout à la fois à fournir la documentation et à échanger avec les utilisateurs (comme BitcoinTalk, établi par Nakamoto, complémentant la *Sourceforge*, en bleu foncé). Ce sont encore eux qui élaborent les premiers dispositifs permettant une appropriation de la technologie dont dépend l'émergence d'usage et d'une valeur économique.

Le domaine du « minage » (en jaune), bien au-delà de sa prédominance *on chain\**, va connaître des bouleversements radicaux. S'il filtrait déjà les acteurs en capacité de rejoindre le réseau\*, ses barrières à l'entrée n'auront de cesse de s'élèver : d'individuelle, l'activité devient collective, suivant la constitution de coopératives (« pools », apparues fin 2010) et la compétition accrue oppose des machines de plus en plus spécialisées (GPU, FGPA puis ASICS ; Sedgwick 2019c; cf. section suivante). Aussi, ouvrir d'autres voies d'accès à Bitcoin et ses UCN\* est impératif à tout développement d'usage. Cela passe d'abord par le domaine des portefeuilles\* et des paiements (en orange) originellement peu diversifié. Comme dans le script original de Nakamoto, la seule solution disponible - Bitcoin QT, 0.1, publié le 9 janvier 2009 - est un client logiciel polyvalent, lourd et contraignant (Sedgwick 2019b) : il porte encore l'ensemble des composants et fonctions impliqués dans la production, la vérification et le traitement des transactions\* et des enregistrements. De ce fait, les erreurs des usagers sont lourdes de conséquences. L'injonction faite de sécuriser individuellement ses clefs cryptographiques (à l'époque un fichier « wallet.dat ») s'érige en enjeu opérationnel crucial, car *être sa propre banque* n'est pas à la portée de tous, ce qui se traduit par des pertes importantes<sup>132</sup> (Banque de France 2013, p. 5; Kaushal, Bagga et Sobti 2017). Les innovations et la diversification des solutions de portefeuilles\* soulageront les utilisateurs de ces coûts. À

---

<sup>130</sup> Entre 2010 et 2011, l'écosystème Bitcoin passe des cinq segments initiaux à 13, voire Rauch 2016, p. 49 à 56.

<sup>131</sup> C'est le développeur Amir Taaki, via le BIP 0001, voire <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki> [consultation au 05/12/2021] qui proposa de standardiser les propositions d'évolution des codes protocolaires, cf. Chap III.2.3.

<sup>132</sup> Soit par un mauvais management individuel (10 aout 2010, première perte d'utilisateur déclarée de 9000 BTC, Sedgwick 2019), soit par attaque informatique (plus tardive, en juin 2011, un mineur se fait voler 25 000 BTC, suivant que la valeur des UCN commence à aiguiser des appétits criminels) (Sedgwick 2018a).

la polyvalence et à la lourdeur du client unique, sont opposées la spécialisation et la légèreté d'une diversité de solutions, recomposant la division du travail, des tâches et des fonctions passées<sup>133</sup>. Mais l'offre « multi-signature », nécessaire à la mise en œuvre de solution de séquestration non centralisée, reste absente, impliquant des échanges de biens et services réels périlleux, car suspendus à l'existence de confiance *intuitue personae* entre coéchangistes. Si l'écosystème passe de 5 segments de marché à 13 entre 2010 et 2011 (Rauchs 2016, p. 50-52), l'extension de la sphère d'usage réelle de Bitcoin (en vert) doit passer par l'existence de dispositifs et de passerelles\* assurant l'interopérabilité de Bitcoin avec le monde réel. La possibilité pour de simples usagers d'achalander leur portefeuille\* en UCN\* et de les dépenser en toute sécurité en dépend, comme l'apparition d'une valeur d'échange. Ces dispositifs à inventer conditionnent l'élargissement des canaux d'accès et de circulation des UCN\* BTC, encore cantonnés à l'activité minière et à ces opérateurs. Pour toucher de nouveaux usagers, G. Andresen lance en juin 2010 le premier site de « *Faucet* », dont les visiteurs reçoivent gratuitement des UCN\* (50 BTC par visite, Sedgwick 2018e). Quant aux premiers échanges et bourses, ils seront d'abord fragiles, « *bancals* » et à « *trous* », dépendant de liens précaires au système bancaire et financier suivant des arrangements locaux et artisanaux (Sedgwick 2018b)<sup>134</sup>. L'émergence de solutions mieux intégrées et stabilisées ne tarde pas : apparaît en 2010 MtGox, lancé par Jed McCaleb<sup>135</sup>, qui devient rapidement la première plateforme pour la paire BTC/\$<sup>136</sup> : de 2010 à 2014, s'y concentreront près de 70% des volumes d'échange (Sedgwick 2018b; Sedgwick 2019o). En tant que passerelle\* aussi essentielle que centrale, ses volumes seraient un indicateur des flux entrants et sortants de l'écosystème (Christin 2013, p. 8). La première bourse en euro, Paymium, est créée en 2011 (Rauchs 2016, p. 50; Entretien n° 24).

---

<sup>133</sup> En 2010 apparaît « *MyBitcoin* », premier service intermédiaire (dit de garde ou “*custodial wallet*”, Rauchs 2016), permettant un accès simplifié au réseau. Un portefeuille\* « léger » non intermédiaire (ou « *non custodial* », Electrum) est lancé fin 2011 (Electrum website 2011), comme des solutions non connectées (ou « *cold wallet* », sous forme de portefeuille\* papier ou « *Paper Wallet* », puis de pièces numismatiques émises par l'entreprise « *Casacius* » en septembre 2011) (Sedgwick 2018d). Un premier service d'anonymisation par « *mixage* » - une technique d'anonymisation mélangeant les UTXO de plusieurs utilisateurs afin de rendre difficiles les analyses *on chain*\* et de préserver la fongibilité des UCN et la vie privée des usagers - était d'ailleurs apparue avec « *BitLaundry* », fin 2010 (<https://bitcointalk.org/index.php?topic=963.0>, Rauchs 2016) [consultation au 05/12/2021].

<sup>134</sup> Le premier échange de BTC contre de la monnaie nationale a lieu le 12 octobre 2009 entre Martti Malmi et « *NewLibertyStandard* » (vente de 5 050 BTC pour 5,02 \$) et le règlement passe par l'utilisation de la plateforme PayPal (Sedgwick 2018b; Sedgwick 2018e). Dès 2010, à la suite des demandes d'utilisateurs, apparaît sur BitcoinTalk un service de séquestration immunitaire et centralisé reposant sur un tiers reconnu : « *Theymos* », modérateur du forum choisi par Nakamoto, assure aux coéchangistes le respect des termes de leur « *contrat* » et le règlement final contre des frais de 1% des BTC échangés (Sedgwick 2020b). Le 22 mai 2010, Laszlo Hanyecz réalise le premier achat de bien physique - deux pizzas - qui passe par un intermédiaire individuel acceptant 10 000 bitcoins en échange d'un paiement en dollars au pizzaiolo (Sedgwick 2018f). Peu nombreux sont ceux qui acceptent le BTC, et le même Hanyecz échoue peu après à acheter une caméra (Sedgwick 2019f). « *Bitcoinmarket.com* », lancé le 17 mars 2010, est la première bourse d'échange (Sedgwick 2018b) et s'érite en première cotation ([https://en.wikipedia.org/wiki/Main\\_Page#prices\\_and\\_values\\_history](https://en.wikipedia.org/wiki/Main_Page#prices_and_values_history)) [consultation au 07/06/2022]). La plateforme dépend encore de PayPal, auquel elle s'arrime pour offrir du Dollar : si « *ce système a fonctionné pendant un certain temps* », « *à la suite d'une série de transactions frauduleuses, PayPal a été retiré de la bourse le 4 juin 2011* » (*Ibid.*).

<sup>135</sup> Créeur dans les années 2000 de la plateforme de partage P2P eDonkey, après MtGox qu'il vend à Mark Karpeles, il participe à fonder le protocole Ripple (section I.3.1, ce chapitre) qu'il forke pour créer Stellar suite à des désaccords (Impellizzeri 2020).

<sup>136</sup> Si le ticker boursier BTC utilisé s'impose à l'usage, il n'est pas conforme aux normes ISO 3166 et 4217:2015 relatives aux codifications des devises internationales : l'une contient la liste des codes pour le nom des pays émetteurs (Bitcoin ne peut s'en prévaloir et le préfixe « BT » sert déjà à la monnaie nationale du Bhoutan, le « ngultrum », ticker BTN), le second y ajoute un troisième terme, idéalement la première lettre du nom de la monnaie (voir <https://www.iso.org/fr/iso-4217-currency-codes.html> [consultation au 12/10/2022]).

Avant MtGox et sans espace de conversion suffisant, la valeur des UCN\* se fait dilemme de la « *poule et de l'œuf* » puisque sans valeur, pas d'acceptation en échange et sans échanges, pas d'apparition de valeur ("The Madhatter" cité par Sedgwick 2019b). Si les premières valorisations, par trop locales et singulières, n'avaient réussi à doter les UCN\* d'un commencement d'objectivité<sup>137</sup>, MtGox sera ici décisif. Son apparition coïncide avec des modifications d'usage : les transactions\* se mettent à utiliser des décimales traduisant une fixation nominale en dollars (Le Calvez 2020; BitMEX Research 2020b) et, corrélativement, une modification des frais de transaction\* par défaut définie par les portefeuilles\* (Möser et Böhme 2015). Par sa facilité d'accès, son étendue et la profondeur de liquidité qu'elle concentre, cette première véritable bourse produit un cours du BTC qui, au-delà de son erratisme, sera tendanciellement haussier. Justement, dans le domaine de l'information et de la connaissance (en bleu foncé), la médiatisation et, conséquemment, la construction des récits sur Bitcoin échappent désormais au premier cercle des *bitcoiners*\*. À côté de Bitcointalk, des médias spécialisés sont apparus (*WeUseCoins*, crypto.fr) qui, s'ils émanent encore de membres d'une communauté Bitcoin grandissante, seront de plus en plus concurrencés par les médias traditionnels, s'emparant d'un objet pour eux spectaculaire. La parité d'un BTC au dollar, atteinte début 2011 (Le Calvez 2020), est ainsi saluée par le média Slashdot (Sedgwick 2019c)<sup>138</sup>. L'intensification médiatique participe de vagues d'engouement-répulsion, se répercutant sur la valeur du cours, comme l'illustre sa poussée à 1\$14 suite à la publication d'un article de *Forbes* le concernant en avril 2011 (Greenberg 2011)... ou sa multiplication par 8 le 14 juin, suite à l'annonce très médiatique de l'acceptation par WikiLeaks et son fondateur J. Assange des BTC en paiement (Banque de France 2013, p. 4). Ce cours devient à la fois dépendant du traitement médiatique comme de la santé des passerelles\*, encore peu nombreuses, permettant sa connexion à l'économie réelle : des problèmes de sécurité avec les hacks rencontrés par MtGox (178000 BTC sont perdus, Sedgwick 2019g; Sedgwick 2019h, d'autres attaques suivront) produiront un « flash crack » en juillet (voyant le BTC passer de 32\$ à 0,01\$ en quelques jours) (*Ibid.*; BitMEX Research 2018). Pour le développement infrastructurel de Bitcoin, l'entrée de WikiLeaks est aussi décisive que complémentaire de celle de MtGox. L'un modifie l'offre des UCN\*, l'autre touche à leur demande, et ce, de manière potentiellement importante au vu de sa renommée et de son réseau\*. Ce n'est pas pour rien que, en mai 2010, Nakamoto avait fait valoir, sur un ton inaccoutumé, qu'il ne mettrait pas en péril le réseau\* pour une extension trop rapide et précipitée de son usage, contrairement à des utilisateurs pressant WikiLeaks d'accepter les BTC (Nakamoto 2010f; Sedgwick 2019e).

Durant cette première phase, la confidentialité de Bitcoin est moins un défaut qu'une nécessité : la croissance du réseau\* doit être lente et harmonieuse et non relever de la seule volonté d'acteurs atomisés. La sécurité de Bitcoin en dépend. Pour preuve, le pénultième message de Nakamoto répond au surcroît d'intérêt causé par un article du journal grand public, *PC World*, sur l'intérêt de WikiLeaks pour Bitcoin, dont l'intérêt qu'il suscite fait planter le site Bitcointalk. Nakamoto y déclare, avant de disparaître, qu'il « *aurait été bon d'attirer cette attention dans un autre contexte. WikiLeaks a donné un coup de pied au nid de frelons, et l'essaim se dirige vers nous.* » (Nakamoto 2010g ; Sedgwick 2019d) Cette publicité extérieure offerte est à l'image d'un premier mouvement où la figure centrale de Nakamoto s'estompe à

<sup>137</sup> En février 2010, visant à dépasser l'absence de cotation, « *NewLibertyStandard propose sur Bitcoin Talk une modélisation d'un prix des BTC déduit du coût énergétique du minage. L'échange entre Malmi et « NewLibertyStandard » au taux de 0.00099\$/BTC* » (Sedgwick 2018b), ou la cotation en continu produite par « *Bitcoinmarket.com* » (Sedgwick 2018b) restent pour le moins éloignés des canons du prix d'équilibre et du marché parfait (liquide et profond) théorisé par la science économique.

<sup>138</sup><https://news.slashdot.org/story/11/02/10/189246/online-only-currency-bitcoin-reaches-dollar-parity>  
[consultation au 21/09/2018].

mi-période. Émancipé de son créateur, Bitcoin continue d'évoluer et d'attirer, de proche en proche par-delà ses premiers cercles, des entrants plus diversifiés.

### La phase de « péché » (d'avril 2012 à octobre 2013)

Avec WikiLeaks, Bitcoin dépasse le statut de preuve de concept, démontrant pratiquement ses ambitions de système de paiement alternatif : il s'érite en canal financier et monétaire auxiliaire, relai de dernier ressort des flux économiques de l'organisation en contournement de sanctions qui tentaient de l'en priver. Sorti de son isolement relatif, émancipé de son concepteur, il entre à partir d'avril 2012 dans sa « phase de péché ». Cette période se caractérise par un changement de régime transactionnel, marqué par une intensification des transactions\* non liées à l'activité de minage, où Bitcoin s'affirme comme moyen de paiement. D'abord pour des activités illégales ou tout du moins hautement encadrées par la société, cachant le développement de services, eux, à visées légales (Tasca et Liu 2018, p. 35). Les jalons précédemment posés, ainsi que leurs codes libres et ouverts, sont des fondations sur lesquelles il est facile de créer. Les recherches passées (en bleu foncé) conduisent à des développements dans le domaine du protocole, en l'absence même de Nakamoto : la « *BIP n°16* », la « *BIP n°39* » (en rouge) donnent lieu à une série d'innovations attendues dans les domaines des portefeuilles\* et des paiements (en orange), ouvrant un éventail diversifié de services en termes de sécurité, de simplicité et d'usabilité : les solutions multi-signatures<sup>139</sup>. Bitcoin pourra dès lors s'intégrer plus solidement (verticalement et horizontalement) à l'infrastructure monétaire et financière existante. Cela conduira, par vagues, à des développements plus nombreux et rapides, dont émergent des arrangements et des systèmes plus ou moins alternatifs, sous le coup d'une concurrence accrue fragmentant un écosystème qui passe de 18 à 22 segments entre 2012 et 2013 (Rauchs 2016, p. 54-57). Aux développements endogènes de Bitcoin s'ajouteront des innovations plus exogènes, comme avec les nouveaux protocoles de registre\* distribué portant de nouvelles UCN\* (*Meta protocole* et *Altcoins\**, cf. section 1.3 suivante). Cet accroissement soutient, de même qu'il en est le produit, le développement de poches d'*« early adopters »* qui, à l'occasion de contacts matériels et idéels situés, conduisent à une diversification des profils d'acteurs. Aux premiers Cypherpunks s'ajouteront des libertariens, des consommateurs de drogue, des technophiles, mais aussi, par intérêt plus économique qu'idéologique, des traders, des investisseurs et des entrepreneurs.

À l'image de WikiLeaks, les premières activités qui se développent touchent à des activités socialement encadrées, très réglementées et moralement, voire légalement, condamnées - marchés noirs et de jeux d'argent. Et comme Assange, les acteurs à l'œuvre se revendiquent encore Cypherpunks, crypto-anarchistes et libertariens. « *SilkRoad* », sorte d'*ebay* de la vente de produits illégaux (narcotiques, faux papiers, etc.) et le jeu en ligne « *Satoshi*

---

<sup>139</sup> Pour simplifier, notre présentation a fait comme si Bitcoin n'avait qu'un type de standard transactionnel. Pourtant, Nakamoto a conçu Bitcoin dès l'origine « *pour qu'il prenne en charge tous les types de transactions possibles et imaginables* » et ce, pour « *éviter de futures modifications majeures* » : « *Transactions de dépôt fiduciaire, contrats cautionnés, arbitrage par un tiers, signature multipartite, etc.* », dont le développement dépendra de son succès (Nakamoto in Champagne 2014, p. 159-160). La BIP 16 introduit le standard de transaction « *pay-to-script-hash* » qui inverse la charge de la preuve d'accès au UTXO « *de l'expéditeur des fonds au receveur* », permettant « *aux commerçants, aux bourses et aux autres logiciels* » la prise en charge de transactions multi-signatures. Implémentée dans la version logicielle Bitcoin d'avril 2013, elle est intégrée dès août par l'entreprise BitGo dans une solution de garde (O'Brien 2014) et essaime (Bitpay, Coinbase, etc). La BIP 39, elle, permet de dériver les clefs cryptographiques d'une phrase lisible par les humains, facilitant leur gestion sécuritaire. Des offres sans conservation simples et diversifiées apparaissent, comme le client léger « *Dark wallet* », développé à l'adresse d'utilisateurs non techniciens par des Cypherpunks reconnus (C. Wilson, A. Taaki ou V. Buterin), offrant un portefeuille\* sans conservation, open source, intégré aux navigateurs Internet, intégrant des options de confidentialité (« *mixing* » et masquage d'adresse, Castillo 2013; Kallenborn 2014).

Dice » sont représentatifs de cette phase « de péché ». Bitcoin est d'abord perçu comme « *un truc cool et nerveux, pas juste un autre PayPal* » et l'engouement à son égard « *concernait principalement le contournement des contrôles* » pour des usages « *exotiques* » (May 2018), déjà décrits et prescrits dans les écrits Cypherpunks (le "BlackNet" de May, 1992; 1994). C'est tôt qu'au sein de la communauté Bitcoin ce type de marché fut discuté, suivi par de premières implémentations<sup>140</sup> : le bientôt prospère « Silk Road », lancé à la phase précédente, affirme être un système militant, et le fondateur Ross Ulbricht se réclame d'un libertarianisme (Sedgwick 2019i) pour lequel les prohibitions nationales ne sont ni efficaces, ni légitimes, d'où sa volonté de les remplacer par une logique de « marché libre » dans la mesure où l'échange est consenti et ne dérange personne (Musiani, Mallard et Méadel 2018, p. 145-146). Inscrits dans ces raisonnements, les sites de jeux d'argent connaissent aussi un développement explosif, dont « SatoshiDice »<sup>141</sup> est à l'avant-garde (Buterin 2013c). La part agrégée de ces activités « pécheresses » culmine sur la période à près de 51% des activités observées *on chain\** (Tasca et Liu 2018, p. 37) et quoique l'on en pense, ce sont là de nouveaux succès pour Bitcoin. En 2013, il aura servi à générer mensuellement près d'1,2 million de dollars en revenu vendeur via « Silk Road », soit 92 000 USD en commissions pour ses opérateurs (Christin 2013, p. 1) et 300 000 dollars pour « Satoshi Dice » (Buterin 2013a), dont la vente en cours d'année rapporte 12.4 millions (Voorhees 2013). Ces activités éclairent les propriétés tant vantées de Bitcoin, comme leurs dimensions relatives et relationnelles. Mais les dimensions de transparence, de programmabilité, de pseudonymat, de « résistance à la censure\* » ne sont ni pleines, ni suffisantes. Ces services reposent sur une chaîne d'intermédiation et de responsabilité complexe, faite d'une multiplicité d'arrangements sociotechniques disparates - liaison au système bancaire, infrastructure centralisée, etc. – qu'il sera possible de remonter dans le cas Silk Road (Musiani, Mallard et Méadel 2018, p. 146-147)

Du reste, à ces succès qui essaient<sup>142</sup> se mêlent des revers médiatiques et politiques : l'écho du premier article sur Silk Road de Chen (2011) conduit, fin 2013, à la saisie du site et à l'arrestation du créateur (Musiani, Mallard et Méadel 2018, p. 145). Cela précipite le déclin des flux attribuables à des activités illégales, ne comptant plus que pour 3% du total en fin de période (Tasca et Liu 2018, p. 37). Attention aux effets loupe, pendant que Bitcoin sert à des activités illégales, s'en développent d'autres à visées légales, dont l'essor *on chain\** éclipse les

---

<sup>140</sup> Dès 2010, un utilisateur de Bitcointalk s'interroge sur les modalités de fonctionnement d'un marché dédié à l'héroïne : « *en tant que libertarien, ce que j'aime le plus dans le projet Bitcoin, c'est la possibilité qu'il soit vraiment perturbateur [...]. Je pense que la prohibition des drogues est l'une des choses les plus néfastes pour la société [...] et j'aimerais donc faire une expérience de réflexion sur la façon dont un magasin d'héroïne pourrait fonctionner, en acceptant les bitcoins, et en mettant fin à la prohibition des drogues dans le processus* » (« Teppy » cité par Sedgwick 2019i). Cet échange pose les bases de SilkRoad - de l'utilisation de Tor, à l'acheminement des colis, etc. – et si on ne sait pas si son créateur s'en est inspiré, il est établi que, « *dans les deux mois qui ont suivi l'apparition du fil, il avait commencé à travailler* » à son élaboration. Les commentaires étaient prudents et prémonitoires : « *si c'est assez médiatisé, vous vous ferez quand même arrêter d'une manière ou d'une autre* » (*Ibid.*).

<sup>141</sup> Le site Internet, lancé le 24 avril 2012 par le très libertarien Eric Voorhees (Miles et Voorhees 2017; McCormack et Voorhees 2019), n'est pas le premier jeu d'argent à user de Bitcoin, un jeu de poker en ligne l'a fait en 2010, mais l'activité suscitée n'est pas comparable (Sedgwick 2019j). Il permet aux utilisateurs, sans autre identifiant qu'une adresse Bitcoin, d'envoyer des BTC à différentes adresses représentant des cotes - envoyer 1 BTC à celle donnant un gain double avec une probabilité de 48% de chances de gagner (Buterin 2013c). Sa simplicité d'usage, là où utiliser « *des virements bancaires serait non seulement illégal[], mais aussi terriblement lent[]* », lui permet quelques jours après son lancement de compter pour près de 40% de l'activité *on chain\** : le résultat est rapide et « équitable », un générateur de nombres aléatoires à « équité prouvée » est utilisé pour les tirages, desquels les gagnants reçoivent automatiquement leur gain à l'adresse utilisée (Le Calvez, 2020).

<sup>142</sup> Après « Silk Road », de nombreuses plateformes aux offres et propriétés différencierées sont apparues (Tasca et Liu 2018, p. 37), comme « Satoshi Dice », qui voit émerger une myriade de concurrents plus ou moins originaux (voir Buterin 2013a).

premières. En parallèle, la visibilité de la nouvelle CM grandit. Aux forums et blogs individuels s'ajoutent des publications spécialisées comme *Bitcoin Magazine* (*Ibid.*, p. 55, Castillo 2013) et les titres généralistes s'emparent définitivement de ce stupéfiant Bitcoin. Le démantèlement de Silk Road illustre l'irruption du domaine de la conformité aux réglementations nationales (en bleu clair) comme l'ambivalence de la période : l'État, qu'Ulbricht excluait de l'équation (Musiani, Mallard et Méadel 2018, p. 146), s'y impose. Les premières publications et mises en garde (European Central Bank 2012, par exemple) poussent à l'émergence de premiers services de conformité guidant les entreprises à respecter un cadre réglementaire encore flou (*Know Your Consumer* ou KYC et *Anti-Money Laundering* ou AML, par exemple *Ibid.*, p. 58). En outre, aux raisons réglementaires participant du déclin de « Satoshi Dice » (interdiction de l'accès aux utilisateurs américains) s'ajoute l'augmentation des coûts de transaction\* (Le Calvez 2020). Cet enchérissement traduit une demande d'espace d'enregistrement excédant celle offerte par Bitcoin, tirée de l'essor des activités financières (Tasca et Liu 2018, p. 33), découvrant pour la première fois les contraintes de montée en charge de Bitcoin (dite de « scalabilité » et autour desquelles de futures CM essaieront d'apporter des solutions, cf. section suivante). L'extension de la sphère d'usages (en vert) est d'abord due à l'élargissement des services monétaires et financiers (Rauchs 2016, p. 54-58) : introduction de comptes épargne, de cartes et services de paiement (pour consommateurs et entreprises, offrant une conversion directe en monnaie nationale), de distributeurs de BTC, de plateformes de financement participatif et de transfert de fonds. Aux usages financiers s'en s'ajoutent d'autres : lancement de l'API de « Blockchain.info », de services de notarisation utilisant Bitcoin pour horodater, certifier et suivre l'existence de données. Les recherches protocolaires vont au-delà de Bitcoin *stricto sensu* et conduisent à l'apparition d'innovations de métaprotocole visant une extension de ses usages non financiers (Omni/Mastercoin, Counterparty, en rose dans la chronologie, Rizzo 2015). Face à ce resserrement réglementaire, à l'image pour longtemps ternie par des usages illégaux qui pourtant se marginalisent et aux enjeux d'une montée en charge de l'infrastructure Bitcoin, s'opposent de premières volontés collectives : fin 2012 est lancée la « Fondation Bitcoin », incarnation formelle d'un écosystème et de son intérêt (comme conçu par ses membres tout du moins) et un comité interprofessionnel est créé en juillet 2013 (« *Digital Asset Transfert Authority* » (Bitcoin.fr). La fondation vise à soutenir son développement matériel et symbolique (financement de développeurs\*, standardisation, promotion, lobbying, etc.) et illustre parfaitement l'interconnexion encore grande entre les différents acteurs structurant l'écosystème<sup>143</sup>. À l'usage croissant de ces UCN\* répondra un accroissement de leur valeur d'échange. Si le cours reste sous les 20 dollars jusqu'en mars 2013, il connaît par la suite des fluctuations d'ampleur poussant sa « capitalisation » au milliard de dollars, suivant qu'il s'érige pour un temps comme « valeur refuge » à l'occasion de la crise

---

<sup>143</sup> Les premiers développements du protocole reposaient sur les ressources propres et les dons reçus par les contributeurs volontaires. La Fondation Bitcoin, société à but non lucratif créée fin 2012, représente une tentative d'acteurs de l'écosystème d'instituer une représentation collective formelle et de répondre d'une voix coordonnée à certaines problématiques cruciales : assurer un financement pérenne de la maintenance du protocole (en centralisant des dons) et « *standardiser, protéger et promouvoir le développement et l'adoption de Bitcoin dans le monde entier* » (Bitcoin Fondation 2013; 2014). Son conseil d'administration est constitué de personnalités comme M. Karpelès, CEO de la bourse MtGox, le développeur G. Andresen, ou encore Charlie Shrem (condamné dans l'affaire Silk Road pour son rôle dans le blanchiment *via la bourse "The Company"* où, ironiquement, il était en charge de « *la conformité de la société avec les lois fédérales et autres contre le blanchiment d'argent* », Musiani, Mallard et Méadel 2018, p. 147 et 153, note 12). La tentative tourne court et, à la suite de sa faillite, le financement du développement de Bitcoin sera dès lors porté de manière disparate par « *la Digital Currency Initiative du MIT Media Lab* », par l'entreprise privée « *Blockstream* » d'Adam Back et, plus généralement, par du capital-risque (Rauchs 2016, p. 12).

chypriote (ce cours bondit à 230 \$ en avril, Banque de France 2013, p. 3)<sup>144</sup>. Ce cours permet de démontrer encore sa dépendance aux aléas infrastructurels exogènes par rapport aux qualités protocolaires de Bitcoin : en mai, il chute à 76 \$ suite à une attaque par déni de service (DDOS, Sedgwick 2020a) rencontrée par MtGox, et la fermeture par le FBI du site SilkRoad est aussi l'occasion d'une chute brutale (*Ibid.*).

« Silk Road » et « Satoshi Dice » sont symptomatiques d'une phase charnière et transitoire du développement de Bitcoin. Pour autant que ces activités y prennent une place matérielle et symbolique importante, leur décrue s'est accompagnée d'évolutions radicales de l'écosystème qu'il ne faut pas escamoter. Le développement infrastructurel de Bitcoin se décentre de son orbite à mesure que des acteurs plus hétérogènes en valeurs et intérêts s'y joignent, pour y établir des activités moins militantes et sensationnalistes. Les arrangements sociotechniques qu'elles nécessitent d'élaborer (plus normalisés) permettront à Bitcoin, *via* ses services et passerelles\*, une bien meilleure intégration à l'infrastructure monétaire et financière existante que par le passé, intégration qui s'opère en phase de maturation.

### **La phase de « maturation » (de novembre de 2013 à aujourd’hui)**

Fin 2013, grâce aux activités précédentes, Bitcoin débute l'ultime période de son développement infrastructurel : la phase de « maturation ». Son usage pour des activités illégales ne disparaît pas, mais évolue et se marginalise (les attaques informatiques, les arnaques et les vols domineront) : les transactions\* impliquées comptent pour moins de 1% de l'ensemble entre la fin 2013 et 2018 (Chainalysis Team 2019, p. 3 et 11). Le régime transactionnel qui s'ouvre est marqué par une diversification d'usages légaux, desquels les activités financières sortent triomphantes. L'usage de Bitcoin croît tendanciellement - comme l'indique le nombre de transactions\*, d'adresses actives ou de comptes ouverts sur « Coinbase », une des plateformes d'échange les plus importantes (en violet, voir aussi Annexe n°2). Le développement de Bitcoin et de l'écosystème des CM se poursuit jusqu'à aboutir à un plateau : la croissance des entrants de 2014 ralentit en 2015, année d'un retournement de marché conduisant à une pléthora de sorties. À partir de cette année 2015, la structure de marché change peu : en 6 ans, 22 segments de marché ont été créés (seuls 4 nouveaux émergent de 2013 à 2015, Rauch 2016, p. 60).

Parmi les derniers segments de l'écosystème apparus, on compte les marchés prédictifs, de nouveaux services et logiciels à visée de conformité, la sécurisation des portefeuilles\* qui progresse avec les premiers portefeuilles\* physiques - Trezor (SatoshiLabs 2019) suivi dès 2014 par Ledger, une firme française devenue leader du secteur [Entretien n°8]. Le secteur financier est incontestablement le plus dynamique : sa part dans l'ensemble des transactions\* *on chain\** ne cesse de s'accroître et le segment bourses d'échange est le premier chaque année en nombre d'entrants (Rauchs 2016, p. 66; Tasca et Liu 2018, p. 37). Suivant un recouvrement d'une logique financière et par leur rôle stratégique de passerelle\*, sas de convertibilité obligé des flux d'investissement, ces bourses s'érigent en acteurs centraux de la valorisation et de la circulation (*on chain\** et *off chain\**) des UCN\* Bitcoin. La plage de services qu'elles offrent est grande et les acteurs d'hier, comme E. Voorhees, à qui l'on doit « Shapeshift », première plateforme d'échange sans conservation, sont concurrencés par des acteurs aux profils différenciés. L'intérêt grandissant d'investisseurs institutionnels pousse à faire des UCN\* BTC

---

<sup>144</sup> Il est rapporté que des utilisateurs auraient usé de Bitcoin afin d'éviter les contrôles de capitaux nouvellement instaurés : de fait, la crise conduit à une augmentation du nombre de recherches concernant Bitcoin, du nombre de téléchargements de logiciel client (Cuny 2013) comme à la création d'un des premiers distributeurs de Bitcoin (“Bitcoin ATM”, Berwick 2013).

des instruments financiers comme les autres : de manière très indirecte d'abord, par simple publication de données de prix agrégées (Nasdaq fin 2013, suivi par le NYSE en 2015), plus directement ensuite, par la création de produit financier spécifique par des acteurs reconnus (marchés futurs par le *Chicago Board Option Exchange* ou le *Chicago Mercantile Exchange*, courant 2017). En outre, l'établissement de liaisons toujours plus nombreuses, diversifiées et solides améliore l'interopérabilité de Bitcoin, non seulement avec le système monétaire et financier traditionnel, mais aussi avec la constellation de systèmes alternatifs apparue autour de lui et à laquelle il s'articule pour former une infrastructure de périmètre supérieur (cf. les métaprotooles et autres *Altcoins\**, en rose, cf. section suivante). L'année 2015 est bien charnière, et la popularité des applications non monétaires grandit suivant que des acteurs financiers, relayés par de grands médias généralistes, font leur publicité : l'important ne serait pas les UCN\*, comme le BTC pourtant au centre du consensus sociotechnique, mais une « technologie de blockchain » qui, proche des consensus « classiques », pourrait s'en passer...<sup>145</sup> Nombreuses sont les entreprises de l'écosystème à pivoter vers de nouveaux protocoles de registre\* distribué et d'UCN\* que la période voit exploser (Rauchs 2016, p. 77). En ce début de période, Bitcoin est encore pour un temps l'astre central de cet univers en expansion et, avant d'être remplacée par les *stablecoins*, c'est son UCN\* qui y tient le rôle d'étalon pivot : en tant que principale paire d'échanges, elle sera le vecteur de l'interpénétration des marchés de CM et cryptoactifs. Le métaprotoole *Omni/Mastercoin*, protocole de surcouche ajoutant des usages non monétaires à Bitcoin, ouvre le bal. Il fait des UCN\* BTC le seul véhicule d'investissement et d'usage de son écosystème : elles sont les seules acceptées lors de sa levée de fonds - ainsi débute le phénomène des « Initial Coin Offering » (voir Annexe n° I.4, pour une Chronologie circonstanciée) - et utilisables en paiement des frais de transaction\* liés à l'usage de son protocole. Ce métaprotoole va permettre l'émission du premier *stable coin* indexé au dollar, le « *Tether* » (USDT), catégorie d'actif dont l'importance infrastructurelle sera croissante<sup>146</sup>. De même, plus tardivement, le protocole Ethereum lancé sur la période se finance via une levée de fonds en BTC ; il abrite l'éclosion d'une multitude d'usages et d'espaces de conversation / circulation pour les UCN\* BTC en propre ou sous forme de représentations synthétiques (des IOU, comme avec le « *Wrapped Bitcoin* », par exemple<sup>147</sup>). Et aux services financiers *off chain\** offrant déjà des usages en dépôt ou en garantie des BTC s'ajoutent dès lors une multiplicité de

---

<sup>145</sup> Cette idée, popularisée par des slogans comme « *Forget Bitcoin, embrace blockchain\** » ou « *It's all about the Blockchain\** », émane d'acteurs de la finance traditionnelle, en l'espèce Blythe Master de JP Morgan dans Bloomberg (Massa 2015) ; voir aussi l'article de *The Economist* d'octobre 2015 : « *The Trust Machine : How the technology behind Bitcoin could change the world* ».

<sup>146</sup> Premier actif synthétique dont la valeur nominale est adossée au dollar, il est une reconnaissance de dettes émises sous forme de jeton par une entreprise, entité légale centralisée, qui conserve les collatéraux en dollars déposés par les usagers. Cette entité est censée garantir le parfait adossement de ces IOU au dollar tenu en compte. Ce type de jeton permet aux places d'échange ne bénéficiant pas de passerelle\* formelle en dollars (donc soumises à des régulations plus faibles) une forme d'externalisation : cela permet d'étendre et de faciliter leurs activités de trading sans qu'elles aient à gérer en propre l'établissement de ces passerelles\*, puisque le dispositif de l'USDT le fait pour elles. À côté de cette famille de *stable coin* adossée aux fiat monnaies et administrée centralement (dont de nombreux émetteurs concurrents à Tether existent aujourd'hui), une autre forme a été développée : adossée à des CM, leur administration relève de *smart contract\** dont l'administration est plus ou moins décentralisée. Dans ces cas, un usager séquestre des CM dans un script à exécution programmatique\* dédié, qui lui autorise à tirer des lignes de crédit en UCN à hauteur d'un certain pourcentage de la valeur dudit collatéral, cette valeur servant à garantir celle des UCN émises (le collatéral est liquidé automatiquement si tant est que sa valeur chute en deçà d'une limite *ad hoc* définie par le protocole en question et ce, afin d'éviter la constitution de mauvaise dette, cf. la valeur des UCN émises deviendrait supérieure à celle des collatéraux servant de garantie).

<sup>147</sup> Assez semblable à l'USDT, ce jeton est une reconnaissance de dette émise via le protocole Ethereum par une entité centralisée (un consortium regroupant Bitgo, KyberNetwork, etc.) qui reçoit des UCN BTC et émet en retour, à l'adresse de l'envoyeur et à parité, le cryptoactif WBTC (Redman 2019b).

solutions hybrides, plus largement *on chain*\* comme la fourniture de liquidité, des dépôts rémunérés, la collatéralisation de prêt, etc.

Comme pour de nombreuses infrastructures, la concurrence et la fragmentation de l'écosystème n'ont cessé de s'accroître sans qu'aucun vainqueur ne s'impose (Edwards *et al.* 2009, p. 367). Mais le décentrement amorcé durant les phases précédentes aboutit à un basculement : le développement de Bitcoin a atteint sa vitesse de libération (l'*« escape velocity »* des ingénieurs). Pour autant qu'il était encore comme poussé par-derrière par des acteurs issus du cénacle Cypherpunks originel, il est désormais comme tiré par devant et de l'extérieur par des centres de gravitation aux préoccupations hétérogènes et moins militantes, dont font partie les acteurs financiers et les régulateurs qu'il était censé supprimer. Preuve de ce changement d'orbite infrastructurel, le financement de l'écosystème : ces acteurs bancaires et financiers y prennent part à l'origine afin de développer des protocoles de type fermé, à consensus plutôt classique. Les banques centrales ne sont pas en reste<sup>148</sup>. Le financement interne sur fonds propre, majoritaire dans les phases précédentes, est supplanté par des flux d'investissements en capital-risque, dont la croissance a débuté en 2013 (Rauch, 2016 ; Tasca et Liu 2018) et ne cesse de se poursuivre aujourd'hui<sup>149</sup>.

Au développement matériel de ces infrastructures répond celui de la valeur de leurs UCN\*, apparaissant épisodiquement comme de nouveaux eldorados, au gré de la médiatisation des variations de cours, des gains colossaux réalisés par quelques-uns (dont le cas WikiLeaks et d'Assange, qui s'enorgueillissent de « *50 000% de rendement sur le bitcoin grâce au gouvernement américain* », est emblématique, Kharpal 2017), ou de l'entrée d'acteurs importants (grandes entreprises, banques, etc.). Ces objets offrent une nouvelle classe d'actifs de portefeuille, un marché pour des produits financiers spécifiques<sup>150</sup>, et même de nouvelles voies de financement mal réglementées. De quoi participer d'un engouement général et d'anticipations haussières, de même qu'aiguiser les appétits d'investisseurs occasionnels et professionnels, pour qui volatilité rime avec opportunités. Dès le début de période, le BTC connaît une envolée importante de son cours (en décembre 2013, il culmine à près de 1000 \$) suivant une intervention, largement médiatisée, marquant un affermississement de sa reconnaissance par les États : le 19 novembre 2013, la Commission du Sénat américain organise une session d'information où interviennent des membres de la « Bitcoin Foundation » (Banque de France 2013, p. 4). De 2014 à 2017, son cours stagne en dessous des 1000 \$, seuil qu'il ne dépasse qu'en début d'année 2017, au cours de laquelle son prix de marché est multiplié par 20 (culminant à près de 20 000 \$ fin 2017) avant, là encore, de connaître une baisse importante durant 2018 et 2019, pour atteindre un point bas d'environ 3300 \$. Durant 2019 et 2020, son cours, bien qu'erratique, se stabilise vers les 8000 \$. Ces cycles impressionnantes de « bull and bear » cachent une tendance du cours haussière et, de 2013 à 2020, son cours, comme les volumes échangés sur les places d'échange et transitant par le réseau\*, sont en hausse régulière (Annexes n°II). Ces systèmes de marché, mieux développés qu'en première période, restent

---

<sup>148</sup> La *Bank of England*, pionnière, publia sur ces questions dès 2013 (Ali *et al.*, 2013) et effectua tôt des recherches concernant des protocoles de Monnaie Digitale\* de Banque Centrale (CBDC) (Danzeis & Meiklejohn, 2015).

<sup>149</sup> Durant les deux premières années du développement de Bitcoin, les projets et les firmes avaient recours à un financement interne. En 2012, les premiers fonds de capital-risque font leur entrée et, dès lors, ce type d'investissement ne cesse de croître et d'irriguer des acteurs plus nombreux : les 2,1 millions de dollars d'investissement réalisés en 2012 apparaissent bien modestes en comparaison des 93 millions investis en 2013 dans 38 entreprises ; des 369 millions dans 69 entreprises de 2014, des 448 millions de 2015, répartis entre un nombre record de 96 entreprises (Rauch 2016, p.70-71). L'entreprise Coinbase réalise la plus grande levée de fonds d'alors avec 75 millions de dollars.

<sup>150</sup> Par exemple, ouverture de marchés au futur que ce soit par le Chicago Board Option Exchange (Cboe) ou le Chicago Mercantile Exchange (CME), tentatives de création de produits d'investissement de type ETF, etc.

comparativement aux marchés traditionnels peu profonds et liquides, conférant à certains acteurs (places d'échange et/ou traders) un poids déterminant sur les volumes et les prix<sup>151</sup>. Cause et effet de cette valorisation de cours, l'accroissement de la demande transactionnelle de Bitcoin se poursuit à partir de 2013, et augmente brusquement courant 2017. Par son succès, Bitcoin doit supporter un nombre d'utilisateurs actifs croissant (mesuré *on chain*\* via le nombre quotidien d'adresses actives uniques ou *off chain*\*, par le nombre de comptes utilisateurs de la bourse Coinbase ; cf. Annexe n° II et I.3), saturant ses capacités de traitement. Cela conduit en retour à une nouvelle poussée haussière des frais de transaction\*. Vanté comme rapide et peu coûteux, son usage devient lent et cher, questionnant la viabilité de certaines des activités qui s'y sont construites...

Finalement, maturation n'est pas maturité : le développement infrastructurel est un processus dynamique auto-entretenu, et les développements passés tracent des voies différencierées qui dépendent de renégociations et de conflits à venir. Cette problématique ancienne de la montée en charge de Bitcoin (ou *mise à l'échelle*\*) devient structurante pour une telle infrastructure, dont les ambitions de système de paiement se heurtent à des limites internes alors que, dans le même temps, elle est de plus en plus contestée par des systèmes concurrents. La réactivation pour le moins conflictuelle de cette question en 2017 est symptomatique. Et comme pour prouver qu'un développement infrastructurel ne suit jamais de chemin univoque tracé à l'avance, voilà que le conflit entourant le « *scaling debate* » débouche sur un « *Fork*\* *contentieux* », une évolution des règles protocolaires canoniques, non unanimement consenties : face à un carrefour sociotechnique dont chaque chemin porte des coûts d'opportunités et de dépendance au sentier, la fixation d'un tel cap de développement futur se paye au prix d'un schisme protocolaire et communautaire retentissant, où la majorité garde Bitcoin et les autres créeront une CM concurrente, Bitcoin Cash (cf. Chap. III). Cet évènement d'ouvrir aussi la voie à des innovations sur Bitcoin, en particulier l'émergence de protocoles de surcouche (dit de « *layer 2* ») comme le « *Lighning Network* » (LN, en rouge), implanté en 2018 et dont les *bitcoiners*\* promettent qu'il résoudra de nombreux problèmes liés à la montée en charge (quantité de transactions\*, temps de traitement, coût, confidentialité, etc.)<sup>152</sup>. Problèmes que les nombreux autres protocoles de registre\* distribué concurrents, comme Ethereum, ambitionnent de corriger pour le supplanter.

---

<sup>151</sup> Largement non régulées, elles ont vu se développer des pratiques qui seraient illégales sur les marchés financiers traditionnels. Des manipulations de cours ont été décrites par des travaux académiques et pourraient expliquer en partie les pics de 2013 [Gandal & Al., 2018] et de 2017, impliquant la plateforme Bitfinex, voir <https://www.nytimes.com/2018/01/31/technology/bitfinex-bitcoin-price.html> [consultation au 11/11/2022].

<sup>152</sup> Lightning Network (LN) est un protocole de paiement en surcouche de Bitcoin formalisé dès 2015 par Joseph Poon et Thaddeus Dryja (<https://web.archive.org/web/20150228162703/http://lightning.network/> [consultation au 24/08/2020]), permettant des paiements très rapides (quasi instantanés) et peu onéreux. Ce réseau construit sur Bitcoin permet à ses utilisateurs de réaliser des transactions *off chain*\* en utilisant Bitcoin comme chambre de compensation périodique uniquement. L'usage applicatif est permis par un standard de transaction particulier dit « à durée déterminée » (« Hashed Timelock Contract » ou HTLC) : l'utilisateur crée une adresse Lightning et la charge en UCN via une transaction Bitcoin de « Layer 1 » de ce type. Ensuite, il appartient aux utilisateurs d'ouvrir des canaux de paiement bidirectionnel entre eux, permettant in fine à tout paiement de se frayer un chemin à travers les canaux de paiement ainsi constitués. La première implémentation logicielle de ce système est publiée en mars 2018 par « Lightning Labs », entreprise fondée par des *bitcoiners*\* de la première heure rejoints par des investisseurs comme Jack Dorsey (PDG de Square, ex CEO de Twitter), David Sacks (ancien directeur général de PayPal), ou encore Vlad Tenev (co-fondateur de Robinhood, Torpey 2018). Après la première année de son lancement, LN compte déjà près de 500 BTC au sein de son réseau, pour une valeur de près de 2 millions de dollars (au 31 décembre). En août 2020, le réseau gère près d'un millier de BTC pour une valeur de près de 11,3 millions de dollars (voir <https://defipulse.com/lightning-network> [consultation au 24/08/2020]).

### I.2.1 Un protocole débordé de « carnavalesques » improvisations d'acteurs

Restitué dans l'épaisseur de son développement historique infrastructurel, Bitcoin ne peut cacher la nature carnavalesque de son développement. Bitcoin et les CM sont des infrastructures composites émergentes, dont les renégociations (faites de détournement et d'inversion) sont opérées par des parties prenantes aux représentations et intérêts hétérogènes. Forme et contenu d'une CM renvoient tant au design initial qu'à la multiplicité des activités et acteurs participant à la (re)définir comme infrastructure. La dimension « carnavalesque » de ce va-et-vient s'établit au-delà de la nature multi-acteurs et multi-niveaux du développement infrastructurel (illustré par la Chronologie 2) : transgression, ironie, inversion sont au cœur d'un développement infrastructurel qui conduit un système destiné à exclure les régulations gouvernementales et les intermédiaires, à être de plus en plus soumis à l'un et à l'autre, *via* les acteurs humains qui en opèrent les espaces de conversion clefs (Kavanagh et Miscione 2017, p. 21). La dynamique est dialectique et, aux forces centrifuges poussant à la décentralisation s'opposent des forces centripètes, poussant en sens inverse. En tant qu'infrastructure sociotechnique, Bitcoin n'est réductible ni aux desseins de son concepteur, ni à ses frontières protocolaires. Nakamoto, pas plus que les autres innovateurs, n'a pu faire preuve d'un réalisme « *divinatoire* » propre à engendrer un objet au fonctionnement « parfait » : Bitcoin comme protocole est soumis à des bogues, des attaques, voire simplement des « inefficiencies » auxquelles des acteurs humains l'adaptent. Plus largement comme CM, il est le fait d'improvisations nombreuses qui, comme dysfonctionnements, soulignent « *l'intervention d'un (f)acteur inattendu* » (Akrich 1989, p. 41). Cette renégociation continue, ontologiquement politique, fait apparaître : d'abord la façon dont, par des contournements d'acteurs, des éléments de réintermédiation sont réintroduits ; ensuite la façon dont le protocole voit ses codes (cristallisation de ses valeurs et les normes politiques) modifiés et adaptés par une communauté connaissant des dissensus.

#### Des renégociations pratiques : réintermédiation de l'accès à Bitcoin et de l'activité de traitement des transactions...

Parmi les diverses improvisations et détournements d'acteurs, attardons-nous sur deux types particulièrement significants : la réintermédiation des conditions d'accès à Bitcoin (portefeuille et bourse d'échange) et celle entourant l'activité de production des enregistrements (émergence de barrières à l'entrée suite à une industrialisation de l'activité, formation de coopératives de minage).

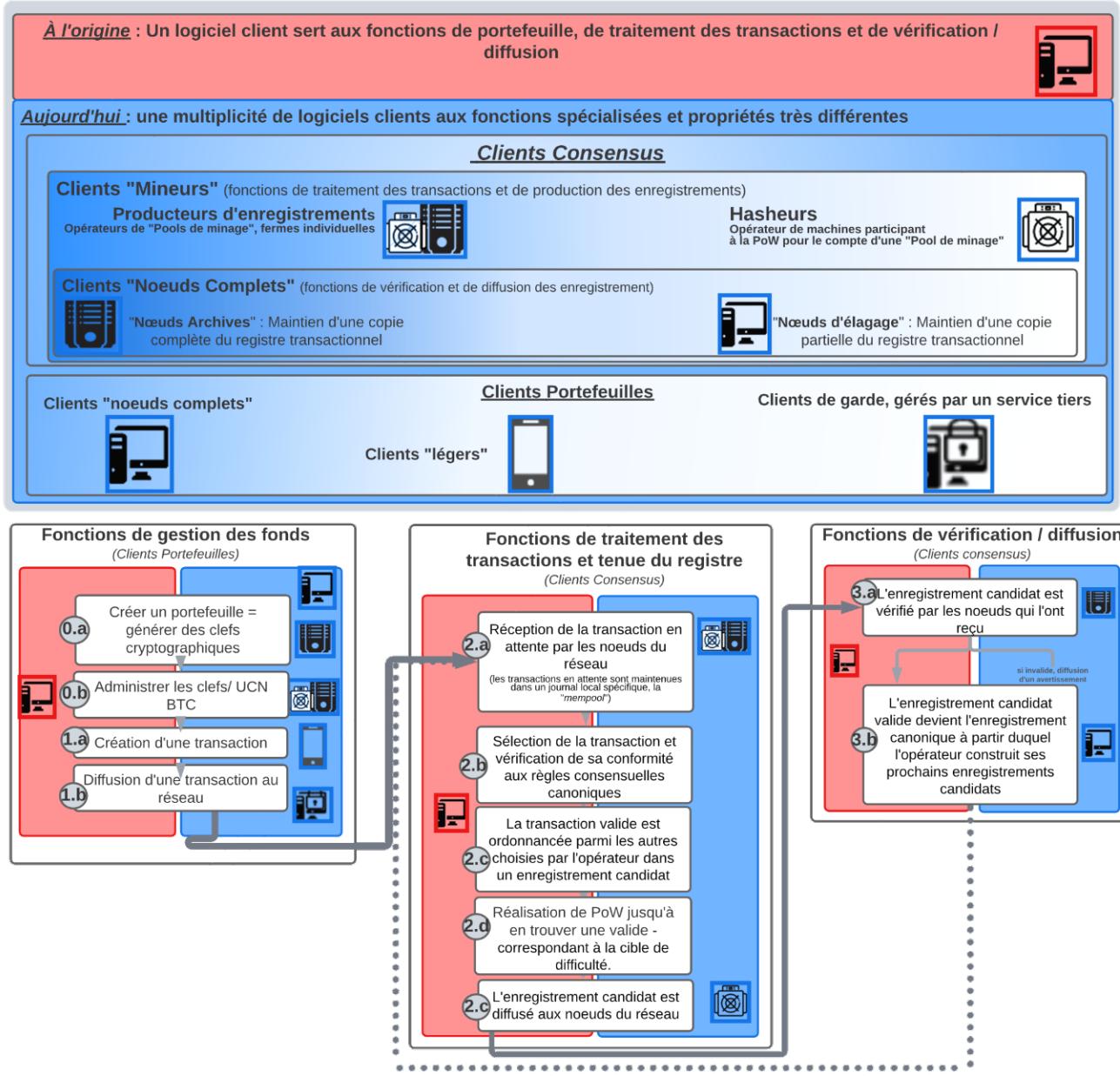
Accéder souverainement à Bitcoin en tant que pair impose d'y participer en propre, *via* un client personnel (client dit « *non custodial* » dans le jargon *coiner*) en capacité de réaliser en propre l'ensemble de ces processus protocolaires. Sans cela, pas de possession « réelle » d'UCN\* : « *not your keys, not your coins* ». La pratique démontre que tous les *bitcoiners*\* ne veulent pas suivre l'injonction d'*« être leur propre banque*», puisqu'elle a comme corollaire de lourdes responsabilités : il faut prendre part à la production de consensus, ou tout du moins à la vérification des transactions\* et à leur diffusion. Dans l'histoire que Nakamoto nous conte et à l'époque de son lancement, Bitcoin est exclusivement accessible par un client logiciel unique, Bitcoin QT dans sa version 0.1, publiée le 9 janvier 2009 et rédigée en langage de programmation\* C++<sup>153</sup>. Tout utilisateur participe à et *use de* Bitcoin *via* ce client logiciel

---

<sup>153</sup> Suivant le choix des langages de programmation utilisés, les performances techniques ou les caractéristiques sécuritaires peuvent être très largement différentes, voir (FreeCodeCamp 2019; Breed 2020; Kumar Jain 2023). Le langage de programmation\* C++, s'il est robuste, n'en est pas moins difficile et peu lisible, car « *plus proche de la machine* » contrairement au langage Python, par exemple [J. De Tychet Entretien n°4]. Nous reviendrons sur ces enjeux dans les chapitres IV et V.

complet qui dispose d'un historique de la chaîne de blocs\* et participe à l'activité de production des enregistrements (Sedgwick 2019f). Le maintien d'un nœud\* n'est pas anodin : aux ressources et compétences requises (d'abord informatives et techniques, rapidement économiques suivant que l'activité de minage rencontre des économies d'échelle vectrices de concentration) s'ajoute une exposition à des risques importants (pertes ou vols par compromission des clefs cryptographiques, monitoring et maintenance du nœud, etc.). Reste que, derrière des codes monolithiques [M. Corallo, Entretien n°15], se cache une hétérogénéité de fonctions relativement indépendantes qui peuvent relever de composants, de processus et d'acteurs différenciés (représentés dans la Figure 5 suivante) : les fonctions liées aux activités de portefeuille, nécessitant un client du même nom ; celles de vérification / traitement des transactions\* et de production des enregistrements impliquant des clients « mineurs » et enfin, celles liées à la vérification / diffusion des enregistrements, qui renvoient à des nœuds\* « complets » (respectivement les étapes 0 à 1, les étapes 2 et les étapes 3, dans la Figure 5). Comme l'illustre la Figure 5, au travers du développement infrastructurel présenté précédemment, Bitcoin a connu un processus de division sociale du travail et chaque acteur – humains et non humains – s'est vu spécialisé suivant des rôles et statuts différenciés.

**Figure 5 : Division sociale du travail protocolaire et spécialisation des acteurs**



Source : Rolland Maël

Notre présentation vise, en les décomposant, à mieux cerner les différents rôles et statuts qui structurent la communauté des *bitcoiners*\*, comme les modalités de leurs interrelations. Si Nakamoto anticipait certains de ces réagencements (administration des UCN\* via des clients portefeuilles\* dits « légers », constitution de fermes industrielles spécialisées dans les activités de minage), les renégociations ne se sont pas faites suivant ses termes et conditions et, par inversion, ce développement a conduit à réintégrer au cœur de Bitcoin hiérarchie, autorité, pouvoir, confiance et délégation.

Nakamoto n'est pas dupé. Si, au lancement de Bitcoin, tout utilisateur doit passer par un client logiciel unique et monolithique, il a conscience que cela représente une barrière à l'entrée pour des utilisateurs qui n'ont cure de l'ensemble des activités protocolaires et qui souhaitent simplement envoyer ou recevoir des UCN\*. Aussi, le WP\* aborde deux types de portefeuilles\* : les portefeuilles\* « nœuds\* complets » et les portefeuilles\* dits « légers » ou « SPV » (pour « Simplified Payment Verification », Nakamoto 2008, p. 5). Pour lancer Bitcoin, c'est le

premier type qu'a implémenté Nakamoto : la création d'une transaction\* nécessite une liste à jour de l'ensemble des UTXO\*, dont dispose le client logiciel complet. En ce sens et en cohérence avec la souveraineté individuelle que Bitcoin promeut, l'utilisateur participe à l'exécution des fonctions de consensus relatives à la validité des paiements qu'il vérifie par lui-même. Une telle solution implique en plus de savoir-faire, un coût de stockage mémoire, puisque ledit historique croît en taille à chaque cycle de mise à jour du registre. Cela, au départ, ne posait pas vraiment problème. Le type de population qui s'intéresse alors à Bitcoin dispose d'un capital culturel adapté et ces coûts étaient peu visibles, car l'historique transactionnel (encore léger) convenait à n'importe quel disque dur. Mais Nakamoto anticipe des contraintes croissantes et décrit un second type de portefeuille moins onéreux pour l'usager : les portefeuilles\* SPV. Selon lui, ils devraient permettre « *de vérifier les paiements sans faire fonctionner un nœud\* de réseau\* complet* » (*Ibid.*). Nakamoto a raison. La montée en charge de Bitcoin passe par le développement de dispositifs logiciels permettant d'envoyer et de recevoir des transactions\* sans pour autant imposer le maintien d'un registre\* transactionnel à jour. Là où il se trompe, c'est sur le fait que ces dispositifs permettront aux utilisateurs de conserver le statut de pair, individuellement souverain. Sa croyance s'est fracassée sur la réalité puisque les solutions trouvées ne permettent pas (pour l'heure du moins) de conserver la capacité du client à « *vérifier lui-même* » les paiements sans « *faire confiance à un nœud\** » tiers (Nakamoto, in Champagne 2014, p. 178) : « *au fur à mesure du temps, les développeurs\* et même le public, moi, on s'est rendu compte que, ben ça va pas marcher en fait parce que on peut pas prouver qu'un bloc n'est pas valide. Il y a plein de détails techniques qui font que en théorie ça marche [...], mais quand on gratte beaucoup ça marche plus* » [A. Le Clavez, Entretien n°20]. L'éventail large de clients légers, développé pour faciliter l'accès à et donc l'usage de Bitcoin à l'endroit de publics moins techniciens, s'est fait au prix de délégations et de recentralisations, que les utilisateurs cibles ne conçoivent nullement comme un problème. Au contraire, éloignés des préoccupations cypherpunks premières, ce sont pour eux des solutions plus simples, facilitant la gestion sécuritaire de leurs fonds.

Citons pour commencer les solutions dites *non custodial*. Bien qu'elles offrent une pleine administration des clefs cryptographiques par l'utilisateur (donc une possession en propre des fonds *on chain\**), elles impliquent de faire confiance à l'opérateur du nœud\* complet auquel elles sont connectées. C'est de lui dont dépend *in fine* l'accès au réseau\* Bitcoin et aux informations transactionnelles. Il pourrait falsifier les informations reçues et faire signer des transactions\* non consenties aux usagers, voire censurer des transactions\* sortantes que les acteurs consentaient à réaliser. De l'autre côté et à l'extrême, se sont développés des types de portefeuilles\* totalement intermédiaires (dits *custodial*). Ici, les utilisateurs finaux, en plus d'affronter les risques précédents, se trouvent privés de la gestion des clefs cryptographiques qui relèvent du seul service tiers : leur compte est un compte *off chain\**. Si le tiers vient à fermer leur compte arbitrairement ou à faire faillite, les utilisateurs n'auront aucun moyen de mouvoir leurs fonds. On retrouve l'idée contenue dans le slogan « *not your keys, not your coins* », qui s'est vu confirmé avec les faillites ou hacks subis par l'écosystème (en violet dans la Chronologie 2) et qui ont laissé de nombreux *coiners\** sans le sou. De telles solutions étaient absentes du scénario de Nakamoto. Suivant sa logique, l'utilisateur « effectif » de Bitcoin n'est ici que le tiers opérant le client nœud\* complet. Qu'importe qu'il le fasse pour le compte de clients, dont il maintient des comptes *off chain\**. Dans leur accès au réseau\*, aux données de transaction\* comme à leurs fonds, ces clients dépendent de ce tiers de confiance qui se tient entre eux et Bitcoin. Mais ces services plus ou moins centralisés, par l'intermédiation, ouvrent en contrepartie la sphère d'usage de Bitcoin et de ses UCN\* au plus grand nombre, ce que le protocole seul n'aurait pu supporter : facilitation et sécurisation de la possession d'UCN\*, services de dépôt et d'investissement, de paiement et de conversion, d'assurance, etc. Si l'intermédiation est pour un problème Nakamoto, comme pour certains *coiners\**, pour d'autres

elle est une solution. Comme pour le système bancaire et financier, l'histoire a montré comment une division sociale du travail et une spécialisation était sinon nécessaire, tout du moins souhaitée par les usagers désirant être soulagés des contraintes de conservation. Comme les marchands et orfèvres d'antan jouèrent un rôle d'institution de dépôts de par leurs compétences et ressources (Galbraith 1976, Chap. 1; Gratsac-Legendre 2017), pourquoi ne pas déléguer la conservation risquée des clefs privées à des acteurs spécialisés disposant de services informatiques dédiés ?

Une autre forme de spécialisation, poussant à une recentralisation, est à l'œuvre pour ce qui est de l'activité de traitement, de vérification et de maintien à jour du registre\* transactionnel (c'est-à-dire l'activité de minage). Le « minage », cœur de la décentralisation et de la « démocratie » du système, s'industrialise et les opérateurs se professionnalisent, suivant que ces dernières nécessitent des équipements plus puissants qu'auparavant. Là encore, Nakamoto avait fait preuve de sagacité et avait anticipé ce type de spécialisation, mais, pour lui, cela ne remettait pas en cause la décentralisation, à l'aune de sa croyance erronée que les portefeuilles\* SPV garantiraient à leurs usagers une pleine vérification. Pour lui, à terme, « *seules les personnes essayant de créer de nouvelles pièces de monnaie* » s'intéresseront à des activités, « *de plus en plus laissées aux spécialistes avec des fermes de serveurs de matériel spécialisé.* [Et] *une ferme de serveurs n'aurait besoin que d'un seul nœud\* sur le réseau\* et le reste du réseau\* local se connecterait à ce nœud.* » (Nakamoto in Champagne 2014, p. 36). Au niveau matériel, les renégociations seront rapides : là où de simples ordinateurs de bureau suffisaient à miner du bitcoin la première année, il faut désormais des équipements spécifiquement dédiés, optimisant le couple quantité de calculs et énergie consommée. Car si la récompense d'émission monétaire est dévolue tout entière à l'opérateur le plus rapide à découvrir un en-tête d'enregistrement\* valide, pourquoi se limiter à la capacité de calcul CPU d'un simple processeur d'ordinateur de bureau ? Une carte graphique, dédiée à l'origine aux jeux vidéo, dispose d'une puissance GPU déjà bien supérieure en termes de *Hash\** par seconde. Alors plusieurs GPU reliées à une même machine... et son nœud\* client sert à constituer des « *rigs de minage* », qui ne seront qu'une première étape, expliquant qu'il n'est pas rare de trouver des « *gamers* » dans la population des premiers mineurs (cf. les profils d'acteurs rencontrés, voir Annexes n° IV.4). Mais ces bidouillages artisiaux seront rapidement supplantés par des dispositifs de plus en plus spécialisés, si bien que le remplacement des GPU par des circuits intégrés configurables (« *Field Programmable Gate Arrays* » ou FPGA) verra aboutir le mouvement dans l'élaboration de machines dédiées produites de manière industrielle : les fameux ASICs<sup>154</sup> (« *Application Specific Integrated Circuit* » ; Rauchs 2016, p. 52). Cette professionnalisation du minage érige des barrières à l'entrée pour les nouveaux mineurs de par la puissance totale déjà disponible et son inégale répartition<sup>155</sup>, évinçant progressivement les « *petits* » mineurs amateurs et indépendants. Mais là encore, c'est un mouvement discret et dialectique. Face à cette concurrence accrue et les barrières à l'entrée qui s'élèvent (particulièrement pour les petits opérateurs de minage), la communauté va rapidement

---

<sup>154</sup> Des sociétés créent des « *"circuits intégrés spécifiques à une application"* (ASIC) spécialisés, conçus et configurés dans le silicium dans le seul but de calculer des milliards de hachages SHA256 pour tenter d'"extraire" un bloc Bitcoin valide. Ces puces n'ont aucune application légitime en dehors de l'extraction de BTC et du craquage de mots de passe, et la présence de ces puces, qui sont des milliers de fois plus efficaces par dollar et kilowattheure lors des hachages informatiques que les CPU génériques, rend impossible la concurrence pour les utilisateurs ordinaires disposant de CPU et de GPU génériques. » (Buterin 2013e)

<sup>155</sup>Comme l'explique un mineur individuel, dès la première année, des « *gens ont commencé à utiliser des ordinateurs équipés de GPU pour le minage, celui-ci est devenu très difficile pour les autres* », moi « *je suis sur le bitcoin depuis quelques semaines et je n'ai pas encore trouvé de bloc (je mine sur trois CPU). Quand beaucoup de gens ont des CPU lents et qu'ils minent séparément, chacun d'entre eux est en compétition entre eux ET contre les riches bâtards de GPU ;-)* » (Sedgwick 2019k).

s'adapter via la constitution de coopératives de minage (ou pools, dont la première fut *Slushpool*, cf. Chap. IV), coopératives qui, à l'époque, ne font pas l'unanimité (Sedgwick 2019k). Bitcoin réalise « *sa première révolution industrielle* » quand, d'individuelle, la compétition de la PoW\* devient collective : des mineurs coopèrent afin « *de combiner leur puissance de hachage* » (*Ibid.*) pour augmenter leurs chances de trouver une PoW\* et ce, malgré une cible de difficulté\* de plus en plus élevée et face à des capacités de minage de plus en plus grandes et concentrées<sup>156</sup>. Ces coopératives de minage induisent des recompositions nombreuses et fondamentales. Cela bouleverse la logique de répartition des récompenses d'émission monétaire. Initialement adressée au seul des contributeurs élu leader parmi l'ensemble des participants (bien que tous soient nécessaires à la résilience d'ensemble et que cela induise l'arbitraire des cas d'enregistrement orphelins), cette création monétaire se trouve dès lors plus largement et sûrement répartie : centralisée par la pool qui la redistribue entre toutes les parties prenantes de la coopérative, à hauteur de leur contribution en puissance de calcul (même les petits génèrent des gains en UCN\*) et ce, en continu<sup>157</sup>. Pourtant, l'idée n'a pas séduit tout le monde lorsqu'elle a été lancée par Slush le 27 novembre 2010. Si, d'un côté, cela participait d'une diversification essentielle de l'activité de minage permettant de ne pas laisser le réseau\* se centraliser autour de « *quelques chanceux disposant de GPU rapides* », d'un autre côté certains *bitcoiners*\* critiques voient derrière ce « *minage coopératif* », « *une forme de communisme [...] fondamentalement défectueux* » (Sedgwick 2019k). Dans tous les cas, ces coopératives reposent sur une segmentation et une spécialisation des acteurs sur différentes fonctions liées aux opérations de traitement des transactions\* et à la mise à jour du registre\* : l'opérateur de la coopérative (une entreprise centralisée) est en charge de l'ensemble des opérations 2 (a, b, c et e) et ne fait que déléguer l'opération 2.d relative à la découverte de la PoW\*, à des mineurs qui n'en sont plus... Devenus simples Hashers, ils sont privés de leur souveraineté de *bitcoins*\* : ils n'ont plus le pouvoir de sélectionner, d'ordonner les transactions\* en attente puisque, à travers l'usage de cet arrangement sociotechnique, ils s'en sont dépossédés au profit des opérateurs de pools de minage<sup>158</sup>.

C'est un pouvoir essentiel qu'accaparent des acteurs peu nombreux et dont le poids se fait menaçant. Si l'un des *pools* venait à contrôler la majorité de la puissance de calcul du réseau\*, cela ouvrirait à un risque de 51%. Dans ce cas, ces opérateurs seraient en mesure de manipuler les transactions\* (retardement, censure), et même de mener des attaques de double dépense *off chain*\*. Pour préoccupant que soit ce scénario pour la sécurité et la décentralisation de Bitcoin, ces forces centralisatrices font face à d'autres qui jouent en sens inverse. Au sein des *bitcoiners*\*, nombreux sont ceux qui reconnaissent de tels risques et travaillent à les contenir ou à les supprimer. Déjà, la grande mobilité des hashers et leur souci d'éviter de telles situations est une force équilibrante : ils disposent de la capacité de rediriger rapidement, en quelques clics, leur puissance de calcul vers d'autres pools de minage, au cas où la leur se comporterait de manière illégitime à leurs yeux ou deviendrait trop puissante [Entretien n°17

---

<sup>156</sup> La taille des piscines renseigne le caractère hautement concurrentiel du minage actuel. Pour une comparaison des Pools (juridiction nationale, taux de hash, frais et taxe) voir [https://en.bitcoin.it/wiki/Comparison\\_of\\_mining\\_pools](https://en.bitcoin.it/wiki/Comparison_of_mining_pools) [consultation au 15/05/2015].

<sup>157</sup> Pour les mineurs de petite taille, ce type de service offre un avantage indéniable, car « *lorsque vous avez un pauvre ordinateur autonome, vous devez attendre de nombreuses semaines, voire des mois, pour trouver la récompense complète de 50BTC. Lorsque vous rejoignez un cluster comme celui-ci, vous recevrez constamment une petite quantité de bitcoins chaque jour ou chaque semaine* » (Sedgwick 2019k)

<sup>158</sup> Voir cette discussion Twitter initiée par Angela Walch à laquelle nous avons pris part : [https://twitter.com/angela\\_walch/status/1420390762647261187](https://twitter.com/angela_walch/status/1420390762647261187) [consultation au 13/03/2021]

et 18] : cela, l'histoire de Bitcoin l'a déjà éprouvé avec le cas Ghash.io, en janvier 2014<sup>159</sup> (Hajdarbegovic 2014). Ensuite, des équipes de développeurs\* travaillent à redonner aux hashers un statut de mineur en réduisant leur dépendance vis-à-vis des pools de minage : c'est le cas de Stratum V.2, développé par Braiin (entreprise liée à Slushpool) visant à améliorer le protocole Stratum, utilisé pour la communication entre les hashers et les pools de minage (Wirdum 2019) : en développement et marginal dans son usage, il permettrait au premiers de retrouver la capacité de choisir, de proposer leurs propres transactions\* et de construire leurs propres blocs.

Le développement infrastructurel de Bitcoin ne pousse pas seulement à renégocier les conditions exogènes avec lesquelles les acteurs articulent leur propre activité à un protocole solidifié par ailleurs. Le protocole Bitcoin n'est pas immuable, il évolue lui aussi au gré des changements de son environnement, démontrant des codes moins secs que ce qu'en disent certains *bitcoiners*\*.

### **Un protocole Bitcoin qui s'adapte : des régulations transactionnelles très politiques**

Bitcoin, ni comme protocole et encore moins comme infrastructure, n'est une machinerie autonome. Au contraire, il est essentiel que certains individus en assurent la maintenance, la sécurité et l'adaptation face à un environnement en constante évolution. Et la disparition de Nakamoto n'y change rien. La propriété d' « *ossification* » du protocole Bitcoin, vantée par certains faisant accroire que ses codes sont figés et immuables (Shinobi 2022), est contrefactuelle. Aux partisans d'une ossification décrite comme nécessaire au maintien de la confiance et de la stabilité de Bitcoin s'oppose une histoire démontrant l'exact inverse : confiance et stabilité se construisent, *reconstruisent* même, au travers des modifications, des adaptations du protocole et de ses règles canoniques consensuelles. Et ce, que Nakamoto en soit l'architecte ou non. La notoriété grandissante de Bitcoin devenue menaçante l'a poussé au départ<sup>160</sup>. Impossible de savoir précisément les raisons de son retrait ou du choix de l'anonymat. Mais il semble qu'il ne voulait pas que sa notoriété et les recherches sur son identité ne détournent l'attention de ce qui, pour lui, était le plus important : Bitcoin, ses potentialités et surtout ses contributeurs<sup>161</sup>. Cet aveu, Nakamoto le fait dans son pénultième mail privé (daté d'avril 2011, adressé au développeur Mike Hearn), où il déclare que, s'il « *est passé à autre chose* », l'important reste pour lui que le projet « *est entre de bonnes mains avec Gavin Andresen et tous les autres* »<sup>162</sup> (Nakamoto 2011). Ces « bonnes mains » sont celles de développeurs\* volontaires (comme Martti Malmi, Hal Finney, Gavin Andresen...) qui travaillent dès l'origine sur des codes sources Bitcoin. Ce sont elles qui ont joué et jouent toujours un rôle essentiel, effectuant la maintenance, proposant des modifications qu'elles implémentent dans de nouvelles versions logicielles que pourront télécharger les usagers

---

<sup>159</sup> Le 8 janvier 2014, la coopérative de minage Ghash.io, lancée par la bourse d'échange CEX.io, accumule près de 42% de la puissance de calcul total de Bitcoin, ce qui souleva l'inquiétude. La situation est vocalement dénoncée sur les réseaux sociaux, l'érigent en problème public. Les réactions vont de la mise en place, par le pool, d'un plan pour s'assurer qu'elle ne franchira jamais la barre des 51% , puisqu'« *elle cesse temporairement d'accepter de nouvelles installations minières indépendantes dans la pool et [implémente un service] permettant aux utilisateurs existants de miner des bitcoins à partir d'autres pools [...] de leur choix* », aux boycotts des hasheurs qui démontrent leur efficacité, en une journée la part retombe « à 38%, contre 42% » (Hajdarbegovic 2014).

<sup>160</sup> Après être resté actif sur les forums, Nakamoto va disparaître sans crier gare. Son dernier message public date du 12 décembre 2010 et annonce simplement quelques correctifs nouvellement implantés (Nakamoto 2010a).

<sup>161</sup> Le dernier écrit de Nakamoto est un mail privé adressé à Gavin Andresen le 26/04/2011 dans lequel il déclare : « *J'aimerais que vous arrêtez de parler de moi comme d'une mystérieuse figure d'ombre, la presse ne fait qu'en faire un angle d'attaque de la monnaie pirate. Peut-être que vous devriez plutôt parler du projet open source et donner plus de crédit à vos contributeurs au développement ; cela les motive.* » (Nakamoto 2011).

<sup>162</sup>Voir l'échange de mail original sur <https://plan99.net/~mike/satoshi-emails/thread5.html> [consultation au 03/08/2020].

(Nakamoto 2010a; Finney 2009; Andresen 2011; Gaurav 2019; H 2020). Elles encore qui institutionnalisent le cadre même (fait de normes et procédures évolutives) au sein duquel elles seront régulées et contraintes dans leurs activités (comme avec la BIP 001, cf. Chap. III). Les paramètres originaux qu'a « *sortis de son chapeau* » Nakamoto [A. Le Calvez, Entretien n°20] cachent mal leur dimension politique et normative ; il en est de même pour leurs modifications *a posteriori*. Certaines évolutions clefs des règles transactionnelles démontrent comment sont prescrites des interactions dites légitimes, et proscrites d'autres reléguées à l'illégitimité.

Ainsi, le protocole Bitcoin repose sur un ensemble de régulations transactionnelles nécessaires afin d'en assurer un fonctionnement tant efficace que soutenable. La distribution des nouvelles UCN\* sous la forme de récompense à la participation « honnête » au réseau\* est une règle protocolaire fondamentale, tenant le rôle d'incitation politique première. Mais elle ne peut être la seule, et d'autres ont été ajoutées ou supprimées, démontrant comment le protocole s'adapte dynamiquement. Déjà, car le choix d'une quantité maximale d'UCN\* se fait eschatologique : ce financement a une fin annoncée. Dès lors, le fonctionnement et la sécurité de Bitcoin devront être supportés par d'autres subsides et une seconde incitation est entrevue originellement : lorsque l'ensemble des récompenses aura été distribué, « *le système pourra prendre en charge les frais de transaction\* si nécessaire* » et grâce à « *la concurrence du marché ouvert [...] il y aura probablement toujours des nœuds\* prêts à traiter les transactions\* gratuitement* » (Nakamoto cité par Champagne 2014, p. 91). Nakamoto pèche encore par optimisme. Au lancement de Bitcoin, les récompenses initiales suffisent et l'absence d'un « mécanisme de marché » ne pose pas problème, lui laissant croire qu'une gratuité de traitement sera toujours offerte. Il n'en est rien. Ce mécanisme de frais de transaction\* n'attendra pas le tarissement des récompenses d'émission. Si le réseau\* naissant n'était pas saturé (toute transaction\* était facilement traitée à moindres frais), les conditions initiales changent dès la période de péché et deviennent un problème récurrent lors de la phase de maturation. En outre, Nakamoto sait dès le départ que, si « *les transactions\* gratuites sont agréables* », encore faut-il que « *les gens n'en abusent pas* », sans quoi le réseau\* affronte l'un des risques principaux des réseaux\* P2P déjà présentés : les attaques DOS (Champagne 2014, p. 209). La gratuité induit une illimitation potentielle de la demande d'espace d'enregistrement quand l'offre de traitement et d'enregistrement des transactions\* est, elle, une ressource limitée et un coût pour les opérateurs de nœuds\* (mineurs et complets). Ces attaques DOS, sans même relever de la présence d'un bogue à proprement parler (cf. Chap. III), peuvent prendre la forme de simples « spams » ralentissant le traitement réalisé par les nœuds\*.

Pour encadrer ce risque, Bitcoin intègre une série de règles transactionnelles qui, loin d'avoir été fixées dès le départ, se sont vues ajoutées et modifiées suivant les contraintes propres que le réseau\* rencontrait. D'autres « *limites ont été ajoutées pour empêcher une attaque par déni de service du réseau\* de type "bloc empoisonné"* [c'est-à-dire « *des blocs intentionnellement coûteux à valider* »] » (Andresen 2016). Ces régulations sont souvent réduites à l'établissement d'une taille limite des enregistrements (la limite de 1 Mo) et de mécanismes encadrant les frais de transaction\*. Présentées d'ailleurs comme originelles, ces deux régulations étaient pourtant absentes au moment du lancement de Bitcoin (Bier 2021d). S'agissant de la limite de la taille des blocs fixée à 1 Mo, elle n'est pas le choix initial (contrairement à ce qu'en disent De Filippi et Loveluck 2016, par exemple) : à son lancement, Bitcoin n'avait pas formellement « *de limite de taille de bloc, bien qu'il soit probable que des blocs plus grands, peut-être plus de 32 Mo, auraient brisé le système* » (Bier 2021d). La seule limite présente dans la première version (définie par un nombre de « *verrous de base de*

*données ») était passée inaperçue<sup>163</sup>. La limite de 1 Mo n'a été introduite que le 15 juillet 2010<sup>164</sup> et fut dissimulée par Nakamoto (Apodaca 2015), qui demande alors même « aux personnes qui l'ont découverte de ne pas en parler [...], afin d'éviter que la controverse ou les attaquants ne perturbent le changement de règles en cours » (Theymos 2015). S'agissant du mécanisme des frais de transaction\*, il renvoie à l'existence de « deux seuils à respecter lors de la création d'une transaction\* » (J. Garzik, repris par Bradbury 2014) : le premier renvoie à l'existence de « frais relais » et le second à l'existence de « frais de transaction\* » à proprement parler. Ces deux mécanismes encadrent séquentiellement deux activités qu'implique le traitement des transactions\* : « Le premier permet au réseau\* de relayer votre transaction\*, tandis que le second persuade les mineurs de bitcoins d'inclure votre transaction\* dans un bloc [de ce fait,] la première opération doit avoir lieu avant la seconde, afin que la transaction\* parvienne aux mineurs en premier lieu » (J. Garzik, repris par *Ibid.*). Des deux mécanismes, seul celui des frais de transaction\* existait dès l'origine, autorisant les opérateurs de nœuds\* mineurs à en fixer librement le montant. Face à la faible demande initiale d'espace de transactions\* des premiers temps du protocole, la majorité d'entre eux les acceptaient sans frais (la valeur par défaut du logiciel client, Möser et Böhme 2015, p. 3). C'est dans un second temps que des frais relais minimums seront implémentés protocolairement et leurs paramètres seront d'ailleurs modifiés plusieurs fois (Bradbury 2014, par exemple les versions 0.8.2, 0.9, etc.). La fixation d'un seuil minimum de « frais relais » vise directement à parer aux risques DOS causés par les « *flood attacks* » - l'envoi d'un très grand nombre de transactions\* de montant infinitésimal pour surcharger le réseau\* - en prévenant en amont le relais des transactions\* (Bradbury 2014; Lopp 2021). Ces deux mécanismes ne sont d'ailleurs pas les seuls. Nakamoto a ajouté une « limite de poussière » (« *dust limit* ») visant à parer aux situations similaires : toute UTXO\* inférieure à 0.01 BTC envoyé nécessite de s'acquitter du versement de 0.01 BTC de frais (Champagne 2014, p. 205 à 212). Finalement, loin d'être réductible à « une offre du marché libre pour payer la rareté de l'espace de bloc » (Keir 2022), cet ensemble de contraintes et planchers, modifiés à l'envi, relève de problématiques hybrides.*

Le mécanisme de frais de transaction\*, nécessaire à l'inclusion des transactions\* dans un enregistrement et couplé à la limite de la taille des enregistrements, devait permettre l'émergence d'un « prix libre », équilibrant une offre de capacité de traitement et de stockage des transactions\* – offerte par les « mineurs » - à une demande, opérée par les utilisateurs. Du côté de l'offre, ces frais doivent inciter au maintien à long terme de la sécurité et de la viabilité du réseau\*, même quand la création monétaire aura cessé. En outre, ces frais doivent réguler les tensions potentielles (présentes et futures) sur les capacités mémoires et la bande passante, qu'un accroissement illimité du nombre de transactions\* (donc du poids des enregistrements) engendrerait pour les opérateurs de nœuds\* (Nakamoto 2008a). En pratique, cette limite est un rationnement de l'offre, restreignant la quantité maximale de transactions\* que le protocole peut traiter sur un temps donné (Cromam et al. 2016, p. 1). En plus d'un rationnement planifié, les transactions\* en attente ne sont pas discriminées entre elles suivant ce seul niveau de frais de transaction\*. Nous l'avons vu, il aura fallu aux développeurs\* ajouter d'autres frais spécifiques, permettant tout à la fois de « dissuader les spammers et l'utilisation inefficace du

<sup>163</sup> Cette limitation originelle n'est redécouverte par la communauté qu'en 2013, suite à la survenue d'une scission de chaîne (crise n°19, CVE 2013 #3220) consécutive à une incompatibilité entre ladite limite et l'ancienne version de la base de données « BekleyDB » implantée dans les clients logiciels antérieurs à la version 0.8 (Voir [https://github.com/bitcoin/bips/master/bip-0050.mediawiki](https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki) ou Buterin 2013) [consultation au 03/08/2020].

<sup>164</sup> La limitation de 1 Mo est faite par Nakamoto qui n'ajoute qu'une ligne de code (« Static Const Unsigned Int MAX\_BLOCK\_SIZE = 1000000;<sup>[1]</sup> ») (<https://github.com/bitcoin/bitcoin/commit/a30b56ebe76ffff9f9cc8a6667186179413c6349>), elle est implantée dans la version 0.3.2, publiée le 19 juillet 2010, mais son entrée en vigueur ne s'est faite que le 07/09/2010 (Bier 2021d) [consultation au 03/08/2020].

*réseau*\* » (Lopp 2021). Ces paramètres, « *codés en dur* » au lieu d’être laissés à l’appréciation des opérateurs de nœuds\*, ne font pas l’unanimité : certains y voient « *un bug* », une décision arbitraire là où « *un système dynamique de frais de transaction*\* "flottants" » permettrait à un « *marché libre* » de décider « *à la fois des limites de relais et des seuils d’inclusion des blocs* » (Garzik, cité par Bradbury 2014). Ces régulations transactionnelles formelles, contraignant économiquement l’usage de Bitcoin, ne peuvent cacher leurs dimensions prescriptives et normatives. Elles définissent explicitement des activités jugées « *inutiles* », « *inefficaces* » voire « *dangereuses* » pour Bitcoin. Pourtant, dans une acceptation rigoriste et idéale typique du « *Code is Law* » des *bitcoiners*\*, la catégorie de « *spam* » est privée de sens, car « *d’un certain point de vue, les transactions*\* de *spam bitcoin* n’existent pas - si elles sont valides et qu’elles paient les frais appropriés, elles doivent être confirmées. » (Lopp 2021). Au-delà des codes, c’est de leur âme dont il est question (cf. Chap. III.2.1) : le qualificatif de *spam*, normatif, renvoie à un jugement de valeur d’autres qualités transactionnelles que leurs seules validités techniques<sup>165</sup>. Finalement, ces régulations transactionnelles prescrivent (et proscripent en retour) des plages de paiement et des types de transactions\* suivant qu’elles sont considérées comme légitimes ou non.

Ces régulations transactionnelles (taille des blocs, « limite de poussière » ou « frais minimum de relais ») et leur prescription/proscription par essence politique iront même jusqu’à engendrer un conflit, l’« *Op\_Return War* ». Traité dans la section suivante, ce désaccord entre *bitcoiners*\* dévoile exemplairement les attentes disparates qu’ils ont quant aux caractéristiques qu’ils attendent de Bitcoin, et comment ces régulations protocolaires, loin d’être neutres, sont des cristallisations normatives pouvant être instrumentées contre certains acteurs et certains usages.

### I.3 ETHEREUM : UNE RUPTURE ASSUMÉE D’AVEC BITCOIN ET LES PREMIERS ALTCOINS

Restituer et comprendre la dynamique carnavalesque du développement infrastructurel de Bitcoin a nécessité d’articuler des développements endogènes à d’autres plus exogènes. Parmi eux, ceux produits par l’émergence de nouveaux protocoles de registre\* distribué portant de nouvelles UCN\*. Cette constellation de systèmes alternatifs s’est créée autour *de* et s’est articulée *à* Bitcoin, formant une infrastructure monétaire et financière plus large et complexe. Cette dernière section présente notre deuxième cas d’étude, Ethereum, dont nous souhaitons, là encore, saisir la forme et le contenu des arrangements sociotechniques, comme leurs conditions d’élaboration. Comme précédemment, comprendre le *comment* et le *pourquoi* des recompositions d’alliances recherchées, des attachements / détachements établis, impose d’en restituer les inspirations hétérogènes et les problématiques hybrides qu’elles incorporent. La socio-histoire de Bitcoin présentée est nécessaire à la compréhension des grandes lignes de son fonctionnement, du contexte de son émergence ainsi que de la dynamique tout aussi carnavalesque de son développement infrastructurel. Mais s’y adjoint celle de la galaxie d’*Altcoins*\*, à laquelle Bitcoin a ouvert la voie. En outre, ce développement ne sera abordé que

---

<sup>165</sup> Lopp (2021) considère comme « *spams* » une transaction qui dispose de l’ensemble de ces attributs : « Moins de 50 entrées » ; « Plus de 50 sorties (destinataires) » ; et « au moins 50 sorties ont exactement la même valeur, soit 0,0001 BTC ou moins ».

superficiellement, considérant que l'exercice réalisé pour Bitcoin suffit au lecteur à comprendre la logique de notre démonstration et les prochains chapitres.

Si toute CM est génétiquement liée à Bitcoin, ses design et paramètres initiaux y ajoutent de manière critique une série de modifications plus ou moins radicales. Les inspirations de Nakamoto, qui visaient à dépasser les projets passés, se sont faites elles-mêmes inspirantes. Lui visait à déplacer la frontière des protocoles de consensus distribué « classiques » et centralisés. Les CM lancées à sa suite souhaiteront, elles, déplacer les frontières de Bitcoin. Une partie des *bitcoiners*\*, dits *Bitcoiners*\* Maximalistes\*, condamne et rejette tout objet apparenté à une CM autre que leur sacro-saint Bitcoin, alors même qu'ils se réfèrent à un *free banking* valorisant la concurrence monétaire (cf. Chap. II). Voilà que, parmi les plus rigoristes, beaucoup dénoncent (pourfendent même) une pluralité monétaire pourtant nécessaire au « *processus de sélection naturelle des monnaies [...] que propose Hayek dans The Denationalization of money* » (Dréan 2013). La consistance de leurs représentations n'est pas celle attendue de leur protocole ! Pourtant, comment être surpris par la création de « *shitcoin* » ou « *scamcoin* » (appellation indigène cachant mal les représentations normatives et morales qui les fondent) par des concepteurs qui ne font que reproduire le geste critique de Nakamoto en déplaçant l'objet ? Mais cette dénonciation paradoxale des *Altcoins*\*, en particulier d'Ethereum, relève peut-être du fait que ces gestes critiques, réalisés par d'autres, mettent en exergue ce que ces *bitcoiners*\* cherchent (consciemment ou non) à escamoter : le caractère politique et normatif de Bitcoin. Elle occulte aussi des intérêts plus économiques. Avec l'explosion de CM, Bitcoin, jusqu'alors l'astre central de cet univers en expansion, perd de sa centralité. S'il conserve un rôle de référent et une forme de *leadership* (en termes de capitalisation boursière), l'infrastructure cryptomonétaire ne tourne plus exclusivement autour de lui : Ethereum s'érige comme étoile émergente, autour de laquelle gravite le développement de nouveaux protocoles et de nouveaux services. Nakamoto y a prêté le flanc en dotant Bitcoin de codes sources ouverts\* permettant de modifier son architecture. Il invitait à la construction d'une diversité d'objets sociotechniques aux architectures plus ou moins différenciées : en termes d'algorithmes de consensus, de temps et taille des enregistrements, de sécurité du réseau\*, etc. L'objectif n'est pas ici de réaliser une présentation exhaustive, aussi impraticable que futile, de toutes les CM apparues : à leur nombre en croissance constante répond un turnover important (ElBahrawy et al. 2017, p. 2 et 4)<sup>166</sup>. Au moment de l'écriture de ces lignes, près de 6868 cryptomonnaies\* et cryptoactifs sont recensés, s'échangeant sur près de 383 bourses d'échange, pour une capitalisation de près de 400 milliards de dollars<sup>167</sup> (cf. Annexe n°1). Notons que la valeur est concentrée sur un petit nombre de CM, et la capitalisation totale à l'exclusion de Bitcoin atteint les 180 milliards : reste que la domination de Bitcoin baisse tendanciellement (~55% de la valorisation totale), Ethereum se hissant à la seconde place (près de 52 milliards de dollars de capitalisation, soit près de 12,91%), les 25 premiers cryptoactifs représentent, eux, 89% de la valorisation totale, et les 50 premiers, près de 93% de l'ensemble. Ce qui suit présente l'apparition de cette galaxie de *Altcoins*\*, à travers certains représentants typiques et ce, pour mieux cerner la position prise par Ethereum. La compréhension de ses ambitions et de ses choix architecturaux impose de repartir des premières vagues d'innovation consécutives au lancement de Bitcoin et des épreuves que ces expérimentations rencontrèrent, poussant à la construction itérative de protocoles plus ou moins innovants. Un panorama de l'émergence d'un écosystème

---

<sup>166</sup> L'étude de ElBahrawy *et al.* (2017) concernant l'évolution des parts de marché des différentes CM entre le 28 avril 2013 et le 13 mai 2017 montre que près de sept CM apparaissaient chaque semaine et qu'un nombre similaire était abandonné. Publiées en 2017, leurs données (tirées du site coinmarketcap.com) comprennent 1 469 cryptoactifs sur la période, dont ils évaluent à 600 les projets actifs (*Ibid*, p. 4).

<sup>167</sup> Données tirées du site référence CoinGecko ([https://www.coingecko.com/fr/global\\_charts](https://www.coingecko.com/fr/global_charts) [consultation au 01/09/2020]).

de cryptomonnaies\* est présenté, explorant sa profondeur socio-historique. Mais l'ambition, plus illustrative qu'exhaustive, nous fera insister, à travers des exemples caractéristiques, sur les renégociations clefs opérées, qu'elles se fassent *sur* Bitcoin ou *à côté* de lui (1.3.1). Ce sont ces difficultés et contraintes rencontrées qui pousseront certains *coiners*\* à vouloir reconstruire un protocole de registre\* distribué radicalement nouveau en adoptant une stratégie différenciée : Ethereum (1.3.2). Parmi les conditions matérielles et idéelles ayant présidé à son émergence, nous insisterons sur les grandes différences qu'Ethereum a décidé d'entretenir avec l'architecture et le fonctionnement de Bitcoin, permettant de conclure sur la nature ontologiquement normative et politique de chacun des choix qu'opèrent leurs designs respectifs (1.3.3).

### **I.3.1 De la constellation des Altcoins : construire « sur » ou « à côté » de Bitcoin**

Les propriétés d'ouverture et de résistance à la falsification avaient attiré à Bitcoin des cryptographes, des hackers, des technophiles et des acteurs de plus en plus disparates. Elles allaient chez eux rapidement susciter une volonté de transposition à d'autres domaines d'usage. Puisqu'elle permettait l'existence et la cession d'objets numériques dénombrables et exclusifs qu'elle émettait en propre (les bitcoins), son architecture ne pouvait-elle pas servir à en administrer d'autres ? Au travers de l'émergence d'une constellation de nouveaux protocoles à CM propres, a été expérimentée une grande diversité d'architectures nouvelles. Et les modifications d'abord incrémentales ont été vite remplacées par des innovations plus radicales. Certains de ces nouveaux protocoles ne visent, comme Bitcoin, qu'à supporter des usages monétaires et de paiement, tout en offrant des usages différenciés. D'autres cherchent au contraire à offrir un éventail large d'usages non monétaires. Ainsi, primitivement, deux stratégies ont été mises en œuvre : travailler directement sur Bitcoin, au sein de ses codes et de ses contraintes, ou en dehors de lui.

#### **« Namecoin », entre complémentarité et indépendance vis-à-vis de Bitcoin**

Dès son lancement, Bitcoin est aussi ambitieux que prometteur pour des acteurs se revendiquant Cypherpunk et crypto-anarchistes. Si Bitcoin vise à « décentraliser la monnaie », de nombreux acteurs voient aussi l'occasion d'aller plus loin et d'utiliser son architecture pour « décentraliser » d'autres services numériques dont la centralisation est, pour eux, problématique. C'est le cas d'un autre service essentiel à l'infrastructure d'Internet qui est aujourd'hui centralisé : le système de noms de domaine (DNS). Son caractère essentiel tient au fait qu'il est le registre\* commun « *faisant autorité [et] qui permet de transformer les domaines de premier niveau de l'Internet (par exemple, .com, .edu, uk) en adresses IP associées, un peu comme le répertoire téléphonique de l'Internet* » (DeNardis et Musiani 2014, p. 10). Sans lui, pas de traduction possible entre les noms de domaine lisibles par les humains et les adresses IP, compréhensibles des seules machines. Mais voilà, cet arrangement sociotechnique fondamental soulève des préoccupations en matière de censure, de surveillance et de contrôle, bien au-delà des cercles cypherpunks et *bitcoiners*\*. Centralement administré par un organisme gouvernemental américain (l'ICANN), il est au cœur d'une « *lutte de pouvoir mondiale pour [son] contrôle [...], à la fois symbolique et réelle* », qui l'a vu être « *de plus en plus politisé* » tant il sert aujourd'hui « *l'hégémonie des États-Unis sur l'Internet [,] leurs pratiques de surveillance expansives* » et, plus généralement, d'instrument de coercition dans leurs conflits géopolitiques

(*Ibid.*, p. 10-14)<sup>168</sup>. Pour certains acteurs, si Bitcoin peut se substituer à une Banque Centrale, pourquoi l'ICANN ne pourrait-il pas l'être par un protocole de registre\* distribué ouvert ?

Conçu afin d'offrir un système aussi essentiel que celui du registre\* DNS, mais protégé des censures et manipulations, le second protocole de registre\* distribué public émettant sa propre UCN\* après Bitcoin est le « *Namecoin* » (ticker : NMC), lancé en avril 2011<sup>169</sup> (Loibl 2014, p. 107; Sedgwick 2018c). En grande partie similaire à Bitcoin, Namecoin vise le maintien d'un registre\* canonique commun stockant, en plus de ses informations transactionnelles (on retrouve des UCN\* *NMC* prenant la forme d'un système d'UTXO\*), les noms de domaine achetés et contenus dans les transactions\* traitées par les opérateurs des nœuds\* constituant son réseau\*. Un usager pseudonyme (identifié par une simple adresse publique) peut y enregistrer un nom de domaine et le contrôler en propre sans passer par une autorité centrale. Pour ce faire, il doit déjà détenir des UCN\* NMC, seules acceptées en paiement des différents frais impliqués (de transaction\*, mais aussi d'enregistrement du nom de domaine), donc un client portefeuille Namecoin (« *namecoind* »), lui permettant de les stocker et d'interagir avec le réseau\*. L'enregistrement d'un nom de domaine se fait *via* une transaction\* Namecoin. Le suffixe en « .bit », n'étant pas assigné par l'ICANN, implique que « *les serveurs DNS habituels ne peuvent pas en résoudre les requêtes* » et les usagers doivent passer par un logiciel *ad hoc* (Loibl 2014, p. 108-110). La transaction\* d'enregistrement, comme pour Bitcoin, est une demande en écriture associant le nom de domaine choisi à l'adresse publique spécifiée, et le registre\* canonique sera mis à jour une fois la transaction\* intégrée dans un enregistrement canonique\* de la blockchain de Namecoin, suivant des procédures assez similaires ; un propriétaire de nom de domaine doit renouveler son enregistrement tous les 12 000 enregistrements, *via* une nouvelle transaction\*. L'usage originel de Namecoin n'attendra pas longtemps pour être détourné : certains de ses utilisateurs innovent et en usent à d'autres fins... voilà que les premiers « *NFT* » trouveront à s'y consigner (Whiteabbit1111 2022).

Sans aller au fond de ses mécanismes<sup>170</sup>, l'expérience Namecoin est signifiante pour plusieurs raisons. Déjà, elle souligne comment Bitcoin est directement entrevu comme porteur de nombreux usages, non exclusivement monétaires. Ensuite, car ces usages potentiels soulèvent la question des caractéristiques du protocole qui pourrait les supporter : est-il possible d'utiliser Bitcoin afin de construire *sur* lui, ou est-il préférable, de par ses contraintes protocolaires propres, de créer *à côté de* lui des protocoles de registre\* distribué indépendants ? Si cette question est devenue taboue pour certains *bitcoiners*\*, pour qui tout usage non transactionnel de Bitcoin ou de tout autre protocole de registre\* distribué est au mieux inintéressant et inutile ou, au pire, un gâchis de ressources redoublé d'une volonté d'arnaque

---

<sup>168</sup> Le système DNS est devenu un « *site où se manifestent des tensions politiques et économiques mondiales* », un enjeu de « *lutte de pouvoir de longue date et politiquement symbolique [qui] porte sur la question de savoir qui doit contrôler les modifications apportées au fichier de la zone racine de l'Internet [puisque] cette fonction, assurée par l'Internet Assigned Numbers Authority (IANA) au sein de l'ICANN, a toujours été exécutée dans le cadre d'un contrat avec le ministère du Commerce des États-Unis, qui joue également un rôle direct dans l'autorisation des modifications du fichier de la zone racine.* » (DeNardis et Musiani 2014, p. 10). Il est au cœur de la démonstration de la « *gouvernance par l'infrastructure* » et du « *recours à l'infrastructure* » (« *turn of infrastructure* ») comme extension des moyens et conflits (géo)politiques que réalisent ces autrices.

<sup>169</sup> Voir <https://www.namecoin.org/> et <https://bitcointalk.org/index.php?topic=6017.msg88356#msg88356> [consultation au 21/04/2021].

<sup>170</sup> Ces mécanismes sont proches de ce qui a été déjà présenté : « *Namecoin est basé sur le code du Bitcoin, il utilise le même algorithme de preuve de travail et est limité à 21 millions de pièces, mais il a sa propre blockchain\* qui commence avec un bloc de genèse différent et c'est donc une monnaie distincte* », n'ajoutant à Bitcoin que « *des commandes RPC (remote procedure call) supplémentaires qui permettent à ses utilisateurs d'enregistrer et de transférer des noms arbitraires (clés) et d'attacher des données (valeurs) à ces clés dans la blockchain\* en envoyant des transactions spéciales.* » (Loibl 2014, p. 108)

(cf. Chap. III), en 2010, il n'en est rien. Namecoin s'inspire d'un projet de DNS distribué discuté dès novembre 2010 sur Bitcointalk, « *BitDNS* », dont l'annonce sur Bitcointalk fut reçue avec enthousiasme dans la communauté des *bitcoiners*\* d'alors. Pour preuve, S. Nakamoto et H. Finney s'impliquent dans les réflexions préalables à sa création sans voir aucun problème à ce que d'autres protocoles de registre\* distribué existent, avec leur propre UCN\* rémunérant leurs mineurs (Nakamoto 2010b). Ce projet n'était pas perçu comme concurrent de Bitcoin. Nakamoto reconnaît pourtant une impossibilité pratique : si Bitcoin permet la consignation distribuée d'informations (transactionnelles ou non), il est clair qu'il n'est pas souhaitable de l'utiliser pour agréger une multiplicité de données induites par une multiplicité d'usages dans un seul ensemble de données, cela ne tiendrait pas la montée en charge (*Ibid.*). Nakamoto ajoute que les systèmes Bitcoin et BitDNS devront avoir des développements différenciés et « *des destins distincts* », suivant les désirs et intérêts respectifs de leurs communautés (par exemple, la taille de la couche base de données, (*Ibid.*)<sup>171</sup>). Nakamoto n'en propose pas moins, suivant les besoins spécifiques qu'il entrevoit pour BitDNS, un design permettant tout à la fois à « *BitDNS d'être un réseau\* complètement séparé et une chaîne de blocs\* séparée, tout en partageant la puissance du processeur [de] Bitcoin* » : il suffit « *que les mineurs puissent rechercher des preuves de travail pour les deux réseaux\* simultanément* »<sup>172</sup>. Nakamoto vient d'inventer le « merge mining » (ou « *AuxPoW\** ») qu'emprunte effectivement Namecoin en guise de consensus de PoW\*<sup>173</sup> (Champagne 2014, p. 313; Sedgwick 2018c; D 2020). Ce dernier permet que deux réseaux\* partagent le même algorithme de PoW\* (ici SHA 256) sans se cannibaliser. Au lieu d'imposer aux nœuds\* mineurs de travailler exclusivement sur l'un ou l'autre des protocoles, ce qui fragmente la puissance de calcul et baisse la sécurité relative des deux, le merge mining permet une mutualisation accroissant leur sécurité respective. Malgré des règles de consensus propres, Namecoin partage avec Bitcoin la même fonction de hashage, offrant aux mineurs d'user de leur puissance de calculs afin de participer aux « *deux réseaux\* en parallèle [...] de telle sorte que s'ils obtiennent un résultat [un hash\* d'en-tête d'enregistrement\* valide], ils pourraient résoudre les deux problèmes en même temps* » (*Ibid.*). Cette complémentarité architecturale a un double avantage. Incitant les mineurs de Bitcoin à participer aux deux protocoles, Namecoin y gagne en sécurité, puisqu'il s'aliène les mineurs ayant le plus de puissance de calcul de l'écosystème. Les mineurs de Bitcoin y gagnent une nouvelle source de rémunération, qui réduit leur dépendance à Bitcoin : à coûts presque inchangés, le travail fourni permet la découverte de *hash\** cible valide et l'obtention de récompenses d'émission au sein des deux protocoles.

Namecoin, première itération de CM construite après Bitcoin, sera suivie par de nombreuses autres. Innovation incrémentale à partir de l'architecture de Nakamoto, cette CM partage avec lui, en plus de nombreux codes et paramètres, sa sécurité en termes de PoW\*. Mais pour avantageuse qu'elle apparaisse, cette complémentarité avec Bitcoin est aussi porteuse d'inconvénients et de limitations, pour qui veut concevoir une architecture aux usages différenciés.

<sup>171</sup> Là où « *Les utilisateurs de BitDNS pourraient être totalement libéraux en ce qui concerne l'ajout de fonctions de données volumineuses [...] tandis que les utilisateurs de Bitcoin pourraient devenir de plus en plus tyranniques en ce qui concerne la limitation de la taille de la chaîne, afin qu'elle soit facile à utiliser pour un grand nombre d'utilisateurs et d'appareils de petite taille* », voir <https://bitcointalk.org/index.php?topic=1790.msg28878#msg28878> [consultation au 21/08/2022].

<sup>172</sup> Voir <https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696> [consultation au 21/08/2022].

<sup>173</sup> Voir <https://bitcointalk.org/index.php?topic=1790.0> ; <https://bitcointalk.org/index.php?topic=1790.msg28938#msg28938> ; <https://bitcointalk.org/index.php?topic=1790.msg28959#msg28959> [consultation au 23/08/2022].

## Des CM qui s'émancipent de plus en plus de l'architecture Bitcoin

Comme Namecoin, nombreuses sont les CM apparues à sa suite qui ne seront que des variations légères et incrémentales du protocole Bitcoin. Dans les pas de Nakamoto et à la différence de Namecoin, elles ne visent qu'à couvrir des usages monétaires (d'où le qualificatif de « Bitcoin-Like »). Une grande diversité d'architectures sera expérimentée, et les modifications d'abord incrémentales céderont vite la place à des innovations plus radicales. Offrir, comme Bitcoin, des usages monétaires et de paiement aux caractéristiques singulières nécessite que ces CM reposent sur des protocoles autonomes et indépendants. Aux avantages de la complémentarité d'avec Bitcoin que maintenait Namecoin au travers du lien formel du merge mining répondent également des inconvénients : cela implique des complexités techniques et, surtout, une dépendance et des interférences d'objectifs entre ceux du projet « auxiliaire » et ceux du projet parent, auquel ses logiciels et son infrastructure doivent s'adapter pour rester compatibles et fonctionnels. Cette dépendance politique à Bitcoin trouve à s'exprimer tant dans ses codes protocolaires que dans les arrangements sociotechniques qui s'y étaient, ce que certains perçoivent comme problématique. La pléthora de CM à venir ne cesse de vouloir s'en émanciper. Preuve que, derrière la perception de rigidité de Bitcoin (à la fois aux niveaux protocolaire et infrastructurel), se joue un conflit d'ordre politique pétri de volontés d'émancipation et d'autonomie : les concepteurs et promoteurs de ces CM introduisent toujours leur présentation du constat critique par « *le problème du Bitcoin est ...* ». Les « problèmes » annoncés vont des modalités du minage (trop énergivore, trop concentré et difficile d'accès du fait de l'apparition des ASICs) aux conditions du monnayage (définition du plafond de l'offre monétaire, quantité de récompenses, temps de traitement des transactions\*, etc.) en passant par la limitation à des usages monétaires et financiers simples, la rigidité de l'obtention de consensus communautaire, la préservation de la vie privée, la mise à l'échelle\* ou les questions de financement. S'ensuit toujours une description plus ou moins technique des solutions à implémenter pour les résoudre.

Les modifications de tout ou partie de l'architecture et des codes sources Bitcoin peuvent concerter les règles et l'algorithme de consensus\* (type de PoW\* utilisé, passage au PoS) pour améliorer l'efficacité et/ou l'équité du traitement des transactions\* ; les mécanismes d'émission monétaire ; le langage de programmation\* et les standards transactionnels ; les propriétés de montée en charge afin de pouvoir traiter un plus grand nombre de transactions\*, obtenir des cycles de traitement plus rapides et en baisser les frais. Dans tous les cas, qu'elles concernent les activités de traitement des transactions\*, de production des enregistrements ou de tout autre domaine, les alliances au cœur de Bitcoin sont renégociées, et chacune des recompositions renvoie à autant d'arbitrages et de compromis hybrides, situés, politiques et conflictuels (sécurité, équilibre économique, distribution du traitement et de l'enregistrement des transactions\*...).

Sans modifier profondément l'architecture protocolaire de Bitcoin, il est possible de substituer l'algorithme de consensus\* SHA 256 par un autre, dont les caractéristiques cryptographiques permettent d'établir des propriétés transactionnelles différencierées. Le « *Litecoin* » (ticker : LTC), qui ambitionne de « *créer une véritable monnaie alternative similaire à Bitcoin* » (Charli Lee 2011) est exemplaire tant les modifications effectuées, à l'image de sa communication, sont simples. Il est lancé début octobre 2011 par Charlie Lee, ancien employé de Google et frère de Bobby Lee (fondateur des pièces numismatiques Cascascius et de la plateforme d'échange Chinoise BTCC, Sedgwick 2018d, cf. Chronologie 2 et section I.2.I). Filant l'analogie du métallisme numérique de Bitcoin (Maurer, Nelms et Swartz 2013, p. 2; cf. Chap. II) et à la manière d'un système bi-métalliste, Litecoin serait la monnaie d'argent moins onéreuse, plus commode et accessible que l'est hors numérique Bitcoin. Suite

à une simple modification d'un facteur 4 de certains paramètres (la quantité de monnaie est plafonnée à 84 millions et le cycle de traitement des transactions\* réduit à environ 2 minutes 30), Lee vante un « *temps de confirmation\* des transactions\* plus rapide et [...] une meilleure efficacité de stockage* » : son protocole serait « *capable de gérer un volume de transactions\* plus important que son homologue* [du fait d'une] *génération plus fréquente de blocs.* » (Charli Lee 2011). Cette rapidité tient à l'abandon de l'algorithme de PoW\* SHA 256 pour un autre, « Script » aux propriétés qui le rendraient résistant à l'utilisation des GPU et des ASICs perçus comme vecteurs de centralisation<sup>174</sup>. Celle-ci bouleverse le travail demandé aux nœuds\* pour produire un hash\* valide et permet, sans entrer en concurrence avec les puissants mineurs du protocole Bitcoin, de fixer cette nouvelle temporalité avec un mécanisme d'ajustement de la difficulté similaire<sup>175</sup>. La longévité de cette CM, l'une des rares de cette époque à être encore active aujourd'hui, s'explique par le choix de grande proximité aux codes Bitcoin, qui lui a permis de développer des synergies infrastructurelles (certaines innovations proposées pour Bitcoin sont d'abord implémentées sur Litecoin, Bier 2021a, voir « Scaling Debate », Chap. III.3.1).

Plus radicalement, la première CM à remettre en cause le consensus par la PoW\* est le « *Peercoin* » (ticker : PPC) annoncé en août 2012. Sa communication est claire : elle serait plus écologique, car sa sécurité à long terme s'émancipe d'une PoW\* dont les vertus reconnues sont conçues comme problématiques à terme. Cependant, toute attache n'est pas rompue. L'innovation repose dans un consensus hybride mêlant PoW\* et preuve d'enjeu (« *Proof of Stake* » ou *PoS*)<sup>176</sup>. Le protocole conserve une PoW\* afin d'assurer «  *principalement la frappe initiale* [« *Jusqu'à 99 % de tous les Peercoins sont créés avec l'algorithme PoW\** »] et n'est pas essentiel à long terme. » (Sunny King et Nadal 2012, p. 1). Il est présenté comme un « *dérivé du Bitcoin* », plus économique en énergie quant à la découverte d'un nouvel en-tête d'enregistrement\* valide<sup>177</sup>. La PoS « *remplace la preuve de travail\* pour assurer la majeure partie de la sécurité du réseau\** » (*Ibid.*). Elle est la variable déterminante de la règle consensuelle de réconciliation sur un registre\* canonique commun, puisqu'elle sert à établir le caractère canonique d'un enregistrement candidat\* valide : c'est « *la chaîne dont l'âge des*

<sup>174</sup> On parle de propriété de résistance aux ASICs, car, suivant l'algorithme choisi, le « travail » demandé change et permet de rendre « inefficace » l'utilisation des machines dédiées. Historiquement, cette propriété n'a jamais tenu ses promesses, car, avec la valorisation des récompenses, il est toujours devenu rentable pour des entreprises de créer du matériel dédié. Certains arguent d'ailleurs qu'une telle propriété limite la sécurité de la chaîne au lieu de l'accroître : une machine dédiée est un investissement non récupérable là où des machines généralistes peuvent être facilement redéployées (par achat ou location) afin d'orchestrer des attaques 51% (O'Leary 2018).

<sup>175</sup> Au sein de Litecoin, « *la difficulté sera ciblée à nouveau tous les 3,5 jours. La combinaison des temps de reciblage rapides et de la preuve de travail Scrypt (Litecoin ne sera pas en compétition avec Bitcoin pour les mineurs) signifie que nous nous attendons à ne pas voir le genre de problème que Namecoin a rencontré ; la puissance de hachage qui part plus soudainement qu'elle n'est arrivée, causant une difficulté élevée pour tous ceux qui sont restés.* » (Charli Lee 2011)

<sup>176</sup> Voir l'annonce ici <https://bitcointalk.org/index.php?topic=99735.0> [consultation au 27/08/2022]. Au sein des communautés de *coiners\**, avantages et inconvénients de la PoW\* et de la PoS sont controversés. Les *bitcoiners\**, promoteurs de la PoW\*, critiquent la PoS comme moins sécurisée. À l'inverse, ses détracteurs soulignent que, si la « *preuve de travail a contribué à la percée majeure de Nakamoto* », elle induit une dépendance à « *la consommation d'énergie, introduisant ainsi des frais généraux significatifs [...] supportés par les utilisateurs via une combinaison d'inflation et de frais de transaction. Le ralentissement du taux de frappe dans le réseau Bitcoin pourrait à terme exercer une pression sur l'augmentation des frais de transaction afin de maintenir un niveau de sécurité satisfaisant.* » (Sunny King et Nadal 2012, p. 2)

<sup>177</sup> Produire un enregistrement valide est « *un processus stochastique similaire* » entre PoW\* et PoS. Celles-ci diffèrent « *dans le fait que l'opération de hachage est effectuée sur un espace de recherche limité [...] au lieu d'un espace de recherche illimité comme dans le cas de la preuve de travail, ce qui n'entraîne pas de consommation d'énergie significative.* » (Sunny King et Nadal 2012, p. 3)

*pièces PoS<sup>178</sup> est le plus long qui gagne en cas de division de la chaîne de blocs\* » (peercoin) et non plus la plus lourde en calcul. En PoS, les participants au consensus ne sont pas dénommés *mineurs*, mais *mineurs*. Toujours en concurrence les uns avec les autres, leurs chances d'être « tirés au sort » ne dépendent plus d'une ressource externe (l'énergie), mais interne : en l'espèce, il faut immobiliser, pour un temps, des UCN\*. Dorénavant, c'est la part relative des UCN\* immobilisées (et leurs « âges ») qui devient déterminante : « chaque transaction\* dans un bloc contribue à l'âge de ces pièces consommées au score du bloc. La chaîne de blocs\* dont l'âge total des pièces consommées est le plus élevé est choisie comme chaîne principale » (Sunny King et Nadal 2012, p. 3). À cette modification franche s'ajoute une autre : un monnayage opposé au métallisme numérique de Bitcoin. Choix est fait de ne pas fixer de plafond d'émission. Une fois les récompenses dédiées à la PoW\* taries, resteront celles allouées à la PoS, calibrées pour offrir un rythme de création monétaire de 1% par an, pour une durée indéterminée. Ainsi, les opérateurs de traitement des transactions\* sont assurés d'un revenu continu à long terme, qu'importe la présence de frais de transaction\*. Avec Peercoin, c'est l'utilité et la fiabilité de la PoW\* qui sont questionnées. Dans ce sens, le même King lance en juillet 2013 la CM Primecoin (ticker : XPM), dont le système de PoW\* sert une utilité autre que la seule sécurisation de la chaîne des transactions\*, en l'espèce découvrir « *des séquences de grands nombres premiers présentant un intérêt mathématique* » (Bonneau et al. 2015, p. 12).*

Les tentatives de King de « révolutionner » les voies de consensus feront des émules. Septembre 2012 voit « *Ripple* » (ticker : XRP, BitMEX Research 2018), proposer une architecture très différenciée de Bitcoin<sup>179</sup>. Par bien des côtés, il en prend même le contrepied. Il ne vise tout d'abord pas la désintermédiation. Souhaitant offrir des paiements interbancaires et transfrontaliers simplifiés, rapides et peu coûteux, il s'adresse aux institutions financières et bancaires à qui il promet des transferts dans tout type de devise existant. Présentant la PoW\* comme inefficace, il réintroduit dans son architecture un consensus de type « classique ». La production et la validation\* des enregistrements y sont aux mains de nœuds\* sélectionnés de manière *ad hoc* par Ripples Labs, acteur central d'un protocole fermé fondé sur la confiance *intuitu personae*. D'où le fait que l'UCN\* XRP est accessoire, sans aucun rôle protocolaire spécifique : la création monétaire d'UCN\* ne joue pas le même rôle d'incitation, ce qui explique que, à son lancement, Ripple a pu s'en passer pendant plusieurs mois (l'émission de janvier 2013 est postérieure au lancement du protocole, BitMEX Research 2018). En outre, redoublant l'affront à Bitcoin, ces UCN\* ont été émises via le mécanisme dit de « *premine* » : la totalité des 100 milliards d'UCN\* prévue protocolairement fut générée une fois pour toutes à son lancement, et seulement 45 milliards sont actuellement en circulation<sup>180</sup>. La distribution des XRP n'est pas la contrepartie de contributions encadrées par les règles protocolaires, mais

---

<sup>178</sup> Ce concept « *d'âge des pièces était connu de Nakamoto au moins depuis 2010 et utilisé dans Bitcoin [...] pour aider à hiérarchiser les transactions [...]. L'âge des pièces est [...] défini comme le montant de la monnaie multiplié par la période de détention [...] si Bob a reçu 10 pièces de la part d'Alice et les a conservées pendant 90 jours, nous dirons que Bob a accumulé 900 jours-pièces d'ancienneté.* » (Sunny King et Nadal 2012, p. 1)

<sup>179</sup> Ses inspirations remontent à Ryan Fugger qui, avec sa compagnie « *RipplePay* » lancée en 2004, visait à créer un réseau de confiance P2P où chaque utilisateur peut prêter directement aux autres (BitMEX Research 2018b). Aux fondations du projet et de la société qui le gère, *OpenCoin* - devenue *Ripples Labs* - on trouve des acteurs reconnus de l'écosystème comme le fondateur de MtGox, Jed McCaleb et Arthur Britto, qui s'associent à Jesse Powell (CEO de la plateforme d'échange *Kraken*), à David Schwartz, ainsi qu'à Chris Larsen (*Ibid* et [Bradbury 2013](#)) [consultation au 28/08/2022].

<sup>180</sup> <https://www.coingecko.com/fr/pi%C3%A8ces/xrp> [consultation au 24/09/2020].

à la discréption des fondateurs qui s'en sont réservé 20%<sup>181</sup>, quand les 80% restant ont été octroyés à Ripples Labs qui les met en circulation au gré de ventes ou de distributions à des entreprises partenaires. Cette concentration ajoute à la centralisation du protocole et du réseau\* un pouvoir de marché important conféré à l'entité émettrice et aux fondateurs. Ce curriculum explique les réserves et critiques qu'il suscite au sein des communautés de *coiners*\*.

Pour exemplaire que soit cette première vague de CM, elle n'épuise pas la diversité grandissante des expériences qui, par milliers, émergeront encore. À la multiplicité d'architectures protocolaires expérimentées s'ajoutent des voies de différentiation plus sociales que techniques. Comme l'illustre, en décembre 2013, le Dogecoin de Billy Markus et Jackson Palmer. Lancé comme une satire de Bitcoin dont les fondateurs souhaitaient se démarquer, il revendique un usage en paiement contre un Bitcoin de plus en plus conçu comme simple réserve de valeur. L'important avec Dogecoin, c'est que ses caractéristiques remarquables tiennent moins à la technique<sup>182</sup> qu'à sa dimension infrastructurelle et communautaire : utilisés encore aujourd'hui, ses codes n'ont pas évolué depuis des années. Puisqu'il ambitionne d'être un moyen de paiement à circulation ample, Dogecoin doit cibler une base d'utilisateurs large, excédant les groupes sociaux constitués par les *bitcoiners*\*. Il partira du « même » Internet « doge » (et le chien Shiba Inu<sup>183</sup>), dont le logo reprend l'image, il s'adresse aux utilisateurs de réseaux\* sociaux existants. Il se verra popularisé sur Reddit où il sert de pourboire aux créateurs de contenu. Et puisque la communauté valorise la circulation, les membres de sa communauté en useront régulièrement pour lever des fonds pour différentes causes<sup>184</sup>. Concluons par le « Darkcoin » / « Dash » (ticker : DASH), lancé début 2014. Il démontre comment les différentes expériences passées peuvent être combinées pour créer des architectures toujours plus éloignées de celle de Bitcoin et qui, contrairement à lui, ne visent pas à soustraire la gouvernance politique de la monnaie aux discussions et décisions humaines. On retrouve une PoW\* fondée sur l'algorithme X11 annoncé comme résistant aux GPU et ASICs, mais aussi un système de PoS qui lui permet d'offrir à ses usagers différentes options de paiement. Son architecture à deux étages, alliant PoW\* et PoS, permet optionnellement des transactions\* anonymisées par mixage via « *CoinJoin* » et des paiements instantanés. Deux types de noeuds\* de statut différent structurent le réseau\* : les noeuds\* simples, qui s'occupent des transactions\* standards en PoW\*, et les noeuds\* maîtres (« *master nodes* »), qui fonctionnent sur une PoS et ont la charge exclusive du traitement des transactions\* avancées (« *PrivateSend* » et « *InstantSend* »). Ces derniers sont aussi les seuls à avoir un droit de vote, car au sein du protocole est formalisé un cadre de gouvernance définissant les modalités de prise de décision (avec proposition communautaire et vote) et un budget commun, auquel est allouée une partie des récompenses de création monétaire. Pour Bitcoin, les coûts de développement ont été supportés par Nakamoto et les premiers contributeurs, sans qu'aucun n'ait de certitude quant à leur

---

<sup>181</sup> Chris Larsen a reçu 9,5 milliards et, en 2014, il s'est engagé à verser 7 milliards XRP à une fondation caritative ; J. McCaleb a reçu 9,5 milliards. En quittant Ripple - en 2013 -, il a conservé 6,0 milliards (sous réserve d'un accord de séquestre définissant les conditions dans lesquelles il peut les revendre), ses enfants ont reçu 2,0 milliards (avec, là encore, un accord de séquestre) et 1,5 milliard a été donné à des organisations caritatives et à d'autres membres de la famille McCaleb (non soumis à séquestre). A. Britto, quant à lui, a reçu 1 milliard (avec accord de séquestre) (BitMEX Research 2018).

<sup>182</sup> C'est un fork du « Luckycoin », lui-même fork de Litecoin et on retrouve la PoW\*, une absence de plafond d'émission, des récompenses de minage d'abord aléatoires, puis, fixé en 2014, un temps inter-bloc d'une minute, etc.

<sup>183</sup> Voir <https://knowyourmeme.com/memes/doge> [consultation au 29/08/2022].

<sup>184</sup> En janvier 2014, inspirée par le film *Rasta Rocket*, la communauté Dogecoin lève près de 50 000\$ pour permettre à l'équipe jamaïcaine de bobsleigh de se rendre aux J.O. de Sochi (Rodriguez 2014) et fera de même en levant près de 6 000 \$ pour un athlète indien(Coldewey 2014); la communauté lance aussi l'opération « *Doge4Water campaign* » et lève des fonds pour la Kenyan Water Charity(David Gilbert 2014), ou enfin, elle sponsorise le pilote de NASCAR Josh Wise (Estrada 2014).

recouvrement par la vente des UCN\* reçues de leur activité de minage. Et la « Bitcoin fondation », qui visait à rendre plus soutenable ce développement, fut constituée tardivement, restant suspendue à des donations d'entreprises incertaines. Voilà qu'à l'instar de Bitcoin où la totalité des incitations est dirigée vers le minage et ses opérateurs, ici l'émission monétaire est répartie entre les nœuds\* simples, les nœuds\* maîtres et un fonds commun qu'il faudra répartir par une procédure de vote *on chain\** (respectivement 45% pour les deux premiers et 10% pour le budget). Le Dash se fait exemplaire, démontrant que, derrière la grande diversité des protocoles de CM, c'est finalement à la normativité de l'architecture et des paramètres de Bitcoin que tous essayent de se soustraire. En outre, ils renseignent une autre normativité, celle-ci moins protocolaire qu'infrastructurelle : son concepteur Evan Duffield, *bitcoiner* dès 2010, a d'abord travaillé à « améliorer » l'anonymat de Bitcoin. C'est quand il a « *compris que [son] code ne sera[it] jamais ajouté à Bitcoin [car] les développeurs\* veulent vraiment que le protocole de base reste le même [...] et que tout le reste soit implémenté par-dessus* » (Duffield 2014), qu'il s'est résigné à en faire une CM indépendante et autonome.

Du reste, à cette stratégie de construire *à côté* de Bitcoin s'est historiquement opposée une autre qu'il nous reste à présenter. Comme avec Namecoin, d'autres protocoles allaient être conçus afin que de nouvelles fonctionnalités « *soi[en]t implémenté[es] par-dessus* » Bitcoin et non à côté de lui (*Ibid.*). Ces expériences de protocoles en « surcouche » ou métaprotocole allaient devenir une pierre d'achoppement conflictuelle et donner lieu à des modifications des codes Bitcoin hautement politiques, visant à interdire des comportements jugés inappropriés que le *protocole de base* autorisait à l'origine.

### Guerre des « métaprotocoles » : modifier Bitcoin pour en interdire certains usages

À partir de 2012, les « *monnaies alternatives* [sont] *un sujet populaire dans l'espace Bitcoin* » et à côté de « *Litecoin [,] Primecoin [,] Ripple*, [en émergent] *de nouvelles [...] chaque semaine* » dont « *un projet particulièrement intéressant [sera] l'objet d'une grande attention* » : Mastercoin / Omni (Buterin 2013b). C'est un métaprotocole qui n'est ni le premier - il succède à celui des « *pièces colorées* » (« *Colored Coins* » de Meni Rosenfeld, 2012 et Rosenfeld et al. 2013 et d'Alex Mizrahi de ChromaWay<sup>185</sup>) -, ni le dernier, car « *Counterparty* » (de Krellenstein, Slama et Dermody, 2014) suivra. Ces métaprotocoles susciteront l'attention car, plutôt « *que d'essayer de créer une blockchain entièrement nouvelle, comme le font toutes les autres cryptomonnaies\**, [ils cherchent] à créer un réseau\* entièrement nouveau de monnaies, de marchandises et de titres au-dessus du Bitcoin lui-même. » (Buterin 2013b). Leur principe est simple : Bitcoin comme base de données peut servir à consigner des informations autres que celles transactionnelles et ainsi, étendre son champ d'application au-delà des usages monétaires : horodater des documents, émettre/gérer des jetons numériques (ou « *token* ») auxquels sont assignées diverses fonctions. Si cette idée peut apparaître à certains *bitcoiners\** comme dangereuse (cela surcharge la base de données d'octets « *inutiles* », compromettant sa décentralisation), souvenons-nous que Nakamoto est l'instigateur de ce type d'usages, ayant inscrit la une du *Times* dans l'enregistrement de genèse\*. Les concepteurs de ces métaprotocoles ne cherchent pas à construire à côté, mais sur « *Bitcoin pour tirer parti de son réseau\* puissant et sécurisé soutenu par des pétahashes de puissance* » de calcul, ce qui n'est pas nouveau, Namecoin l'ayant déjà expérimenté « *sous une forme beaucoup plus faible, sous le nom de "merged mining"* » (*Ibid.*). Mais ces métaprotocoles vont plus loin en empruntant à Bitcoin non seulement sa sécurité (via la puissance de calcul des mineurs), mais aussi sa base de données et ses règles transactionnelles. L'idée est simple : le « *réseau\* bitcoin existant peut être utilisé comme une couche de protocole, sur laquelle de nouvelles couches monétaires avec*

---

<sup>185</sup>Voir <https://chromaway.com/about-us> [consultation au 29/08/2022].

*de nouvelles règles peuvent être construites sans changer les fondations* » (Willett 2012, p. 1). Pour ce faire, et bien que Bitcoin ne soit pas pensé pour les usages entrevus, ces protocoles utilisent certaines des instructions de son langage de programmation\*, en particulier les OP\_CODE « EPOBC » ou « OP\_RETURN », pour que de « *minuscules transactions\** Bitcoin [soient] *encodées dans la chaîne de blocs\** afin de prendre en charge et de représenter des transactions\* dans des couches de protocole plus élevées » (Bartoletti et Pompianu 2017, p. 1). Afin de sauvegarder et de lire des données sur la base de données Bitcoin, l'encodage et le décodage relèvent d'outils spécifiques à cette surcouche protocolaire, adaptés à leur logique de programmation propre. C'est une contrainte importante : ces protocoles, bien qu'ils usent de Bitcoin, relèvent d'une série de logiciels et services spécifiques (c'est-à-dire explorateur, portefeuille) nécessitant de leurs usagers, déjà *bitcoiners\**, l'administration de nouvelles clefs cryptographiques et de nouveaux logiciels. Enfin, leur fonctionnement partant du langage Bitcoin Script et des règles protocolaires canoniques existantes, leur développement n'est au départ pas censé rendre nécessaire l'obtention d'*« un consensus et [...] une adoption généralisée de la part de la communauté bitcoin [...] étant donné qu'aucune modification du protocole bitcoin de base n'est requise* (Ibid.). Ils pensent ne pas avoir besoin de l'avis des autres *bitcoiners\**. En s'en tenant à « *adhérez [...] aux règles du réseau\** [et à] *payez (...)* les frais appropriés », Bitcoin traitera leur transaction\* comme n'importe quelle autre, « *indépendamment de tout le reste* » (Keir 2022). Sur ce point, Willet et les autres se trompent : ces usages sont controversés et conduiront à l'entrée dans la « *guerre de l'OP\_RETURN* » (BitMEXResearch 2022).

Le protocole des *Colored Coins* a ouvert la voie, jouant sur l'absence de fongibilité des BTC (chaque UTXO\* est unique et traçable) ; il permet de « colorer »<sup>186</sup> une (micro)transaction\* en BTC et ainsi, de lui ajouter des informations supplémentaires permettant la création d'actif doté de propriétés et usages propres : produits financiers dérivés, tickets, points de fidélité, vote, financement d'un projet et parts dans celui-ci, versement de dividende au porteur, tokens d'accès à des services, représentation d'une propriété (numérique ou physique), etc. Pour ce faire, il use de l'OP\_CODE EPOBC afin d'implémenter en son sein deux types de transactions\*, celles de « genèse » servant à l'émission de *Tokens* et celles de « transfert », permettant leur circulation (Bartoletti et Pompianu 2017, p. 1). En parallèle des « pièces colorées », des métaprotooles plus complexes sont développés. Offrant un éventail étendu de fonctions, ils disposent de leurs propres UCN\* qui, comme pour Bitcoin, sont nécessaires à l'acquittement des frais afférents à leur usage. D'abord, le métaprotoole « Mastercoin » (pour « *Metadata Archival by Standard Transaction\* Embedding Records* », ticker : MSC) devenu « Omni » à la faveur d'un rebranding effectué en 2015 par les concepteurs (Rizzo 2015). Son réseau\*, lancé le 31 juillet 2013, fait suite à la publication par J.R. Willet, dès janvier 2012, du WP\* modestement intitulé « *The Second Bitcoin Whitepaper* » (Lars 2019a). La modestie ne s'arrête pas là, puisque les ambitions de *Mastercoin/Omni* sont d'éliminer « *les deux principaux obstacles à l'adoption généralisée du Bitcoin : l'instabilité et l'insécurité* » (Willett 2012, p. 1). Les concepteurs sont des *bitcoiners\** qui veulent moins concurrencer que compléter Bitcoin. Ils sont critiques de CM déjà apparues puisqu'elles « *concurrencent financièrement les bitcoins, brouillent [le] message au monde* », « *diluent [les] efforts* » et « *entravent la dynamique d'adoption du bitcoin et des autres monnaies, quelle que soit la qualité de leurs règles.* » (Ibid.). Cette stratégie de construire sur et non à côté doit susciter des effets opposés : en plus de permettre « *aux individus et aux groupes d'émettre de nouvelles monnaies avec de nouvelles règles expérimentales* » (Ibid.), le succès de ces métaprotooles doit renforcer « *la valeur et le succès du protocole Bitcoin de base* », puisqu'il

---

<sup>186</sup> La couleur n'est que métaphorique et l'identification se fait par un symbole (« ticker ») et un hash (Rosenfeld et al. 2013, p. 7).

*« bénéfie financièrement à l'ensemble de la communauté des utilisateurs de bitcoins, y compris à ceux qui n'utilisent pas » Mastercoin/Omni*, sans pour autant brouiller le message ou fragmenter les efforts de développement. Mais, comme avec les CM précédentes, une opposition apparaît sous forme de proposition : contrairement à Bitcoin et comme avec DASH, la question du financement de l'écosystème n'est pas laissée à une charité aussi arbitraire qu'incertaine. *MasterCoin/Omni vise à pouvoir « financer son propre développement logiciel, en se lançant lui-même dans l'existence, en utilisant une entité de confiance pour détenir des fonds et embaucher des développeurs\**. » (*Ibid.*). Ce protocole et son équipe seront financés par une vente publique des token MSC, sous forme d'une campagne de financement participatif d'un mois, acceptant exclusivement les BTC (sont levés 5 120 BTC équivalant à environ 500 000 dollars), par l'entremise d'une fondation (la « MasterCoin Foundation ») qui dispose de l'ensemble des UCN\* émises par prémine, très largement critiquée par les *bitcoiners\**, pour qui « une véritable cryptomonnaie\* ne devrait privilégier aucune partie centralisée spécifique de quelque manière que ce soit » (Buterin 2013a). En outre, J.R. Willet inaugure le phénomène des ICO, qui culmine en 2017. Sont critiqués : la concentration des UCN\* dans les mains du fondateur (J.R. Willet détient près de 30% du total) et le statut particulier octroyé à la fondation, seule entité à percevoir les frais de transaction\* de l'utilisation du protocole (Russo 2020, p. 41-42). S'il « est vrai que le modèle d'émission de Mastercoin n'est pas comme celui de Ripple [...], Ripple Labs est une société privée, tandis que la Mastercoin Foundation est une organisation à but non lucratif », reste que « la Mastercoin Foundation est une partie privilégiée, car personne d'autre n'a la possibilité de gagner des BTC grâce au processus d'émission » ; aussi, de « nombreux utilisateurs de Bitcoin estiment que [cela] empêch[e] le Mastercoin d'être considéré comme une monnaie véritablement décentralisée » (Buterin 2013a). Pour autant, ce protocole rencontre des succès qui permettront, en plus de son développement infrastructurel, celui d'autres CM dont Bitcoin. Au-delà des ICO, *MasterCoin/Omni* concrétise un cas d'usage annoncé dans le WP\* : permettre « aux utilisateurs finaux de créer des couches de protocoles monétaires ayant une valeur stable, liée à une monnaie ou à une marchandise extérieure » (Willett 2012). « Tether » (ticker : USDT) choisit ce métaprotocole pour l'émission et la circulation de ces USDT. En tant que premier *stablecoin* adossé au dollar, Tether participe grandement au développement des bourses d'échange et, ce faisant, de la valeur des CM et cryptoactifs qui s'y échangent. Il pose les bases d'une catégorie d'actifs qui deviendra centrale dans l'écosystème et qui conteste à Bitcoin son statut d'UCN\* pivot sur les marché cryptos : la grande majorité des volumes d'échanges de CM sera désormais libellée en *stablecoin* et non plus en BTC, dans ce qui s'apparente à une « *dollarisation de Bitcoin* » (Jp Koning 2015).

Finissons par le métaprotocole « Counterparty » (ticker de l'UCN\* : XCP), puisque nous l'avons nous-même utilisé pour recevoir, acheter et émettre nos premiers NFT et qu'il nous a permis d'appréhender l'opprobre communautaire que ces usages suscitaient (voir Annexe n°IV.1). Lancé en janvier 2014, il est assez similaire à ses prédécesseurs, bien que plus complet en ce qu'il introduit les scripts à exécution programmatique (ou « *Smart Contract\** ») et « une série d'outils [fournissant] à ses utilisateurs la première bourse d'actifs numériques peer-to-peer au monde, une fonctionnalité de paris et un marché de produits dérivés » (Dermody 2014). On retrouve des UCN\* qui circulent afin d'assurer le paiement des frais afférents à l'usage du protocole et une émission par prémine. Les UCN\* XCP sont créés en échange de l'envoi de BTC, mais les concepteurs se distancent des innovations récentes pour revenir à un ethos plus *bitcoiner*. Pas de centralisation : ils créent un mécanisme de brûlage de BTC (« *proof of burn* ») où les souscripteurs envoient des BTC à une adresse dont la clef privée a été détruite (donc est devenue inutilisable), permettant de recevoir en contrepartie les XCP (l'émission débutée le 02

janvier 2014 dura 30 jours et près de 2 131 BTC furent brûlés<sup>187</sup> pour la création de près de 2,6 millions d'XCP créés ; (Brokaw 2014; Lars 2019a). En ce « début 2014, l'expérimentation, l'activité des développeurs\*, l'innovation et l'enthousiasme étaient considérables autour de Counterparty, qui avait une longueur d'avance sur une plateforme rivale » Mastercoin/Omni : elle pouvait héberger des « Applications décentralisées » (ou « Dapp ») comme des plateformes d'échange distribuées (ou « DEX »), l'émission de jetons, etc. (BitMEXResearch 2022). Pour ce qui est de la mesure de ces usages de surcouche, l'analyse des transactions\* utilisant l'instruction « OP\_RETURN »<sup>188</sup> en départira quatre types ((Bartoletti et Pompianu 2017, p. 6) : la création et la gestion d'actifs (27,2%); la notarisation de documents (9,3%) ; l'Art digital avec des protocoles de déclaration des droits d'accès et de copie sur les fichiers numériques (6,3%) ; enfin des applications regroupant des usages différents des trois autres (« Autres », pour 11,9%). Les transactions\* analysées constituent seulement 0,92% de l'ensemble des transactions\* Bitcoin (et près de 0,3% de son espace d'enregistrement, *Ibid.* p. 11). Chacun d'eux se développe sur le fait que Bitcoin jouit d'une perception positive en terme de « sécurité et de [...] persistance de [s]a blockchain » (*Ibid.*, p. 11). Pour autant, de quelques centaines de transactions\* OP RETURN effectuées par semaine en 2014, on est passé à près de 20 000 en novembre 2016, suivant une augmentation régulière depuis mars 2015.

Avant même d'atteindre de telles proportions, ces usages non monétaires de Bitcoin furent controversés et ces métaprotocoles, malgré une volonté de complémentarité, allaient ouvrir un conflit que certains qualifient de « guerre de l'OP\_RETURN » (BitMEXResearch 2022). Si, avant 2014, les codes originaux de Bitcoin faisaient que « les transactions\* contenant un OP\_Return n'étaient pas standards et n'étaient pas relayées par les nœuds\* Bitcoin ordinaires » (*Ibid.*), ils ont toujours autorisé malgré eux<sup>189</sup> la consignation de données arbitraires en sus de celles transactionnelles : il suffisait qu'elles soient incluses par un mineur pour être considérées comme valides (*Ibid.*) et d'autres méthodes pouvaient être utilisées<sup>190</sup>. Dans tous les cas, cela impactait négativement les nœuds\* Bitcoin qui les stockaient dans leur mémoire vive (Bartoletti et Pompianu 2017, p. 4). C'est contre ces « schémas de stockage de données [...] gonflant ainsi la base de données UTXO\* de Bitcoin » (Bitcoin Core 2014) que, en mars 2014, la version 0.9.0 du logiciel Bitcoin fait de l'instruction OP\_RETURN un type de transaction\* standard, dorénavant relayé par défaut (BitMEXResearch 2022). Il ne faut pas y voir « une approbation du stockage des données dans la blockchain » (*Ibid.*), car c'est au contraire un moyen de l'empêcher ou, tout du moins, de limiter ceux qui étaient considérés

---

<sup>187</sup> Voir <https://blockchair.com/bitcoin/address/1CounterpartyXXXXXXXXXXXXXXUWLpVr> [consultation au 02/09/2022].

<sup>188</sup> Leur analyse couvre les transactions entre le 19 mars 2014 (date de l'implémentation de l'OP RETURN) et le 9 novembre 2016, pour un échantillon de 1 566 192 transactions OP\_RETURN. Ils identifient 23 protocoles (associés à 34 identifiants) et 3 protocoles qui n'utilisent aucun identifiant (dont CounterParty). Aussi, 55% des transactions ont pu être liées à un protocole en particulier, les 45% restant ayant été catégorisés dans les catégories « Unknown » et « empty » (Bartoletti et Pompianu 2017, p. 5). Notons qu'une telle évaluation est une sous-estimation puisque l'OP\_CODE leur servant à discriminer les transactions n'est pas le seul à avoir été utilisé : en plus de OP\_CODE EPOBC utilisé par le protocole des ColoredCoins, Counterparty en a d'abord mobilisé un autre, plus coûteux, OP\_CHECKSIG ou OP\_CHECKMULTISIG, voir [https://github.com/CounterpartyXCP/Documentation/blob/master/Developers/protocol\\_specification.md](https://github.com/CounterpartyXCP/Documentation/blob/master/Developers/protocol_specification.md) [consultation au 02/09/2022].

<sup>189</sup> Suivant la dynamique carnavalesque que nous avons décrite et même si « les transactions Bitcoin ne prévoient pas de champ où enregistrer des données arbitraires [...], les utilisateurs ont imaginé diverses manières créatives d'encoder des données dans les transactions. » (Bartoletti et Pompianu 2017, p. 3)

<sup>190</sup> Étaient impliqués les standards transactionnels « Pay-to-PubkeyHash » (Bartoletti et Pompianu 2017, p. 4) ou, dans le cas de Counterparty, le « pay to script hash » et l'instruction OP\_CHECKMULTISIG (BitMEXResearch 2022).

comme des dommages causés à Bitcoin (Garzik 2014b)<sup>191</sup>. Avant cette version, « les règles de consensus de Bitcoin autorisent une taille d'OP\_Return allant jusqu'à 10 000 octets », avec Bitcoin Core 0.9.0, les transactions\* OP\_Return, pour être relayées, devront être inférieures ou égales à 40 octets et non à 80 octets, limite discutée à l'origine (BitMEXResearch 2022). Le choix par les développeurs\* Bitcoin de cette limite basse rend « difficile le fonctionnement de Counterparty et d'autres plateformes au-dessus du protocole Bitcoin. » (Young 2017) Les bitcoiners\* qui désiraient étendre les usages non monétaires de Bitcoin doivent se rendre à l'évidence que la majorité des bitcoiners\* y est hostile. Déjà, ces métaprotooles et leur logique de fonctionnement sont critiqués techniquelement : il faut y voir une « pure paresse intellectuelle » puisqu'il était possible de remplacer leur donnée lourde par un simple « horodatage\* de hash\* (données) [...] tout aussi sûr, tout en étant plus efficace », voire d'implémenter une chaîne secondaire (dite sidechain) (Garzik 2014a). Ensuite, des débats entourent les effets potentiels de ces usages et la capacité de mise à l'échelle\* de Bitcoin. On interroge les coûts et bénéfices induits et la soutenabilité à long terme : de l'avis général, ces usages sont des comportements de « passager clandestin, étant donné que la majorité écrasante (> 90%) des demandes d'utilisation de la chaîne de blocs\* de Bitcoin sont des demandes de monnaie, utiliser des nœuds\* complets comme terminaux de stockage de données stupides revient [...] à abuser d'une ressource réseau\* entièrement bénévole » (Garzik, cité par Russo 2020, p. 56), obligeant « les non-participants à stocker les données » « contre leur gré » (Dashjr 2014a). Valide protocolairement, les transactions\* des métaprotooles sont considérées par la majorité des bitcoiners\* comme « non conformes au protocole bitcoin », suivant qu'elles détournent les instructions de Bitcoin script de leur fonction première, induisant immanquablement « des conséquences négatives, peut-être involontaires ou inconnues » (Garzik cité par BitMEXResearch 2022). La mise en place de ces limitations d'usages sera majoritairement considérée comme légitime, prouvant qu'il ne faut pas seulement se conformer au protocole, mais aussi « à l'intention des développeurs\* », et c'était le point de vue « partagé [...] par presque tous les développeurs\* actifs à l'époque » (*Ibid.*).

Contre ceux qui détournent ces règles protocolaires, Bitcoin et acteurs non humains ne pouvaient rien. Moins impotents, des acteurs humains réagirent rapidement et discrétionnairement suivant que les « problèmes humains nécessitaient des solutions humaines » : L. Dashjr, développeur Bitcoin reconnu et opérateur d'un pool de minage, développa un dispositif visant à sanctionner / filtrer ce type de « transactions\* abusives/spam » car, selon lui, les « mineurs [doivent] filtrer ces abus » et « prendre leurs propres décisions en matière de politique » sans « jamais se contenter du code minier par défaut de Bitcoin Core » (Dashjr 2014a; Dashjr 2014b). De ces coercitions, la minorité fut critique. Les régulations protocolaires de Bitcoin étaient distordues pour de faux prétextes car, « dans un monde idéal » où le code serait vraiment loi, « le concept d'« "abus" n'existerait même pas ; les frais seraient obligatoires et soigneusement structurés pour correspondre au coût réel qu'une transaction\* donnée impose au réseau\*. » (Buterin cité par BitMEXResearch 2022). Par un effet retour négatif, cette baisse à 40 octets allait « par inadvertance [rendre l'] OP\_RETURN moins attrayant » rapporté aux solutions anciennes, bien plus lourdes, qu'elle était censée empêcher. La volonté des développeurs\* de Counterparty « d'agir en tant que partenaires responsables », prêts à « à travailler ensemble sur ces questions » avec les développeurs\* Bitcoin n'y change rien (*Ibid.*).

---

<sup>191</sup> « C'est un moyen de rendre les données moins dommageables [car] MasterCoin et d'autres projets faisaient des choses encore pires, comme le stockage de données dans des sorties TX indéfiniment inutilisables, gonflant l'UTXO pour l'éternité ». (Garzik 2014b)

L’animosité à l’égard de *Counterparty* d’une part de la communauté de *bitcoiner* était en partie suscitée par le fait que son lancement coïncidait avec la première augmentation des frais de transactions\* que connaît Bitcoin (nous avons éprouvé pratiquement l’un et l’autre de ces phénomènes lors de nos immersions participantes au sein des diverses communautés Counterparty, voir Annexe n°IV.1). Ces frais obéiraient le développement futur des solutions de pièces colorées ou des métaprotooles, et la plupart des projets de DApp lancés sur *Counterparty* se virent poussés à migrer.

### I.3.2 Ethereum : continuité et rupture d’avec Bitcoin et les expériences passées

Ce qui précède joue pour Ethereum, notre deuxième cas d’étude, le rôle d’introduction nécessaire. Les métaprotooles ont inspiré Buterin, qui souhaite offrir un protocole de registre\* distribué hébergeant, au-delà d’usages monétaires de son UCN\*, un éventail large d’activités. Aussi, « *les toutes premières versions du protocole ETH étaient un métacoin de type Counterparty* ». Bitcoin n’a pas été retenu à cause des incertitudes que faisait peser la rigidité de sa communauté : « *les guerres OP\_RETURN se déroulaient à l’époque et compte tenu de ce que certains Core développeurs\* disaient, [Buterin] avai[t] peur que les règles du protocole changent sous [s]es ordres [et ne souhaitait] pas construire sur un protocole de base dont l’équipe de développement serait en guerre contre [lui]* » (Buterin 2017a°; 2017b°; Young 2017). Car « *c'est la culture de la communauté de développement de Bitcoin en 2014 et la vision négative de l'utilisation des données de transaction\* de Bitcoin pour des cas d'utilisation alternatifs qui ont joué un rôle majeur en poussant les développeurs\* de ces Dapps vers des systèmes alternatifs comme Ethereum* » (BitMEXResearch 2022). Ethereum, comme Bitcoin et les autres CM, n’émerge pas *ex nihilo*. Sa conception bénéficie, en plus du terreau matériel et idéal de Bitcoin déjà présenté, des cinq années de développement infrastructurel et d’expérience accumulée au sein de la communauté Bitcoin et de celles, plus larges, de l’écosystème des CM. Comme pour toute CM, son creuset emprunte à Bitcoin et s’enrichit de critiques de ce qui est perçu comme ses rigidités protocolaires ou infrastructurelles, mais ces critiques s’adressent plus largement aux expériences qui l’ont précédé et auxquelles les acteurs de sa conception ont participé. D’où un design et un fonctionnement dont les arrangements sociotechniques sont plus radicalement différenciés.

### Ethereum : une conception par des *insiders* reconnus de l’écosystème des CM

Comme pour la plupart des CM l’ayant précédé et contrairement aux mystères entourant le(s) créateur(s) de Bitcoin, la conception d’Ethereum est le fait d’un groupe formellement reconnu, structuré et financé, et il est donc plus facile de retracer les acteurs et réseaux\* sociaux ayant participé à sa genèse. Ethereum est le fait d’un groupe de *bitcoiners\** de la première heure, au centre duquel un démiurge entouré de fondateurs et de contributeurs, tout sauf anonymes. L’idée originale, remontant à la fin 2013, a été développée par Vitalik Buterin, un jeune Russo-Canadien, qui va constituer autour du projet une équipe composée d’acteurs déjà insérés dans les communautés de *coiners\**. Les membres co-fondateurs, malgré des cursus et compétences diversifiés (ingénieurs informatiques, mathématiciens, investisseurs disposant de capital économique important ; voir Annexe n°III.14) partagent, en plus d’un intérêt pour Bitcoin et les CM, un haut niveau de capital culturel (Russo 2020, chap. 5, 6 et 8). C’est l’intérêt pour Bitcoin et leurs implications dans différents groupes, événements et communautés constituées autour qui est le vecteur de leur rencontre (*Ibid.*). Buterin fait la connaissance de ses futurs collaborateurs au gré de son implication dans l’écosystème Bitcoin, puis dans celui des pièces colorées et des métaprotooles. Ils connaissent donc bien les heures et malheurs de ces expériences et les affres de leur développement infrastructurel, en particulier pour ce qui est de leur évolution protocolaire. Ce qui explique l’altérité de certains de leurs choix architecturaux.

Buterin fut initié à Bitcoin en 2011 par son père ingénieur informatique, alors qu'il n'avait que 17 ans. Piqué d'intérêt, il connaît un parcours de socialisation typique de l'époque : suivant ses nombreuses lectures des ressources en ligne, il participe aux discussions ayant cours sur *BitcoinTalk* qu'il a rejoint en mars 2011. Là, il gagne ses premiers bitcoins en contrepartie de la rédaction d'articles (*Ibid.*, p. 22)<sup>192</sup>. Leur qualité et leur visibilité conduisent, dès août 2011, au rapprochement avec un autre *bitcoiner*, Mihai Alisie (qui a découvert Bitcoin de par ses activités de joueur et coach de poker), avec qui il édite le premier magazine spécialisé : *Bitcoin Magazine* (Russo 2020 Chap. 2). Cette collaboration en entraîne d'autres. Buterin, à la faveur d'un tour du monde, participe à de nombreux événements autour des CM et c'est là qu'il rencontre nombre des acteurs de premier plan de cet écosystème. En 2013, Mihai Alisie l'invite en Europe pour travailler sur *Bitcoin Magazine* et sur son projet d'eBay construit sur Bitcoin – Egora. Lors de leur première rencontre physique, dans la région de Barcelone, ils croisent la route d'Amir Taaki, militant et développeur Bitcoin (à qui l'on doit la procédure des BIP), avec qui ils passent deux mois dans un lieu anarchiste autogéré appelé Calafou<sup>193</sup> (Castillo 2013, Russo 2020, p 35-36). Buterin, en plus de participer au projet *Egora*, prend part au développement de *Dark Wallet* de Taaki. Sa rencontre avec les acteurs des metaprotocoles se fait à Tel-Aviv, où il croise Yoni Assia de la plateforme de trading *e toro*, intéressé à l'époque par les pièces colorées (*Ibid.*, p. 43). Buterin est logé chez un ami d'Amir Chetrit, acteur rencontré en septembre 2013 lors d'une conférence Bitcoin à Amsterdam et qui travaille pour une start-up lancée dans cette technologie. Cela le conduit à rejoindre l'équipe de Rosenfeld et Mizrahi, afin de participer à l'écriture d'une nouvelle version du WP\* (« Colored Coins - Bitcoin X », Rosenfeld et al. 2013). C'est l'occasion d'une première déconvenue : sa proposition est critiquée par l'équipe du projet qui n'y trouve aucune référence à ses travaux passés. Mizrahi est critique : Buterin aurait « *commencé à l'écrire [le livre blanc] sans discussion préalable* », il était « *à peine au courant des sujets* » déjà abordés, et souhaitait « *tout terminer en un ou deux mois* », donnant l'impression d'un WP\* « *rédigé au hasard* » ; quant « *à ses idées, il en avait beaucoup* », mais d'après lui, elles « *n'étaient tout simplement pas bonnes* » et aucune n'est mise en œuvre (Russo 2020, p. 47). Tant pis pour leur rigidité, Buterin forge ses connaissances, ses convictions et son réseau\*. Encore à Tel Aviv, il rencontre Ron Gross, chef de l'équipe de développement du métaprotocole Omni/Mastercoin, avec lequel il collabore (Buterin 2017b). *Idem*, chargé de la rédaction des spécifications techniques d'un dispositif singulier (les « *contracts for differences* », sorte de produit dérivé), voilà que Buterin finit par proposer de remplacer « *presque tout ce* » qui avait été fait auparavant. De nouveau, ses recherches le conduisent à critiquer le protocole d'Omni/Mastercoin et son développement. D'après lui, le protocole est trop compartimenté, « *peu structuré pour développer ses idées* », qui doivent y être traitées « *chacune comme un "élément" distinct* » relevant de règles *ad hoc* « *avec son propre code de transaction\** et ses propres règles » (Buterin cité par Russo 2020, p. 45). Lui a en tête « *quelque chose de bien plus puissant* », « *plus propre et plus généralisé* » (*Ibid.*). Si sa proposition « *de spécifier les contrats Mastercoin [suivant] une philosophie ouverte* » via un langage de programmation\* (« *scripting* ») *ad hoc* fait sur Gross et Willet forte impression, ils la refusent. Willet concéda que ce type de question avait déjà été tranché : lui-même avait initialement « *évité d'écrire des scripts lorsqu'[il a] rédigé les spécifications, [de] peur de ne pas pouvoir prendre en compte tous les cas de figure et les éventuels piratages et failles de sécurité. [...] Quel que soit le scénario [...] défini, les gens allaient trouver des*

<sup>192</sup> L'utilisateur Kiba souhaite payer en BTC des rédacteurs de contenu pour son blog « *Bitcoin Weekly* ». Voir <https://bitcointalk.org/index.php?topic=4916.msg72174#msg72174> [consultation au 04/09/2022].

<sup>193</sup> Ce lieu, décrit comme « *une colonie éco-industrielle post-capitaliste* » a été créé par Enric Duncan, militant anti-capitaliste reconnu. On lui doit un système frauduleux de souscription de crédits bancaires qu'il ne vise nullement à rembourser (492 000 euros dans 39 banques) et le projet de CM coopérative le *Faircoin* (Schneider 2015; Russo 2020).

"transactions\* empoisonnées" » permettant d'« *en abuser* »; *Ibid*, p. 46). Trop radicalement différente des travaux passés, trop complexe et risquée à mettre en œuvre, cette proposition - et son refus - annonce Ethereum : y sont en germes ses avantages comme ses inconvénients<sup>194</sup>.

Pour Buterin preuve est faite qu'il n'y a pas que Bitcoin, qu'il est difficile de changer. Le développement infrastructurel d'une CM produit des dépendances au sentier, reposant sur des équipes constituées et des sentiers de développement qu'il est bien difficile, voire impossible, de faire évoluer radicalement. La « *guerre de l'OP\_RETURN* » lui a prouvé que Bitcoin n'était pas fait pour héberger son métaprotocole, trop contraignant – protocolairement, mais surtout infrastructurellement. Pour garantir à Ethereum et à sa communauté des marges de manœuvre suffisantes, Buterin cherche un espace où ils pourront « *prendre une part plus grande de la communauté* ». Son choix s'arrête sur un protocole qui lui apparaît « *particulièrement ajusté pour son projet [car] plus petit, avec moins de conflits politiques* » : *Primecoin* (Russo 2020, p. 57). Buterin rédige la première version du WP\* d'Ethereum fin novembre 2013<sup>195</sup>, lorsqu'il est hébergé chez Stephan Thomas, le CTO de Ripples qu'il connaît de Jed McCaleb, le fondateur et CEO qu'il avait contacté en février 2013. Ce WP\* circule bien au-delà des 13 personnes auxquelles il était adressé pour avis et c'est l'enthousiasme suscité qui va convaincre Buterin qu'Ethereum mérite d'être un protocole, un réseau\* et une chaîne de blocs\* propres et non de surcouche (Buterin 2013d; Russo 2020, p. 56-57).

### Ethereum : une synthèse matérielle et idéelle critique des expériences passées

Au flou informel du lancement de Bitcoin, les CM qui le suivent répondent par des structures de développement plus formalisées, définissant *a priori* des acteurs, des entités juridiques et même des voies de financement. Ethereum n'y déroge pas. À la manière de Nakamoto, Buterin est considéré comme le démiurge d'Ethereum auquel on concède la paternité de l'idée originale, d'où un capital symbolique important (Buterin 2013a; Buterin 2013d). Mais la mener à bien nécessite d'être entouré. Fin 2013 se constitue une équipe de fondateurs autour de Buterin, qui recrute parmi ses connaissances. Au départ, cinq sont reconnus : Buterin, Alisie, Di Iorio, Hoskinson et Chetrit (sur les liens qui les lient, voir l'annexe n°3) ; s'y ajouteront trois autres - Wood, Wilcke et Lubin, gratifiés de ce statut de par l'importance de leur contribution au lancement d'Ethereum. Contrairement à Bitcoin, le WP\* d'Ethereum n'en expose que des orientations générales, et aucun logiciel client n'est encore implémenté. L'architecture et les spécifications du protocole Ethereum de Buterin sont loin d'être finalisées. Nécessaires à toute implémentation logicielle, ces spécifications sont développées par Gavin Wood et Buterin, à partir de décembre 2013. Wood joue un rôle de premier plan dans le développement de la couche protocolaire (Buterin 2017b) puisqu'on lui doit le développement du langage de programmation\* natif d'Ethereum : Solidity<sup>196</sup>. Il est aussi en charge du développement de l'implémentation de logiciel client rédigée en langage C++, en parallèle de J. Wilcke en charge d'un client en langage Go, et de Buterin s'occupant de celui en

---

<sup>194</sup> Willet mobilise l'une des principales critiques faite à Ethereum. S'il reconnaît « *que le scripting pourrait être une fonction avancée qui apporterait beaucoup de valeur ajoutée* », reste deux obstacles à son implémentation rapide : déjà « *nos développeurs\* risquent de s'enlisier dans les détails* » ; ensuite et surtout, cela impliquerait que « *le nombre de cas critiques se multiplierait (je pense) de façon exponentielle* ». Privilégiant la sécurité, Willet « *préfère voir Mastercoin faire ses fonctions de base avant* » d'*« expérimenter avec les scripts.* » (Russo 2020, p.46). Cette crainte est fondée, comme le cas d'étude The DAO du Chap. III l'illustre, et à la grande plasticité offerte par Ethereum répond une plus grande surface de vulnérabilités et d'attaques.

<sup>195</sup> Voir <https://ethereum.org/en/whitepaper/> [consultation au 07/03/2016].

<sup>196</sup> Voir <https://solidity.readthedocs.io/en/v0.7.2/> [consultation au 26/07/2021].

Python (Buterin 2014c)<sup>197</sup>. Les clients de Wood et Wilcke donneront corps au protocole envisagé, fonctionnant de concert pour donner naissance au premier réseau\* testnet (Russo 2020, p. 112). Enfin, c'est le même Wood, en avril 2014, qui publie les spécifications protocolaires à proprement parler à travers un « *Yellow paper* »<sup>198</sup> complétant en détail ce que n'avait qu'introduit le WP\* de Buterin. Finalement, huit personnes sont gratifiées du statut de co-fondateurs d'Ethereum, bien que Hoskinson et Chetrit soient mis de côté rapidement sur décision de Buterin (Russo 2020, p. 123).

D'autres personnalités de l'écosystème rejoignent le développement d'Ethereum, comme Stephan Tual, nommé *Chief Creative Officer* et Taylor Gerring (ayant travaillé sur des applications en surcouche de Bitcoin, il rencontra Alisie lors d'un Hackathon à Milan, fin 2013, Russo 2020, p. 99). L'annonce officielle d'Ethereum est faite le 26 janvier 2014, à Miami, durant la conférence « North American Bitcoin Conference » où est réuni l'ensemble des fondateurs, suivant la présentation de Buterin intitulée « Vitalik Buterin, head writer at *Bitcoin Magazine* », qui va connaître un succès notable. S'ensuivront de nombreux événements et conférences, durant lesquels de nouvelles recrues rejoindront l'équipe de développement (Russo 2020, p. 87)<sup>199</sup>. Au total, pas moins de 83 contributeurs initiaux travaillent sur Ethereum avant même sa campagne de financement et son lancement (Russo 2020, p. 138). Du haut de leurs expériences accumulées dans l'écosystème, Buterin et ses co-fondateurs reprennent en partie certains des arrangements que d'autres CM ont introduits : ICO, création d'une fondation, prémine d'une partie des UCN\*, etc. Puisque les problématiques liées au financement du développement de l'écosystème (de la couche protocolaire, mais aussi applicative) sont cruciales, le modèle choisi s'inspire plus de *Mastercoin/Omni* que de Bitcoin. Dès les premières conceptualisations d'Ethereum, les co-fondateurs envisagent une campagne de financement participatif permettant d'assurer, à moyen terme, les conditions d'un développement durable d'Ethereum par constitution de fonds propres dédiés : le mécanisme de financement présenté dès le WP\* de 2013 repose sur la prévente d'UCN\* Ether préminées à hauteur des contributions reçues en BTC et serviront à couvrir les coûts - passés et futurs - du développement du protocole (Buterin 2013d)<sup>200</sup>. Malgré l'expérience de *MasterCoin/Omni*, des incertitudes juridiques subsistent sur ce nouveau canal de financement qui pourrait tomber sous le coup des réglementations relatives à l'émission de titres financiers (Russo 2020, p. 89). Choix est fait qu'une levée de fonds réalisée sous l'égide d'une entité juridiquement reconnue, dont il reste à définir les statuts (entreprise privée à but lucratif ou fondation à but non lucratif) et la juridiction (Suisse ou Singapour, (Alisie 2014) Russo 2020, Chapitre 10). Pour la juridiction, c'est la

---

<sup>197</sup> À côté du langage C++ (déjà abordé pour Bitcoin), se trouve une diversité de langages de programmation. Go ou Goland, un langage open source créé par Google en 2009, se distingue des autres (dont il combinerait les avantages) par sa facilité d'utilisation, son efficacité de haut niveau et ses performances avancées pour la mise en réseau et l'utilisation de la puissance multicoeur. Python, lui aussi, bénéficie d'une syntaxe simple et lisible qui en fait un des langages de programmation de blockchain\* les plus populaires. Pour les avantages et inconvénients de chacun, voir FreeCodeCamp 2019; Breed 2020; Kumar Jain 2023.

<sup>198</sup> Voir la dernière version ici <https://ethereum.github.io/yellowpaper/paper.pdf> [consultation au 17/03/2018].

<sup>199</sup> Témoin de ce succès cette photo <https://ohiobitcoin.com/vitalik-buterin-ethereum-a-star-is-born-north-american-bitcoin-conference-in-miami-jan-2014-2/>, présentations accessibles ici <https://bobsummerwill.com/ethereum-foundation-timeline/> [consultation au 26/06/2021].

<sup>200</sup> « *L'Ether sera distribué par une vente [...] au prix de 1 000 à 2 000Ether par BTC, un mécanisme visant à financer l'organisation Ethereum et payer les développements qui a été utilisé avec succès par d'autres plateformes telles que Mastercoin et NXT. [...] Les BTC reçus seront utilisés en totalité pour payer les salaires et les primes des développeurs\* et à investir dans divers projets, à but lucratif ou non, de l'écosystème Ethereum et des cryptomonnaies en général. 9,9M du montant total vendu (60 102 216 ETH) seront alloués à l'organisation pour rétribuer les contributeurs initiaux et régler les dépenses liées à ETH effectuées en amont du bloc de genèse. 9,9% du montant total vendu sera conservé comme réserve de fonds à long terme. 26% du montant total vendu sera chaque année alloué aux mineurs, sans limite dans le temps.* » (Buterin 2013d)

Suisse, pour ses facilités légales et fiscales, précisément le canton de Zoug, s'érigeant à l'époque en « crypto valley »<sup>201</sup>. Mais la question du statut et subséquemment du positionnement d'Ethereum est à l'origine d'un conflit entre co-fondateurs dont la résolution passe par l'éviction d'Hoskinson et Chetrit. Deux camps se font face : les uns (Hoskinson, Di Iorio et Lubin) militent pour la création d'une entreprise à but lucratif, là où les autres, au premier chef desquels Buterin, préfère le statut d'une fondation à but non lucratif (Shin 2022, p. 43-44; camps structurant de la crise du HF consécutif à l'attaque de "The DAO", cf. Chap. III.3.3). Cette option partagée s'inscrit dans l'esprit libertaire d'une partie de l'équipe et doit garantir un développement infrastructurel plus décentralisé. D'ailleurs, ce choix n'obère en rien la possibilité pour des entreprises de développer des activités lucratives sur la couche applicative. Buterin tranche, l'« Ether Genesis Sale » sera réalisée sous l'égide de l'« Ethereum Fondation » (EF<sup>202</sup>), qui n'est ni « une entreprise, ni un organisme à but non lucratif traditionnel » et dont le rôle est de « soutenir "Ethereum" et les technologies qui y sont associées » sans pour autant « ni [...] contrôler ni [...] diriger Ethereum, ni [...] être la seule à financer le développement essentiel des technologies » connexes. L'EF est conçue pour n'être qu'une des parties prenantes « d'un "écosystème" bien plus grand » constitué « d'organisations, d'individus et d'entreprises qui soutiennent Ethereum »<sup>203</sup>. Avant même le lancement, la conception d'Ethereum a induit des coûts substantiels, et les contributeurs ont travaillé plus de 6 mois sans rémunération, se finançant sur deniers personnels<sup>204</sup> (Russo 2020, p. 94). Lever des fonds devient nécessaire et l'« Ether Genesis Sale » débute le 22 juillet 2014 pour une durée de 42 jours (Gerring 2014; Buterin 2014c). En échange de BTC, on peut acheter de futures UCN\* ETH, non encore réellement émises, et la prévente incite les primo-entrants : le prix de l'Ether est de 2 000/BTC pour les 14 premiers jours, puis ce ratio diminue linéairement jusqu'à son atteindre 1 337 ETH/BTC (pour les 6 derniers jours, Buterin 2014). Le montant total d'Ether créé par la prévente est une variable essentielle, d'où le fait qu'il ne soit fixé aucun plafond pour la création d'ETH, ni pour le montant collecté. Il détermine la création d'ETH alloués au développement d'Ethereum (19,8% du montant créé par la prévente) répartis à parts égales entre les contributeurs et la Fondation Ethereum (Hasu 2018). Mais il détermine aussi en partie le monnayage, puisqu'aux UCN\* de la prémine s'ajouteront celles émises comme récompense de création monétaire, qui ne devront pas dépasser 26% du total des ETH vendus (Buterin 2014c). Cette prévente est un succès, que certains voient comme relevant d'une orchestration soulevant des questions juridiques<sup>205</sup>. En seulement 12 heures, 3 700 BTC sont

<sup>201</sup> En une décennie, la Suisse est devenue une juridiction privilégiée des acteurs de l'écosystème des CM, de par son cadre légal. Le canton de Zoug, par la forte présence de start ups qui s'y enregistrent (Raynal 2017), et sa réglementation locale favorable (une partie des impôts locaux peut être acquittée en cryptoactifs, Baker 2020) a ainsi été dénommé de « crypto valley ».

<sup>202</sup> L'EF n'est pas la seule structure juridique mise en place, l'entreprise EthSuisse GmbH doit recevoir les fonds levés (Russo 2020, Chapitres 12 et 14) ; ou l'entreprise Ethdev servant à payer les développeurs\* [B. Summerwill, Entretien n° 26], cf. Chap. III.

<sup>203</sup> Voir <https://ethereum.org/fr/foundation/> [consultation au 23/03/2022].

<sup>204</sup> Notons des dépenses dédiées au financement locatif (bureau et logement) et aux coûts juridiques induits par la campagne de financement (comprise entre 500 000\$ et 800 000\$, à en croire Lubin ou Di Iorio, voir Russo 2020, p. 94), auxquels s'ajoutent des dépenses personnelles, car « certains avaient quitté leur emploi et n'avaient pas vu un seul satoshi dans leur portefeuille\* Bitcoin depuis six mois, tandis que d'autres s'inquiétaient de nourrir leur famille et de payer leur hypothèque » (Gerring 2016).

<sup>205</sup> L'avocat spécialisé Preston Byrne (2018) « se demande si cette vente ne relèverait pas d'une émission de titres » car, contrairement à la décentralisation souvent avancée pour invalider cette qualification juridique, il lui semble que les données *on chain\** de la présale pointent l'inverse, elles apparaissent « presque trop parfait[es] pour un effort non coordonné de plusieurs milliers de contributions sur deux semaines, surtout [comparé à] d'autres collecteurs de fonds comme Kickstarter, Swarm ou Tezos ICO. »(Hasu 2018).

levés (Tanzarian 2014) et, à sa clôture, pas moins de 31 725 BTC<sup>206</sup> (pour une valeur de 18 Millions de \$ à l'époque)<sup>207</sup>. Finalement, à cette occasion, ce sont 72 102 216 d'ETH qui sont créés (60 102 216 seront distribués aux participants de la levée de fonds). L'émission et la distribution effective de ces UCN\* attendront le lancement du réseau\* et la production de l'enregistrement de genèse<sup>208</sup>. Ce lancement effectif sera précédé d'efforts marketing, comme avec l'organisation de conférences dédiées à Ethereum (exemple de la *DEVcon-0*, à Berlin le 24 novembre 2014<sup>209</sup>) et d'efforts de développement : « Olympic », dénomination de la neuvième itération du testnet, en date du 9 mai 2015, établit la dernière preuve de concept avant le lancement (9 auront été développées, slacknation 2017). Ethereum passe du « rêve » (Gerring, 2016) à la réalité le 20 juillet 2015, avec la publication de « Frontier » (première version « mainnet » du protocole). Suivant la création du bloc de génèse, les 60 000 000 d'ETH de la prévente sont libérés à l'adresse des participants, comme la part de 5,9 millions dédiée au développement (Buterin ayant reçu près de 553 000 ETH, Russo 2020, p. 138).

À ces UCN\* qui peuvent déjà circuler, Ethereum ajoute protocolairement celles distribuées sous forme de récompenses aux opérateurs du traitement et de l'enregistrement des transactions\*, mais, comme nous allons le voir, Ethereum et ses concepteurs radicalisent leur différence d'avec Bitcoin dans ce domaine.

### 1.3.3 Ethereum, des recompositions d'alliances contre les rigidités de Bitcoin

Ainsi, à la suite de Bitcoin, les CM ont essayé d'étendre sa logique de consensus à d'autres domaines suivant deux grandes voies : soit par la création de protocoles autonomes à usage spécialisé, soit par l'utilisation de dispositifs permettant des usages non spécifiquement monétaires et reposant en surcouche de Bitcoin. Buterin, qui suit les évolutions de l'écosystème depuis 2011, reconnaît l'intérêt de ces stratégies, dont les réponses communautaires suscitées sont « *la seule preuve qu'elles essaient de faire quelque chose qui est très nécessaire* » (Buterin 2014j). Restent selon lui, des limites intrinsèques, expliquant des succès relatifs.

### Ethereum : des arbitrages sociotechniques différenciés

Buterin vise en premier lieu à éviter la fragmentation induite par les stratégies précédentes : différentes technologies nécessitent différentes connaissances, outils et savoir-faire (chaque CM possède différentes suites logicielles, etc.), reposant sur différentes communautés. Ensuite, créer de nouveaux protocoles de registre\* distribué autour d'usages et d'applications spécifiques est coûteux, risqué et potentiellement non soutenable. Cela induit une grande complexité technique et un travail de conception important, car chaque nouvelle « *implémentation doit recommencer à zéro une chaîne indépendante, et nécessite l'écriture et les tests de tout le code de transition d'état et de réseau\** », sans même que ces protocoles ne soient assurés de rencontrer une demande justifiant leur développement. Puisque, pour Buterin, « *l'ensemble des applications de la technologie de consensus décentralisé suivra une distribution en loi de puissance où la très grande majorité des applications seront trop peu importantes pour justifier leur propre blockchain* » (Buterin 2013d). Enfin, aux difficultés précédentes s'en ajoute une autre pour les CM construites en surcouche de Bitcoin (pièces colorées et métaprotooles) : « *le protocole de bas niveau sur lequel ils essaient de construire*

<sup>206</sup> Voir <https://www.blockchain.com/btc/address/36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2?filter=2#> [consultation au 02/04/2022].

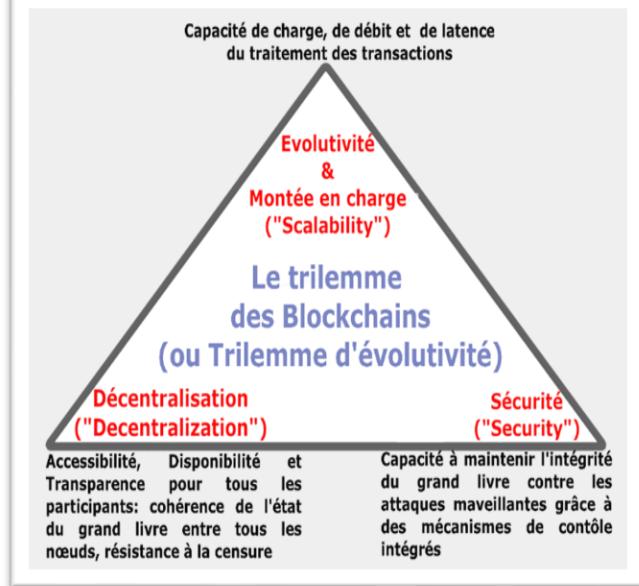
<sup>207</sup> Pour consulter des données graphiques, concernant le déroulement de la prévente, se reporter à Hasu, 2018, <https://medium.com/@hasufly/ethereum-presale-dynamics-revisited-c1b70ac38448> [consultation au 03/04/2022].

<sup>208</sup> Consultable ici : <https://etherscan.io/txs?block=0> [consultation au 03/04/2022].

<sup>209</sup> <https://devcon.org/devcon-0/details/> [consultation au 03/04/2022].

*leurs protocoles de haut niveau n'est tout simplement pas taillé pour cette tâche. »* (*Ibid.*). L'architecture de Bitcoin et ses arrangements sont conçus autour de certaines propriétés. La volonté d'ajouter des fonctionnalités se heurte tant à ce que permet la logique de ses codes qu'à la réticence de sa communauté de les faire évoluer radicalement au risque de les dénaturer. N'en déplaise à certains *bitcoiners*\*, aucune architecture de CM ne peut être « parfaite », et les protocoles de registre\* distribué renvoient toujours à une série d'arbitrages et de limitations qu'on ne peut miraculeusement résoudre : on travaille autour.

**Figure 6 : Une ontologie politique des CM en forme de triangle d'incompatibilité**



Source : Rolland Maël

les participants, et implique que de nombreux acteurs indépendants contribuent au fonctionnement du réseau\* et prennent des décisions collectivement, sans qu'une seule entité ou un groupe restreint ne puisse exercer un contrôle excessif, ce qui induit que la participation au protocole doit être facile et peu onéreuse. Enfin, l'évolutivité\* - ou la montée en charge - concerne la capacité d'un protocole de registre\* distribué à gérer un grand nombre et une grande variété de transactions\* de manière efficace.

C'est à l'ensemble de ces difficultés qu'Ethereum entend offrir des solutions. Dès l'introduction du WP\* d'Ethereum (cf. deuxième épigraphie de ce chapitre), les ambitions de Buterin sont claires et s'inscrivent dans une stratégie différente de celles entreprises jusqu'alors : créer un protocole de registre\* distribué « *qui se veut aussi généralisé que possible, permettant à quiconque de créer des applications spécialisées par-dessus, pour presque tous les usages imaginables.* » (Buterin 2014j). Dans cette optique, Buterin prend le contrepied des expériences passées. Avec Ethereum, il s'agit moins d'*« ajouter de la complexité et d'augmenter le nombre de "fonctionnalités" »* que d'en supprimer : « *le protocole ne "prend pas en charge" les transactions\* multi-signatures, les entrées et sorties multiples, les codes de hachage, les temps de verrouillage ou de nombreuses autres fonctionnalités que même Bitcoin fournit. Au lieu de cela, toute la complexité provient d'un langage d'assemblage tout puissant, Turing-complet, qui peut être utilisé pour construire littéralement n'importe quelle fonctionnalité qui est mathématiquement descriptible* » (Buterin 2013a). La conception d'Ethereum renvoie ainsi à une volonté de positionnement différent au sein de ce trilemme,

Cette dimension irréductible de compromis peut être représentée sous la forme du « Trilemme des blockchaînes » (ou d'évolutivité\*) proposé par Buterin (2021, cf. Figure 6 ci-contre), pour décrire le dilemme auquel tout protocole de registre\* distribué est confronté. À la manière des triangles d'incompatibilité connus en science économique, qui soulignent comment certains choix (ici sociotechniques), sont ontologiquement politiques, voilà que toute CM doit trouver une architecture équilibrée entre trois objectifs qui, bien que principaux, sont contradictoires : la sécurité, la décentralisation et la scalabilité (ou évolutivité\*). Pour ce qui est de la sécurité, il s'agit de garantir l'intégrité du registre\* contre les attaques et les tentatives de censure. La propriété de décentralisation fait référence à la répartition du pouvoir et du contrôle entre

relevant d'une stratégie de long terme. L'architecture de Bitcoin privilégierait la sécurité et la décentralisation au détriment de la scalabilité : son protocole et son langage script simples sont conçus pour être extrêmement sécurisés et ouverts au plus grand nombre. Cependant, cela limite également sa capacité à traiter un grand nombre de transactions\* rapidement. La conception d'Ethereum revendique de garantir une meilleur scalabilité avec une capacité de traitement transactionnelle plus grande et plus rapide que Bitcoin, sans pour autant sacrifier l'essentiel en termes de décentralisation et de sécurité (ce que les *bitcoiners*\* contestent, cf. Chap. III). En outre, il est envisagé dès l'origine que des évolutions protocolaires radicales et des sauts technologiques périlleux seront nécessaires. À plus longue échéance, différentes équipes travailleront à dépasser ce trilemme et à rendre chacune de ces propriétés complémentaires et non exclusives entre elles. En premier lieu, le WP\* envisage comme probable qu'Ethereum « passe à un modèle de proof-of-stake (preuve d'enjeu) pour des raisons de sécurité » : conçu comme « plus sûr, [ce mécanisme serait aussi] moins gourmand en énergie et mieux adapté à la mise en œuvre de nouvelles solutions de mise à l'échelle\* par rapport » à la PoW\* (Ethereum Foundation 2023a). Du côté de cette mise à l'échelle et à l'image du développement infrastructurel de Bitcoin, celui d'Ethereum le conduira à atteindre certaines limites de capacités, « ce qui a créé le besoin de "solutions de mise à l'échelle\*" » nombreuses, qui « font l'objet de recherches, de tests et de mises en œuvre et [...] adoptent des approches différentes pour atteindre des objectifs similaires » : « augmenter la vitesse des transactions\* (finalité plus rapide) et le débit\* des transactions\* (nombre élevé de transactions\* par seconde), sans sacrifier la décentralisation ou la sécurité » (Ethereum Foundation 2023c). Deux grands types se distinguent : les solutions dites *on chain*\* et celles *off chain*\*. Dans la première catégorie, on trouve le « sharding », par exemple : « depuis longtemps sur la feuille de route d'Ethereum », elle correspondrait à diviser la base de données en sous-ensembles (« shards ») que des sous-groupes de validateurs auraient à charge de vérifier, sans avoir à « assurer le suivi de l'ensemble d'Ethereum » ; dans la seconde, des solutions de type « Layer 2 » qui, comme *Lightning Network* pour Bitcoin, sont « mises en œuvre séparément de la couche 1 du réseau\* principal [et n'impliquent] aucune modification du protocole Ethereum existant » (*Ibid.*). Toutes n'étaient pas anticipées et leur mise en œuvre par mises à jour du protocole relèveront d'un sentier de développement infrastructurel aussi carnavalesque que singulier, que notre chapitre III permettra d'éclairer, dans la mesure où le cas d'étude du *Hard Fork*\* consécutif à l'attaque de « The DAO » a participé à le tracer. Développement qui s'inscrira dans une philosophie et des principes de conception distingués de ceux de Bitcoin et précisés dès le WP\*.

En premier lieu, Ethereum vise la simplicité, condition nécessaire à la réalisation du plein « potentiel de démocratisation sans précédent qu'apportent les » CM (Buterin 2013). Qu'importent les coûts induits (stockage de données, manque d'efficacité), Ethereum doit être accessible au plus grand nombre (même à « un programmeur moyen ») et toute optimisation ajoutant de la complexité sans apporter d'avantage substantiel ne devra pas être implémentée (*Ibid.*). L'universalité ensuite, puisqu'Ethereum, par son langage Turing-complet pensé par Buterin (2014h, 2014i), permet d'écrire tout type de contrat ou de transaction\* intelligente pouvant être défini(e) mathématiquement : cette modularité conduit à ce que chaque modification apportée ne remette pas en cause le fonctionnement d'autres éléments. L'agilité détonne face à l' « immutabilité » vantée de Bitcoin, puisque les arrangements sociotechniques d'Ethereum « ne sont pas gravés dans la pierre » : pas de défiance *a priori* envers des modifications radicales, si tant est qu'elles induisent des améliorations substantielles, leur implémentation sera discutée (cela, notre Chapitre III le confirmera). Enfin, un principe de non-discrimination et de résistance à la censure\*, qui assure que les évolutions d'Ethereum ne peuvent servir à restreindre ou empêcher des catégories spécifiques d'usages et d'usagers ou à s'opposer à des applications considérées par certains comme indésirables... Là encore, la communauté Bitcoin et ses rigidités sont visées.

## Ethereum contre Bitcoin ? Emprunts et différences de fonctionnement

Comme pour Bitcoin, présentons brièvement le fonctionnement d’Ethereum. Celui-ci partageant avec Bitcoin un certain nombre de principes de fonctionnement déjà traités, nous insisterons sur ses spécificités notables. Ethereum repose sur un protocole de registre\* distribué ouvert et open-source\*, constitué de nombreux composants clefs de Bitcoin (chiffrement asymétrique à la base des signatures numériques, fonction de *hash*\*, minage par PoW\*, etc.) structurant trois couches interdépendantes : une couche protocolaire, une couche réseau\* P2P et une couche de base de données publiques, contenant l’état du système. Là encore, les usagers peuvent interagir *on chain*\* via la production et la diffusion de transactions\* dont le traitement est effectué non pas par des autorités centrales ou des tiers formellement reconnus, mais par un ensemble indifférencié de nœuds\*. Comme pour Bitcoin, ces opérateurs du traitement des transactions\* vont recevoir, traiter et enregistrer (de manière distribuée) des transactions\*, dans un registre\* public (ou chaîne de blocs\*) répliqué et mis à jour par chacun des nœuds\*. Là encore, le protocole institue des incitations à la participation : en contrepartie de leur travail coûteux, les opérateurs du minage vont recevoir des récompenses sous forme d’UCN\* nouvellement émises (création monétaire d’ETH), auxquelles s’ajoutent les frais versés pour chaque transaction\* par son émetteur. On retrouve une cohérence assurée par un mécanisme de consensus entre les pairs sur une même copie de l’historique des transactions\* (l’état canonique du réseau\* à un instant t) fondé sur un algorithme de consensus\* de type PoW\* et des règles protocolaires. Là encore, l’infrastructure Ethereum doit garantir les propriétés tant valorisées de transparence, d’auditabilité, d’immutabilité et faisant de la résistance à la censure\*. Mais Ethereum et son ETH ont été conçus pour permettre aux utilisateurs d’y effectuer des transactions\* excédant le périmètre monétaire. Ils visent à offrir « *la couche fondamentale abstraite ultime : une blockchain intégrant un langage de programmation\* Turing-complet, permettant à quiconque de rédiger des smart contracts\** (contrats autonomes) *et des applications décentralisées où l’on peut créer ses propres règles concernant la propriété, les formats de transaction\* et les fonctions de transition d’état* » (Buterin 2013d). Ce qui est marketé comme un « ordinateur mondial distribué » doit permettre l’implémentation de tout type de *script à exécution programmatique\** imaginable, c’est-à-dire « *des applications plus complexes où des actifs numériques sont directement contrôlés par un bout de code exécutant des règles diverses (smart contracts\*)* ». Ethereum permettrait l’émission d’actifs numériques (tokens) de toutes sortes (monnaie ou titres financiers), des objets non fongibles (comme les noms de domaine, de l’art, etc.), « *ou même encore des organisations autonomes décentralisées basées sur la blockchain "decentralized autonomous organizations" ou DAOs.* » (*Ibid.*). Pour réaliser ses ambitions, Ethereum ne pouvait partir de l’architecture de Bitcoin sans la modifier radicalement. Il doit pouvoir traiter plus de transactions\*, dans un temps plus court (la durée d’un cycle de mise à jour du registre\* ne peut convenablement être de dix minutes) et, ce faisant, c’est une série d’arbitrages différents sur laquelle repose Ethereum<sup>210</sup>.

Bitcoin et son architecture ne couvrent qu’une fonction (la cession d’UTXO\*) suivant les propriétés de son langage de programmation\* Bitcoin Script (majoritairement utilisé par les premiers Altcoins\*). Critique d’un langage trop simple ne permettant qu’un choix limité de

---

<sup>210</sup> À la conception d’Ethereum, la taille de la blockchain\* Bitcoin était « *d’environ 15 Go, augmentant d’environ 1 Mo par heure. Si le réseau Bitcoin devait traiter les 2 000 transactions par seconde de Visa, elle augmenterait de 1 Mo toutes les trois secondes (1 Go par heure, 8 To par an). Ethereum [risque] de pâtir d’un modèle de croissance similaire, aggravé par le fait qu’il y aura de nombreuses applications sur la blockchain\* Ethereum et non uniquement une monnaie comme [...] Bitcoin* » (Buterin 2013d).

fonctions<sup>211</sup>, Ethereum a développé un langage de programmation\* propre : « *Solidity* » (Wood 2014b; Wood 2014a). Ce langage serait « *tout-puissant* », car « *Turing-complet* », créé sur mesure par Christian Reitwiessner et Gavin Wood, suivant différentes itérations et preuves de concepts (Buterin 2014g; Buterin 2014h; Buterin 2014i). Décomposé en une « *série d'octets où chaque octet représente une opération* », ce langage permet d’« *accéder à la valeur, à l'expéditeur et aux données du message reçu, ainsi qu'aux données des en-têtes de bloc* » (Buterin 2013d). Appelé aussi code « *Ethereum Virtual Machine* » ou « *code EVM* », ce langage transactionnel est décodé par l’environnement d’exécution incorporé dans le dispositif de traitement des transactions\* du protocole Ethereum sous forme de la machine virtuelle Ethereum (EVM), permettant de codifier une grande diversité de structures de règles et d’interactions au sein de la chaîne. L’EVM est au cœur du processus de vérification des transactions\* et de la production des nouveaux enregistrements. C'est elle qui traduit les instructions (OP\_CODE)<sup>212</sup> contenues dans une transaction\* ou un message reçu par les opérateurs de traitement des transactions\* afin de déterminer les transitions d'état ordonnées par les transactions\* et messages : elle agit comme « *une fonction qui accepte comme entrées un certain état et en sort un nouveau basé sur un ensemble arbitraire de règles.* » (Ichiba Hotchkiss 2020). Si la complexité de ce langage permet à Ethereum une grande plasticité, c'est un arbitrage qui se paye au prix de la sécurité : on renoue avec les critiques de Willet adressées aux recherches de Buterin sur Mastercoin/Omni, la complexité introduisant de nombreuses possibilités d’erreurs, de failles ou d’attaques. Ce langage Turing-Complet permet l’exécution d’une multitude de calculs et même des boucles, ce qui peut être utilisé pour saturer volontairement les nœuds\* et le réseau\* en leur demandant de traiter des opérations lourdes et infinies (problème connu en informatique sous le nom de « *halting problem* », Buterin 2013). Pour réguler ces risques, c'est encore l'établissement des frais de transaction\* qui est crucial.

Autre différence notable, dépendante de la première, Ethereum repose sur un système basé sur compte\* et non sur UTXO\* : les « *blocs Ethereum contiennent à la fois une copie de la liste des transactions\* et de l'état le plus récent* » (Buterin 2013d), qui « *est composé d'objets appelés "comptes", chaque compte ayant une adresse [...] et les transitions d'état [correspondent à] des transferts directs de valeur et d'information entre les comptes* ». Ceux-ci contiennent « *quatre champs : le nonce\*, un compteur utilisé pour s'assurer que chaque transaction\* ne peut être traitée qu'une seule fois ; le solde en Ether actuel du compte ; le code du contrat du compte, s'il est présent ; le storage ou mémoire de stockage du compte (vide par défaut)* » (*Ibid*, Polrot 2017) qui en déterminent deux grands types distincts (*Ibid*, Polrot 2017) :

---

<sup>211</sup> Pour Buterin (2013), le langage Bitcoin script est trop limité : d’abord, n’étant pas « *Turing-complet* », il ne contient qu’un ensemble limité d’opérateurs logiques, arithmétiques et cryptographiques. S’il couvre les types de calcul nécessaires à son fonctionnement, lui manque la capacité de traiter des « *boucles* » ; ensuite, il serait « *ignorant à la valeur* » du fait de script UTXO trop simple et binaire : c'est tout ou rien, ou l'on possède une UTXO en entier ou on ne la possède pas ; en outre, il manquerait « *d'état* », là encore du fait du caractère binaire des UTXO qui empêche les interactions plus complexes (différentes étapes ou créations de scripts d'un état interne plus nuancé) ; enfin, il fait face à l' « *ignorance de la blockchain\** », car les UTXO ignorent certaines données inscrites dans la chaîne de blocs\* (comme l’empreinte de l'enregistrement précédent, le “nonce\*” c'est-à-dire la numérotation des transactions passées), limitant encore la complexité des interactions possibles.

<sup>212</sup> L'exécution de code correspond à « *une boucle infinie* » consistant « *à effectuer l'opération présente au compteur de programme actuel [...] puis à incrémenter le compteur de programme jusqu'à la fin du code, une erreur ou la détection d'une instruction STOP ou RETURN. Les opérations ont accès à trois types d'espace pour stocker des données : la stack (pile), un conteneur premier-entré-premier-sorti auquel on peut ajouter et retirer des valeurs ; la memory (mémoire), un tableau d'octets extensible à l'infini ; le storage (stockage) à long terme du contrat, un tableau de clefs/valeurs. Contrairement à la pile et à la mémoire, qui sont réinitialisées après exécution, le stockage est conservé dans le temps* » (Buterin 2013d).

1. Les « Comptes à Propriétaire Externe » (ou *Externally Owned Account* ou EOA) sont contrôlés par des acteurs humains, interagissant via des transactions\* signées de leur clef privée. Ces transactions\* contiennent : « *le destinataire du message, une signature qui identifie l'envoyeur [...] , un champ VALUE – le montant en wei (subdivision d'éther) à transférer de l'envoyeur au destinataire, un champ de données optionnel, qui peut contenir le message envoyé à un contrat, une valeur GASLIMIT, représentant le nombre maximum d'étapes de calcul que la transaction\* est autorisée à réaliser, une valeur GASPRICE, représentant la commission que l'envoyeur est prêt à dépenser pour chaque unité de gaz. Une unité de gaz correspond à l'exécution d'une instruction atomique, c'est-à-dire une étape de calcul* » (Polrot 2017, nous y reviendrons).
2. Les « comptes de contrat » représentent des acteurs non humains dont les actions sont déterminées par leurs codes internes : activés par la réception d'un message/transaction\*, ils peuvent lire et écrire dans leur mémoire de stockage interne et envoyer d'autres messages, ou créer d'autres comptes de contrat (*Ibid*). Ils mobilisent l'instruction « call » pour leurs interactions *on chain\** leur permettant l'envoi de messages (équivalant à des transactions\*, à la différence qu'ils ne sont pas émis par un EOA) contenant : « *l'expéditeur du message (implicite) ; le destinataire du message ; la quantité d'Ether à transférer avec le message ; un champ optionnel de données ; une valeur GASLIMIT.* » (*Ibid*).

Contrairement à Bitcoin, où toutes les interactions dépendent ultimement d'acteurs humains, les comptes de contrat d'Ethereum sont un nouveau type d'acteurs non humains qui, contrôlés par leur code, agiront suivant un éventail d'actions programmées. Szabo (1996) nous représentait ces types de contrat comme des robots, « *des "agents autonomes" qui vivent à l'intérieur de l'environnement d'exécution Ethereum, en exécutant toujours un bout de code spécifique lorsqu'ils sont appelés par un message ou une transaction\*, et en conservant le contrôle direct de leur propre solde d'Ether et de leur propre collection de clefs/valeurs pour garder une trace des variables persistantes.* » (*Ibid*). Avec eux, le principe au cœur de Bitcoin et des philosophies cypherpunk/crypto-anarchiste visant à substituer les tiers de confiance par des codes informatiques connaît une extension de son domaine d'application. Là où Bitcoin régissait seulement les interactions de paiement/règlement induites par des interactions d'autres ordres, reléguées à un extérieur *off chain\**, Ethereum va plus loin : une multiplicité d'interactions se trouve régulées directement *on chain\** et peuvent trouver à être payées/regrées *on chain\** via l'UCN\* Ether.

Par ailleurs, le schéma général de fonctionnement séquentiel d'Ethereum reste assez similaire à celui entrevu pour Bitcoin (cf. schéma n°3). Partons de notre transaction\* simple, impliquant une cession d'1 ETH par A vers B, comme dans l'exemple décrit pour Bitcoin (pour des transactions\* plus complexes, impliquant des comptes de contrats, cf. Chap. III). Via un portefeuille, l'acteur A, qui dispose déjà de 3 Ethers (crédit existant sur son compte suivant les transitions d'état passées), génère et signe une TX qu'il diffuse au réseau\*. Le traitement de la transaction\* s'opère encore par les noeuds\* mineurs de manière séquentielle et sert à vérifier la validité de la TX et de la transition d'état qu'elle contient (Buterin 2013). Il s'agit (i) de vérifier que la transaction\* a le bon format, que la signature est valide et que le nonce\* de la TX correspond bien à celui du compte émetteur ; (ii) de calculer les frais de transaction\* (valeur GASLIMIT \* GASPRICE, où le prix du GAS est défini par A, nous y reviendrons), de déterminer l'adresse d'envoi en fonction de la signature, de déduire les frais du solde du compte émetteur et d'incrémenter le nonce\* de l'expéditeur ; (iii) de soustraire la quantité de GAS par octet correspondant aux frais à payer pour le poids de la TX ; (iv) de transférer la valeur du compte de A vers B ; enfin (v), soit la quantité de GAS allouée dans la TX est suffisante pour

les opérations qu'elle contient, le transfert est réalisé et le mineur reçoit les frais correspondant au GAS consommé par les opérations réalisées (les frais de GAS non consommés sont remboursés à l'expéditeur), soit, dans le cas contraire, le transfert échoue et est annulé l'ensemble des changements d'état à l'exception du paiement des frais qui sont crédités au compte du mineur. Toutes les transactions\* traitées par les mineurs sont intégrées dans un enregistrement candidat\* qui deviendra consensuellement canonique ou non. Un enregistrement Ethereum contient plus d'informations qu'un bloc Bitcoin ; s'y trouvent consignés : une copie de la liste des transactions\*, l'état le plus récent du registre, le numéro de bloc et la difficulté (Buterin 2013). Comme sur Bitcoin, après avoir traité les transactions\* de son choix, un mineur doit encore produire un enregistrement candidat\* valide, passant par la découverte d'une PoW\* respectant la cible de difficulté\* définie par le protocole. L'enregistrement candidat\* finalisé sera diffusé aux nœuds\* du réseau\* qui vérifieront sa conformité aux règles protocolaires canoniques. L'algorithme de vérification implique que chaque nœud\* mineur vérifie séquentiellement : que le nouvel enregistrement fait référence à un bloc précédent existant et valide ; que son horodatage\* est supérieur (et qu'il n'excède pas les 15 minutes dans l'avenir) ; que le numéro de bloc, la difficulté, la racine de transaction\*, la racine oncle et la limite de gaz sont valides ; que la preuve de travail\* du bloc est valide ; que les TX ne rencontrent pas d'erreur (relevant d'une erreur de l'application ou parce que les frais alloués en GAS ne suffisent pas à son traitement); enfin que la racine de l'arbre de Merkle\* de l'état de sortie est bien égale à la racine de l'état final fournie dans l'en-tête de bloc : si c'est le cas, le bloc est valide, sinon il est invalide (*Ibid*). L'état du système est stocké dans une structure en arbre, mais, contrairement à Bitcoin, Ethereum utilise un type d'arbre particulier appelé « arbre Patricia », qui correspond à une forme dérivée de l'arbre de Merkle\* (Buterin 2013). Cela lui permet d'intégrer toutes les informations d'état dans le dernier bloc et rend inutile le fait de stocker tout l'historique de la chaîne de blocs\*.

Après la présentation de ces quelques différences dans la continuité d'Ethereum avec Bitcoin, insistons en guise de conclusion sur des ruptures plus particulièrement significantes pour notre thèse, touchant au cœur politique de toute CM : les mécanismes de consensus et de monnayage.

### **Ethereum : des réformes du consensus et du monnayage en forme de révolution**

Pour son mécanisme de consensus, Ethereum utilise initialement une PoW\*. À la manière de Nakamoto, Buterin doit manier « la carotte et le bâton » à travers le design du jeu d'incitation au cœur de la viabilité, sécurité et soutenabilité de tout protocole de registre\* distribué public. Mais bien qu'Ethereum reprenne certains traits de cet arrangement politique essentiel, l'architecture et les paramètres initiaux choisis induisent des bouleversements radicaux : quantités, rythme et modalité de distribution des récompenses d'émission monétaire, frais et régulations transactionnelles, etc.

Si les concepteurs d'Ethereum conservent à l'origine la PoW\*, ils sont critiques à son encontre. Considérée comme énergivore, rigide et potentiellement insécure (du fait de la centralisation constatée sur le minage), il est prévu dès l'origine qu'Ethereum nécessite une autre architecture, basée cette fois-ci sur une PoS (dit Eth2.0), suivant que les avancées des équipes de développement garantiront à terme des coûts plus faibles et, par conséquent, une montée en charge plus facile, sécuritaire et décentralisée (Buterin 2013d; Buterin 2013e; Buterin 2014j; Buterin 2014d; Buterin 2014e; Buterin 2014f). Face à cette transition nécessaire et prenant acte des rigidités infrastructurelles d'une communauté Bitcoin peu enclive à modifier Bitcoin, les concepteurs d'Ethereum (qui en ont souffert) vont implémenter un mécanisme particulier en prenant le contrepied. Là où les *bitcoiners*\* revendiquent des codes résistant à

l'intervention humaine, les codes Ethereum intègrent un mécanisme qui empêche le *statu quo* et oblige au contraire cette intervention : la « *difficulty bomb* » (ou « *Ice Age* »)<sup>213</sup>. Introduite par une mise à jour protocolaire (« Frontier », du 7/09/2015), discutée dans le cadre formel d'un « *Ethereum Improvement Proposal* » (ou EIP, empruntant au BIP de Bitcoin, cf. Chap. III), ce mécanisme codé en dur doit rendre l'activité de minage et la production de PoW\* de plus en plus difficiles. Cette difficulté croissante doit inciter la communauté Ethereum (les mineurs sont visés) à ne pas retarder le passage à l'architecture en PoS (Buterin et Schoedon 2017; Proassetz 2018; Williams 2022). Cette bombe de difficulté incarne à elle seule une différence clef quant à l'approche opposée des communautés Bitcoin et Ethereum concernant les modifications protocolaires.

Néanmoins, au commencement (comme sur la période traitée par cette thèse), Ethereum opte pour un consensus de PoW\*, dont les choix architecturaux s'écartent de ceux de Bitcoin afin de mieux tenir compte de leurs limites. Puisque le développement de nouveaux ASICs est perçu comme un risque de centralisation, érigéant des barrières à l'entrée contrevenant au principe d'ouverture au plus grand nombre, le choix s'arrête sur un algorithme de PoW\* résistant à ce type de matériel. Puisqu'un ASIC est efficace en calcul mais non en mémoire, Ethereum a développé un algorithme de PoW\* *ad hoc*, « *EthHash* » construit sur l'algorithme Dagger-Hashimoto, nécessitant « *non seulement un grand nombre de calculs, mais aussi une grande quantité de mémoire* » (Buterin 2013e; Buterin 2014j). Pour autant, l'expérience montre que ce choix fut vain puisque des ASICs apparaîtront (on retrouve ici l'entreprise Bitmain), charriant avec eux des controverses communautaires quant à l'opportunité d'actions coercitives par modification protocolaire (O'Leary 2018). En outre, Ethereum conserve comme élément essentiel de son monnayage la mécanique d'une UCN\* émise protocolairement, dont le rôle est crucial pour garantir la sécurité du réseau\* et l'intégrité des informations endogènes\* qui y sont consignées. Comme précédemment, les coûts supportés par les opérateurs du traitement des transactions\* donnent droit à une contrepartie sous forme de récompenses de création monétaire et de prélèvement de frais de transaction\* afférents. On retrouve la concurrence entre opérateurs pour la découverte du prochain enregistrement candidat\* valide, et c'est toujours la puissance de calcul de l'opérateur relativement à la totalité de celle accumulée dans le réseau\* qui détermine sa chance d'être tiré au sort comme nœud\* leader. Mais une différence notable d'avec Bitcoin est que, au vu des usages envisagés, les cycles de mise à jour du registre\* doivent être plus courts et la cible de difficulté\* établit un cycle de 12 secondes en moyenne (Buterin 2014d), permettant de traiter 15 et non 7 transactions\* par seconde (Abdelatif Hafid 2022, p. 2). Comme tout n'est qu'arbitrage, à l'avantage de cette fréquence répondent des risques, soulignés par les *bitcoiners*\* : les « *blockchains*\* [avec des temps de confirmation\* plus rapides] sacrifient la décentralisation pour y parvenir. » (Andreas Antonopoulos Bitcoin Q&A 2018). Pour sûr, « *les blockchains*\* avec des temps de confirmation\* rapides souffrent actuellement d'une faible sécurité en raison d'un taux élevé de blocs orphelins [induisant le risque qu']une coopérative de minage ayant un assez large pourcentage de la puissance de calcul du réseau\* [obtienne] de facto un contrôle sur le processus de minage » (Buterin 2013d). Pour les contenir, Ethereum a opté pour une variante du protocole GHOST (« *Greedy Heaviest Observed*

---

<sup>213</sup> Il s'agit « *d'un système d'ajustement de la difficulté conçu pour augmenter la difficulté d'extraction sur le réseau tous les 100 000 blocs, rendant ainsi impossible pour les mineurs de suivre le niveau de difficulté croissant. Cela aurait pour effet de geler le réseau au fil du temps, d'où le nom d'"âge de glace".* » (Williams 2022)

*Subtree »)<sup>214</sup>* qui conserve la règle d'une convergence automatique sur l'enregistrement le plus lourd en calcul : là encore, « *quiconque utilise le réseau\* principal d'Ethereum a, au sens propre ou figuré, "adhéré" à l'histoire d'un état particulier, à savoir celui qui a effectué le plus de travail informatique, comme le détermine le protocole GHOST [...] d'Ethereum* » (Ichiba Hotchkiss 2020, Buterin 2014d). Mais la mesure de la « canonicité » de cet état est modifiée en profondeur : là où Bitcoin exclut les blocs orphelins, Ethereum les y inclut. Parent, ancêtres et blocs descendants (jusqu'à 7 générations, dénommés « oncles » puisqu'ils ne sont plus orphelins, Wood 2014b) participent de la longueur de la chaîne canonique<sup>215</sup>. Ce statut particulier octroyé aux blocs oncles/orphelins bouleverse le monnayage d'Ethereum qui, dès lors, distribue plusieurs types de récompenses d'émission monétaire. Suivant qu'elle offrirait une moindre sécurité, la règle du « *winner take all* » de Bitcoin - qui voit les producteurs honnêtes de blocs orphelins n'avoir droit à aucune contrepartie alors qu'ils ont supporté des coûts - est renversée (ce que les *bitcoiners\** eux-mêmes ont fait avec la constitution de coopérative de minage). Puisque c'est du travail redondant de chacun que dépend la sécurité de tous, la politique monétaire d'Ethereum profite à un plus grand nombre de participants et même la production de bloc orphelin est rétribuée pour le travail réalisé. À l'origine, l'enregistrement canonique\* d'un nœud\* leader donne droit, comme sur Bitcoin, à une récompense de base (5 ETH/bloc au lancement d'Ethereum, Buterin 2013c), à laquelle s'ajoutent les frais de transaction\* consentis par les usagers. À cette récompense de base s'en ajoutent deux autres, liées aux blocs orphelins : une « *récompense "Uncles"*, attribuée au mineur qui a créé un bloc "Oncle" inclus dans un bloc canonique » et une « *récompense pour l'inclusion d'un oncle* » ajoutée à la récompense de base attribuée à l'opérateur qui l'inclut dans son bloc canonique (Hunt 2019). La récompense de base sert de référence aux autres types de récompenses, dont le montant dérive (c'est une fraction de celle-ci, (Buterin 2016a)<sup>216</sup>.

Ethereum, via cette architecture, conserve un monnayage programmatique, mais les choix de conception, d'une grande complexité, suivent des logiques opposées. Déjà, nous l'avons vu, le minage n'est pas le canal exclusif d'émission et de distribution des UCN\* puisque

<sup>214</sup> Le protocole GHOST de Sompolinsky et Zohar (2013) doit permettre de palier les effets négatifs sur la sécurité de Bitcoin qu'impliquerait une diminution du temps entre deux blocs : un temps court induit un risque accru de blocs orphelins, incitant à la concentration du minage (Wood 2014b). Ces problèmes sont résolus « *en incluant les blocs dépréciés dans le calcul de la longueur de la chaîne ; c'est-à-dire non seulement le parent et les ancêtres suivant d'un bloc, mais aussi les descendants dépréciés de l'ancêtre du bloc (en jargon Ethereum, les « uncles » ou oncles) [et en allant] au-delà du protocole décrit par Sompolinsky et Zohar* » puisque Ethereum récompense les « *blocs dépréciés* » (Buterin 2013d).

<sup>215</sup> À l'origine, la chaîne la plus longue est déterminée par la difficulté totale contenue dans l'en-tête du bloc principal, c'est « *simplement à la somme des valeurs de difficulté des blocs sans compter explicitement les oncles* » (Johnson 2017). Cela a changé avec « *l'EIP 100 [de] 2017 [...] qui modifie l'algorithme de calcul de la difficulté pour inclure les oncles.* » (dufferZafar 2019). L'inclusion des blocs oncles concerne uniquement leurs en-têtes et non les transactions qu'ils contiennent. Ces transactions ne sont pas considérées comme valides sur la chaîne principale et ne participent pas à l'état final, même si elles sont techniquement valides. Elles peuvent déjà être incluses dans un bloc parent ou le seront dans un bloc principal futur. Ainsi, les transactions dupliquées dans les blocs oncles ne le sont pas sur la chaîne principale et seul l'en-tête du bloc canonique inclut les transactions validées dans l'état final de la blockchain\*.

<sup>216</sup> Un « *bloc orphelin reçoit 87,5% de sa récompense de base, et le neveu qui inclut le bloc orphelin reçoit les 12,5% restants. Les frais de transaction, en revanche, ne sont pas attribués aux oncles* ». Le statut d'oncle relève des propriétés suivantes : ils « *ne peuvent être inclus que jusqu'à 7 générations* », doivent avoir « *un en-tête de bloc valide, mais il n'est pas nécessaire qu'il s'agisse d'un bloc déjà vérifié ou même valide* » ; ils doivent « *être différents de tous les oncles inclus dans les blocs précédents et de tous les autres oncles inclus dans le même bloc (non-double inclusion)* », ainsi « *pour chaque oncle U dans le bloc B, le mineur de B obtient 3,125% supplémentaires ajoutés à sa récompense coinbase et le mineur de U obtient 93,75% d'une récompense coinbase standard.* » (Ethhub; Buterin 2016). Ces parts (retenues dans notre graphique n°8.2) peuvent avoir évolué, car nous avons rencontré des informations contradictoires. Cette recension sert d'illustration de la mécanique complexe des récompenses.

l'enregistrement de genèse\* du 20 juillet 2015 a mis en circulation les ETH « préminés » de l'« *Ether Genesis Sale* ». Au lancement d'Ethereum, l'offre initiale n'est pas nulle, le premier enregistrement mettant en circulation les 72 000 000 d'ETH de l'ICO. Autre différence radicale quant à la création monétaire, les concepteurs d'Ethereum refusent, comme pour *Peercoin*, le concept d'offre monétaire limitée et finie. Si le trend d'émission explosif mais décroissant est conservé pour sécuriser rapidement le réseau\*, l'émission d'Ether sera illimitée et infinie. L'« *approvisionnement plafonné de Bitcoin* » est remplacé par « *un approvisionnement linéaire permanent* » : le plafond n'est pas absolu mais relatif, puisque l'émission est limitée en proportion des Ethers émis lors de l'ICO. Ce faisant, « *26% du montant total vendu seront chaque année alloué[s] aux mineurs, sans limite dans le temps.* » (Buterin 2013d). Ce choix est « *destiné à amortir certains des effets spéculatifs et d'inégalité de richesse des monnaies existantes* » (Buterin 2014j) et à éviter les risques perçus du tarissement du financement de la sécurité de Bitcoin. D'ailleurs, si les récompenses sont « *d'un montant fixe chaque année, le taux de croissance de la base monétaire (inflation monétaire) n'est pas constant [et] diminue chaque année, ce qui [ferait] de l'ETH une monnaie désinflationniste* » (Lubin 2014) : en effet, « *le "taux de croissance de l'approvisionnement" en pourcentage [de la masse monétaire en circulation] tend toujours vers zéro au fil du temps.* » (Buterin 2013d). En outre, le monnayage d'Ethereum refuse une immuabilité conçue comme risquée, car potentiellement mal paramétrée. S'il était question à l'origine d'avoir un mécanisme de diminution des récompenses de type *Halving à la Bitcoin*, les concepteurs préviennent qu'ils ne font « *absolument aucune promesse en ce sens, si ce n'est que le taux d'émission ne dépasse pas [la limite relative des] 26,00% par an de la quantité d'Ether vendue dans la vente Genesis.* » (Buterin 2014c). Dans le cadre de cette promesse, rien n'est fixé une fois pour toutes. La communauté d'Ethereum pourra plus tard « *adopter d'autres stratégies consensuelles, telles que la preuve hybride de l'enjeu, afin que les futurs patchs puissent réduire le taux d'émission à un niveau inférieur* » (*Ibid.*). Les concepteurs ont bien conscience que la complexité du système à mettre en œuvre nécessite des tâtonnements. Pour preuve, le taux de production de blocs oncles est difficile à anticiper et, suivant le retard de livraison de l'architecture d'Eth 2.0, la bombe de difficulté tarde le nombre d'enregistrements produit. Ces phénomènes conjugués induisent des écarts entre l'émission monétaire d'ETH effective et celle anticipée à l'origine (Annexe n°III.2), et que la complexité précédente rend plus difficile à évaluer *on chain\** qu'avec Bitcoin. Des modifications protocolaires d'ampleur seront implémentées pour s'y adapter : la bombe de difficulté est repoussée plusieurs fois, et pour « *maintenir la stabilité du système, une réduction de la récompense des blocs* » est décidée afin de compenser « *le retard de l'ère glaciaire [et de laisser] le système dans le même état général qu'auparavant* » (Buterin et Schoedon 2017). Soumise à des évolutions proposée sous forme d'*Ethereum Improvement Proposal*, la politique monétaire connaît donc des réductions de récompenses successives (de 5 à 3 ETH/bloc avec l'EIP 649 et de 3 à 2 avec l'EIP 1234, *Ibid.*, Ethhub NC).

Si le « *réseau\* Ethereum inclut sa propre monnaie, l'éther* », c'est aussi pour « *fournir une couche de liquidité primaire pour permettre un échange efficace entre les différents types d'actifs numériques et, plus important encore, pour fournir un mécanisme pour le paiement des frais de transaction\** ». » (Buterin 2013d). Suivant l'exemple de Bitcoin, l'éther est conçu comme le « *carburant* » (« *crypto-fuel* », *Ibid.*) nécessaire à l'usage d'Ethereum. La fixation des coûts nominaux d'usage (cf. coûts de transaction\*), comme leur règlement, passe exclusivement par cette UCN\*. Reste que l'analyse des mécanismes d'imputation à l'œuvre révèle des logiques économiques très différentes. Comprendons que « *le registre\* d'une cryptomonnaie telle que Bitcoin peut être considéré comme un système de transition d'état où il y a un "état" consistant en l'état de la propriété de tous les bitcoins existants et une "fonction de transition d'état" qui prend un état et une transaction\*, et en fait résulter un nouvel état.* » (*Ibid.*). Que ce soit pour Bitcoin, pour Ethereum, ou toute autre CM, assurer la conservation de l'état, ainsi que ses

transitions (par traitement des transactions\* et production d'enregistrement<sup>217</sup>), impose la mise en œuvre de ressources : l'un nécessite de la mémoire de stockage et l'autre de la puissance de calcul. Et la structure des incitations fixées par le protocole se doit de le rendre soutenable, tout en équilibrant une offre de capacité de traitement et de stockage des transactions\* – offerte par les « mineurs » - à une demande, opérée par les utilisateurs. Pour autant, souvenons-nous que, sur Bitcoin, la tarification des frais de transactions\* renvoie seulement à une offre d'espace de stockage disponible puisqu'elle est tout entière basée sur la taille octets des transactions\* (plus le nombre d'UTXO\* en entrée est grand, plus la transaction\* est lourde et chère). C'est pour cette raison qu'il a fallu aux *bitcoiners*\* ajouter des régulations transactionnelles afin d'éviter des « abus », qui, pour Buterin, n'en sont que du fait d'une mauvaise structuration des coûts et de leurs contreparties : dans son « *monde idéal* », où les frais seraient « *soigneusement structurés pour correspondre au coût réel qu'une transaction\* donnée impose au réseau\** », « *le concept d'« "abus" n'existerait même pas* » (Buterin cité par BitMEXResearch 2022). À partir de cette volonté de tarification soigneusement structurée, la détermination des frais de transaction\* sur Ethereum prend en compte non seulement les coûts mémoires, mais aussi ceux liés à la computation des opcodes réalisés par les mineurs. Cela ne relève plus d'une variable unique (la valeur en octet de la transaction\*), mais passe par l'établissement d'une unité de mesure *ad hoc* - le « *GAS* » - auxquelles s'attachent deux variables, les valeurs GASLIMIT (ou STARTGAS) et GASPRICE précédentes, qu'il nous revient d'expliquer.

Ce GAS représente l'*« unité fondamentale de calcul »* d'Ethereum. Du côté de l'offre, il sert à fixer une quantité d'enregistrements disponibles à chaque cycle de mise à jour du registre. Là où, sur Bitcoin, cette offre est limitée en matière de mémoire, via « *une limite [...] rigide sur les blocs* » (cf. 1 Mo), Ethereum « *fixe ses limites de blocs avec [ce] GAS* » : initialement, c'était « *8 000 000 unités de gas par bloc* » (Majuri 2019) qui étaient disponibles par cycle. Mais, comme pour Bitcoin, le développement infrastructurel d'Ethereum conduira à une augmentation de son usage. Face à une « *forte demande [...], ces blocs fonctionnaient à pleine capacité* », « *ce qui entraînait une mauvaise expérience* » suivant l'augmentation des délais de traitement et des frais de transaction\* afférents (Ethereum Foundation 2023b). À la faveur d'une EIP (EIP 1559, PhilH 2021), le code protocolaire canonique fut modifié afin de rendre l'offre d'enregistrement en partie élastique à la demande. Comme pour se distinguer un peu plus de Bitcoin, voilà qu'Ethereum établit des « *blocs de taille variable* » : « *chaque bloc a une taille cible de 15 millions de gaz, mais la taille des blocs augmente ou diminue en fonction de la demande du réseau\*, jusqu'à la limite de 30 millions de gaz (deux fois la taille cible du bloc)* » (Ethereum Foundation 2023b). À cette offre de GAS par bloc répond une demande déterminée par les instructions EVM contenues dans les transactions\* à traiter, elles-mêmes mesurées en GAS : chaque instruction du langage *Solidity* d'Ethereum se voit définir au niveau protocolaire un coût en cette unité<sup>218</sup> (devant couvrir les coûts mémoires et computationnels afférents) : « *généralement, une étape de calcul coûte 1 gaz, mais certaines opérations coûtent davantage*

<sup>217</sup> Pour Bitcoin, « *chaque transaction dans le bloc doit fournir une transition d'état valide vers un nouvel état à partir de ce qui était l'état canonique avant que la transaction n'ait été exécutée. On note que l'état n'est pas encodé dans le bloc de quelque façon que ce soit ; ce n'est qu'une abstraction dont le noeud\* qui valide doit se souvenir et il ne peut être calculé (en toute sécurité) pour tout bloc qu'en partant de l'état d'origine et en y appliquant séquentiellement chaque transaction dans chaque bloc.* » De la même manière, « *dans Ethereum, l'état est composé d'objets appelés "comptes", chaque compte ayant une adresse sur 20 octets et les transitions d'état [sont] des transferts directs de valeur et d'information entre les comptes* » relevant de message et transaction (Buterin 2013d).

<sup>218</sup> Les différentes instructions / *Op\_Code* et leurs coûts en GAS sont listés dans l'appendix G du Yellow Paper (Wood, p. 25). Par exemple, l'instruction la plus simple, l'envoi d'ETH, s'est vu attribuer le coût de 21 000 unités de Gas, mais cette nomenclature évolue au gré des besoins, des instructions peuvent être ajoutées ou supprimées et les coûts en GAS de chacune peuvent aussi être implémentés.

*car elles sont plus coûteuses en calcul ou elles augmentent la quantité de données devant être stockées dans l'état.* » (*Ibid.*). Ainsi, cette unité *ad hoc* sert à évaluer / contraindre les besoins transactionnels, par fixation de frais de transaction\* selon la relation suivante : « *les frais de transaction\* [=] STARTGAS\* GASPRICE* », où la valeur *STARTGAS* (ou *GASLIMIT*) correspond au « *nombre maximum d'étapes de calcul autorisé pour l'exécution de la transaction\** » et la valeur *GASPRICE* représente le prix par unité de GAS « *que l'expéditeur paie par étape de calcul* » (*Ibid.*). Ainsi, pour l'usager, le coût d'une transaction\* est fonction de la quantité d'unité de gaz totale qu'il demande d'exécuter au sein de la transaction\* (le « *GASLIMIT* », fonction des *OP\_CODE* mobilisés). À cette quantité de GAS est appliqué un prix par unité de gaz (le « *GASPRICE* », exprimé en *Wei*, l'unité la plus petite de l'Ether, comme le *Satoshi* du bitcoin ; cf. Annexe n°). Et comme sur Bitcoin, c'est ce prix qu'il pourra spécifier suivant ses préférences en termes de temps de traitement : puisque la quantité d'opérations contenue dans un enregistrement est relativement limitée, les transactions\* sont en concurrence entre elles et ce prix du GAS vient à les discriminer. Ces variables, au cœur de l'activité de traitement des transactions\* par minage, sont cruciales au « *modèle anti-déni de service d'Ethereum* », puisqu'elles limitent et régulent « *le nombre d'étapes de calcul dans l'exécution du code* » des transactions\*, afin « *d'éviter les boucles infinies accidentnelles ou hostiles, ou [tout] autr[e] gaspillag[e] de calcul* » (Buterin 2013d). Cette unité abstraite qu'est le GAS, en plus de permettre cette imputation des coûts computationnels (absente de Bitcoin), permet celle des coûts mémoires, suivant l'établissement au niveau protocolaire d'une « *taxe de 5 gaz pour chaque octet de données de transaction\** » à consigner (*Ibid.*). Avec ce « *système de frais [il] est possible d'exiger d'un attaquant qu'il paie proportionnellement chaque ressource qu'il consomme, ceci comprenant le calcul, la bande passante et le stockage ; [finalement] toute transaction\* qui conduit le réseau\* à consommer une plus grande quantité de l'une de ces ressources doit payer des frais [...] proportionnels à cette augmentation.* »

Ces frais à payer pour interagir au sein d'Ethereum servent plusieurs objectifs. Comme sur Bitcoin, ils s'ajoutent aux récompenses d'émission monétaire afin d'inciter les mineurs à participer et dissuadent les attaques de spam et DOS\* que pourraient causer des transactions\* malignes, excessivement coûteuses à cause de la quantité de calcul qu'elles impliqueraient. Et comme sur Bitcoin, des attaques DOS adviendront malgré eux, donnant lieu à des débats et actions communautaires visant à changer la nomenclature des coûts afférents des instructions, au risque de remettre en cause la viabilité d'usages eux légitimes, codés suivant la nomenclature précédente. Parallèlement, du fait des usages applicatifs d'Ethereum, ces frais doivent inciter tout développeur à optimiser les codes qu'il y déploie, poussant à ce que la base de données ne soit pas surchargée d'applications lourdes et non optimisées qui induiraient des surcoûts de stockage et de traitement. En outre, les frais de transaction\* comme mécanisme de discrimination de transactions\* publiques non confirmées se sont traduits sur Ethereum par un bouleversement d'ampleur : la « valeur maximale extractible » (ou « MEV » pour « Maximum Extractable Value », en langage indigène). Les « mineurs » (précisément et comme sur Bitcoin, les *pools de minage* ici et non les *Hasheurs*) conservent la discréption sur l'ordonnancement des transactions\* et choisissent d'inclure les transactions\* pour eux les plus rentables à quantité d'instruction donnée. Ce pouvoir structurel qui leur échoit se matérialise plus clairement sur Ethereum sous forme d'opportunités pour les mineurs d'extraire de la valeur en réorganisant l'ordre d'inclusion des transactions\* dans un bloc (c'est-à-dire d'exploiter la séquence d'exécution des transactions\*, par exemple en réalisant du « *Front running* » de transactions\* en attente, Robinson 2020).

Partir d’Ethereum et de la normativité propre contenue dans ses choix architecturaux nous permet de comprendre, au-delà de sa dimension politique à lui, suivant les cristallisations sociotechniques incarnées dans ses composants et dispositifs, celles des autres CM, dont Bitcoin, contre lesquelles il se positionne.

## I.4 CONCLUSION DU CHAPITRE I

Ce premier chapitre visait à présenter l’émergence historique des CM et de nos deux objets d’étude, d’abord au travers du cas du pionnier Bitcoin, ensuite de certains Altcoins\*, et enfin d’Ethereum. Cette visée se doublait de questions théoriques et méthodologiques relatives à la manière de décrire et d’analyser pleinement ce phénomène. Conçues dans une approche empreinte de STS comme des infrastructures sociotechniques, les CM ont été présentées dans ce chapitre de façon à en restituer toute l’épaisseur socio-historique et relationnelle. Cette démarche a ainsi pris le contre-pied d’approches concurrentes, mobilisant un technologisme selon nous réifiant, partiel et partial, qui réduit les CM à de simples protocoles conçus comme autonomes, et à des propriétés de « nature » supposément « technique » (cryptographie\*, distributions P2P, etc.). C’est en effet ce technologisme qui conduit les analyses les plus fréquentes, qu’elles émanent de *coiners*\* ou de leurs contemporains, à n’insister que sur les seules dimensions protocolaires et *on chain*, et à présenter les CM – positivement pour les premiers, négativement pour les seconds – comme des systèmes monétaires universellement accessibles, non régulés, « apolitiques » et « neutres ». C’est encore ce technologisme qui sert à occulter les questions entourant leur gouvernance, puisque cette dernière serait censée se limiter au cadre même de leurs protocoles, dont les codes logiciels seraient accessibles, transparents et immutables. Ce chapitre s’est inscrit en faux contre ces approches réductionnistes, démontrant que les CM ne sont pas indépendantes de rapports sociaux (matériel et idéal). À l’aune de notre appareillage théorique et de nos matériaux empiriques, point de « neutralité » : ni intrinsèque, leur conception n’étant pas exempte de normativité et d’arbitrage ; ni davantage extrinsèque, les protocoles de CM devant s’arrimer à d’autres systèmes, au premier chef desquels le système monétaire et financier, pour être usés comme tels. Or si leurs règles protocolaires sont indépendantes des réglementations nationales, il n’en est pas de même pour l’usager de CM. Grâce à notre approche en termes d’infrastructure socio-technique, la nature bigarrée du phénomène CM est apparue pleinement.

Partant du Bitcoin de Nakamoto, nous avons démontré de quelle façon chacune des décisions de conception – en particulier l’émission monétaire liée au consensus de PoW\* – renvoyait irréductiblement à des problématiques hybrides et négociées, alliant des considérations tout autant techniques que philosophiques, économiques, sociales et politiques. Ces compromis et choix se sont cristallisés dans un type d’architecture et des règles transactionnelles. Les CM participent d’agencements qui articulent des actions, agissent et font agir (Muniesa & al, 2006). Elles participent à soutenir des partitions du monde : leurs codes attribuent des rôles à certains acteurs (humains ou non) et en relèguent d’autres au second plan ; ils rendent possibles certains modes de relations et en interdisent d’autres (Akrich 1989, 2010). En outre, par-delà les philosophies politiques, les expériences passées et les contraintes pratiques qui ont présidé aux choix de conception de Nakamoto, nous avons montré comment Bitcoin a pu devenir monnaie grâce à sa confrontation avec des usagers, au gré d’un développement infrastructurel carnavalesque et par étapes. Par leurs improvisations très politiques et la nécessité de constituer des passerelles\*, vecteurs d’interopérabilité (d’où l’existence d’inversion et de détournement, cf. réintermédiation diverse), ces usagers ont

travaillé chacun dans leur coin à faire de Bitcoin une CM. À ce titre, loin du scénario et du casting originels, Bitcoin apparaît comme co-produit par une multiplicité d'acteurs et se présente comme un ensemble composite de dispositifs excédant largement son seul protocole. Les usagers agissent de facto en co-monnayeurs, renégociant sans cesse les caractéristiques et les propriétés de Bitcoin, tandis que des intérêts hétérogènes traversent une communauté évolutive. Enfin, à la faveur de notre présentation d'Ethereum, nous en sommes venu à un décentrement de Bitcoin vers les Altcoins\*. Nous avons retracé l'émergence des premières Altcoins\*, précisant leurs emprunts mais surtout leurs différences avec Bitcoin. Leurs renégociations préparaient celles d'Ethereum qui s'inscrit dans une filiation critique de Bitcoin. La lumière jetée sur la normativité propre d'Ethereum a permis de redoubler les conclusions préalables fondées sur l'analyse de Bitcoin et de certains Altcoins\*.

Ainsi, avec ce chapitre, nous avons opéré un détricotage systématique des deux prémisses du syllogisme libéral-techniciste présenté en introduction qui voudrait que, (i) puisque la technique est neutre, que (ii) les CM sont des monnaies purement techniques, alors (iii) les CM seraient par là-même des monnaies neutres, voire (iv) de « meilleures » monnaies. La suite de la thèse va chercher à dépasser le creux (la technique n'est pas neutre) et tenter de qualifier le plein, c'est-à-dire ce qui est spécifique dans les CM et qui n'est pas leur absence de gouvernance et leur apolitisme. La spécificité politique des CM doit selon nous être cherchée dans les formes particulières de leur gouvernance. Si ces objets monétaires non identifiés nous apparaissent comme radicalement novateurs dans le champ monétaire, ce n'est pas parce qu'ils arrivent à évacuer le politique, la délibération et les conflits du champ de la monnaie, mais parce qu'ils les recomposent d'une manière inédite. Mais avant de nous lancer dans ce travail de caractérisation et de description de leur gouvernance, nous devons nous attacher à démontrer la nature monétaire des CM, car sans elle, nos conclusions perdront en capacité à contribuer aux travaux théoriques sur la monnaie. C'est l'objet du deuxième chapitre de la thèse.

## CHAPITRE II - DÉPASSER LA CONTROVERSE DU STATUT MONÉTAIRE DES CM PAR UN INSTITUTIONNALISME INTÉRESSÉ AUX USAGES

« Le bitcoin peut être mieux compris comme [...] une monnaie protégée contre l'inflation [...] sans dépendre de tiers de confiance. [...] Bitcoin automatise les fonctions d'une banque centrale moderne et les rend prévisibles et pratiquement immuables en les programmant dans un code décentralisé entre des milliers de membres du réseau\*, dont aucun ne peut modifier le code sans le consentement des autres. [...] Si le bitcoin est une nouvelle invention de l'ère numérique, les problèmes qu'il prétend résoudre, à savoir la fourniture d'une forme d'argent qui est sous le contrôle de son propriétaire et qui est susceptible de conserver sa valeur à long terme - sont aussi vieux que la société humaine elle-même. [...] La résilience du bitcoin ne s'est pas limitée à repousser avec succès les attaques ; il a également résisté avec brio à toute tentative de le modifier ou d'en altérer les caractéristiques. [...], le mode de fonctionnement de ses règles de consensus le rend très résistant à l'altération par des individus [,] personne ne contrôle le bitcoin et [...] la seule option disponible est de l'utiliser tel quel ou de ne pas l'utiliser. »

« The Bitcoin Standard » (2018), Saifedean Ammous, p. 14 et p.202

« Il n'y a aucune raison, en principe, pour que les règlements financiers ne soient pas effectués par le secteur privé sans [...] l'intermédiaire de la banque centrale. [Cela] nécessiterait une puissance de calcul bien plus importante que celle dont nous disposons actuellement. Mais il n'y a pas d'obstacle conceptuel à l'idée que deux individus engagés dans une transaction\* puissent se régler par un transfert de richesse d'un compte électronique à un autre en temps réel. Des algorithmes convenus à l'avance détermineraient quels actifs financiers ont été vendus [...]. Et le fournisseur de ce bien ou de ce service saurait que les fonds entrants seront affectés à la combinaison appropriée d'actifs, conformément à un autre algorithme préétabli. Les actifs éligibles seraient tous les actifs financiers pour lesquels il existe des prix de compensation du marché en temps réel. [...] Se pourrait-il que 1999 marque l'apogée du pouvoir des banques centrales ? Je pense que si les banques centrales veulent conserver leur position centrale [...] elles doivent relever les défis intellectuels et technologiques qui les attendent. »

“Challenges for Monetary Policy: New and Old” , Mervyn King, 27 août 1999, p.48 et p.14

« La révolution des technologies de l'information [...] a donné lieu à des spéculations passionnées [...] La promesse de la « nouvelle économie » a excité l'imagination des jeunes [et] parmi les institutions de la « vieille économie » qui se demandent si elles ne seront pas bientôt rendues obsolètes, on peut citer les banques centrales, qui commencent à se demander si leur capacité à stabiliser la valeur de leur monnaie nationale ne risque pas d'être érodée par le développement des moyens de paiement électroniques. [...] La seule véritable question qui se pose à propos de cet avenir est celle de l'importance des politiques monétaires des banques centrales [et celles] qui font preuve à la fois de l'engagement et des compétences nécessaires pour maintenir une valeur stable pour les monnaies de leurs pays devraient continuer à jouer un rôle important dans le siècle à venir. »

« Monetary Policy in a World Without Money », Michael Woodford 2000, p. 1 et p.42

Imaginer une monnaie « idéale », fondée sur un système de paiement interindividuel et décentralisé, sans banque, ni banque centrale (BC), ni aucun intermédiaire est possible. Cependant, pour détacher complètement la monnaie de tout collectif institué, il faut supposer l'émergence d'innovations technologiques se substituant aux autorités centrales et collectives qui ont traditionnellement la charge d'administrer la monnaie. Une telle monnaie n'est concevable que dans des marchés optimaux, sans asymétrie d'information, ni incertitude. Ces idées, bien que radicales, ne sont pas exclusives à Nakamoto et aux *coiners\** libertariens. Elles sont partagées par les professionnels de l'argent : des lauréats de prix « Nobel » d'économie et

des praticiens ont jugé l'idée désirable<sup>219</sup>. King (1999, cf. exergue du chapitre), gouverneur de la *Bank Of England*, à l'occasion de l'apparition des monnaies électroniques, ne voyait aucun problème à l'existence d'un système de règlement purement privé. Les *coiners\**, *bitcoincers\** en tête, disent aller encore plus loin. Ces représentations monétaires décrivant « *un monde sans monnaie* » (Woodford 2000, dans l'exergue), où tout n'est que titres, restent controversées. Simmel (2009, p.166-167) souligne qu'une telle monnaie idéale est inatteignable du fait de l'incertitude et des « *imperfections de la technique économique* » que la monnaie supplée socialement : fiduciarité et liquidité monétaire sont indétachables d'un collectif institué les garantissant<sup>220</sup>. La théorie économique n'ayant pas confirmé ces suppositions, la pratique pourrait donner des réponses. Face à ce qui apparaît tantôt comme un « *rêve* », tantôt comme un « *cauchemar* » monétaire « *libertarien* » (De Filippi 2013; Karlstrøm 2014), les réponses pourraient surprendre.

Ce chapitre participe à la controverse sur le statut monétaire des CM. Nous interrogerons deux des propositions du syllogisme « libéral-techniciste » au cœur des ambitions monétaires des *coiners\**. Ce syllogisme postule, rappelons-le, que puisque (i) la technique est autonome et neutre vis-à-vis du monde social et que (ii) les CM sont des monnaies purement techniques ; alors (iii) elles sont immunisées de la gouvernance humaine et de ses intérêts socio-politiques, ce qui en fait (iv) de « meilleures » monnaies que les monnaies nationales. L'invalidation des deux premières prémisses effectuée au chapitre précédent affaiblit les suivantes, mais celles-ci, s'inscrivant dans le champ de la science économique, nécessitent des déconstructions spécifiques. Ce chapitre questionnera les deux propositions restantes : les CM sont des monnaies et elles seraient « meilleures » que les monnaies nationales, en raison d'un apolitisme prétendument garanti par l'absence de gouvernance humaine.

Ce projet de ce chapitre implique d'interroger le concept de monnaie et, par extension, les problématiques liées à sa gouvernance, qui sont importantes dans l'analyse de la monnaie. En cherchant à mieux caractériser les CM et à apprécier leur prétention à être de « bonnes » ou « mauvaises » monnaies, nous mettrons en évidence que leur singularité tient justement à la forme apparente de leur gouvernance, ni centralisée, ni « *acéphale* » (Favier et Takkal Bataille 2017), mais « *polycéphale* ». Nous affirmerons la nature monétaire de Bitcoin et d'Ethereum, sans pour autant épouser les vues monétaires des critiques académiques et praticiennes ou celles des *coiners\**. Après avoir établi que la question de la gouvernance est au cœur de l'éclaircissement catégoriel sur le statut monétaire des CM, nous interrogerons plus avant cette gouvernance dans le Chapitre III.

De nombreuses ambitions monétaires « libérales technicistes » des *coiners\** renvoient à des controverses structurantes du champ monétaire, sur la définition de la monnaie, les propriétés attendues pour qu'elle soit « bonne » et la gouvernance qui la garantit comme telle.

---

<sup>219</sup> J. Nash voyait dans la révolution technologique la possibilité qu'une entité indépendante calcule un indice monétaire mondial (en relation à des indices de prix de marchandises) permettant de garantir des prix nominaux homogènes et stables, à la manière des poids et mesures et ce, hors intervention des Banques centrales et des États, dispendieux, car « pardonneurs » des « péchés des personnes surendettées [...] des banques » ou de leurs « propres péchés » (Nash 2002, p.6) ; ou M. Friedman (1999; [https://www.youtube.com/watch?v=j2mdYX1nF\\_Y](https://www.youtube.com/watch?v=j2mdYX1nF_Y) ; [consultation au 11/11/2021]). M. Friedman, quant à lui, voyait dans Internet la promesse de l'émergence d'un eCash anonyme, qui priverait les gouvernements de leurs capacités à lever l'impôt.

<sup>220</sup> Simmel (2009), dans le chapitre 2 de son ouvrage, dessine l'évolution historique et philosophique « inachevable » de l'argent, de la substance à la fonction. Le recouvrement de la valeur-substance (caractéristique des monnaies marchandises) par la valeur-fonction (caractérisant les monnaies papier), tendant à faire de l'argent un pur symbole, ne saurait être total : à mesure que la garantie substantielle s'efface, des garanties collectives émergent, garantissant la circulation économique (cf. le monopole étatique d'émission et la marque crédible d'un représentant de la totalité sociale).

Ces ambitions réactualisent un débat ancien et récurrent dans l'histoire monétaire, que condense la formule « la règle contre la discrédition» qui pose la question d'une monnaie neutre.

L'orthodoxie, camp de la *règle*, regroupe les partisans de la neutralité (ou neutralisation) de la monnaie, conçue comme une marchandise dont l'équilibre dépend d'un marché concurrentiel. Pour ce courant, seule compte la stabilité de l'unité de compte, et il faut donc tout sacrifier à une monnaie saine (« *sound money* ») à l'offre limitée pour garantir sa valeur dans le temps. Cette stabilité, vue comme neutralité, serait « bonne » pour l'économie, car elle permettrait aux acteurs de fixer leurs anticipations. Si, historiquement, l'administration centrale de la monnaie est un mal nécessaire, ce courant prône des règles rigides pour contraindre strictement les politiques monétaires et les autorités. Dans le camp de la *discrédition*, la monnaie est d'abord un cadre politique. Sa qualité se mesure à la capacité du système monétaire à assurer sa reproduction selon les principes fondateurs reconnus par ses membres. La monnaie et ses qualités dépendent d'arbitrages de la communauté de paiement : la stabilité de l'unité de compte est un choix, assurer la viabilité du système de paiement en est un autre, non moins important suivant le contexte. Ultimement, la communauté de paiement décide des fins et moyens à mettre en œuvre. Bien que les autorités monétaires doivent rendre des comptes à la communauté, elles doivent aussi disposer de marges de manœuvre et de pouvoirs discrétionnaires (cf. prêt en dernier ressort). Pour ce courant, une « bonne » monnaie maintient un consensus politique autour d'elle. L'estimation des qualités et de la légitimité de la monnaie dépend de l'analyse des usages, de l'utilité et des attentes des acteurs.

Dans ces controverses, les ambitions libérales technicistes des *coiners*\* s'inscrivent dans le camp d'une *règle radicalisée* où toute centralisation est une compromission. Malgré leurs différences, nombreux sont les *coiners*\* à penser que toute monnaie fait face à un problème fondamental : la confiance ! (Nakamoto 2009c). Face aux problématiques entourant la stabilité de la valeur de la monnaie, les *coiners*\* considèrent Bitcoin et les CM comme des solutions inédites. Par leur architecture, les CM se posent comme des alternatives à un ordre monétaire contemporain jugé incapable d'offrir une monnaie et une politique monétaire indépendantes et de qualité, en raison d'une conception fondée sur une collusion entre les pouvoirs politiques et bancaires. Pour les *coiners*\*, les CM offriraient des monnaies saines d'une « dureté » et d'une crédibilité inégalées<sup>221</sup>, car l'immutabilité du monnayage garantirait une cohérence temporelle à toute épreuve. Le design des CM réussirait un tour de force inédit : se protéger une fois pour toutes des interférences politiques, des manipulations monétaires et de l'inflation qu'elles produiraient toujours<sup>222</sup>. Certains promoteurs voient en elles de « meilleures » monnaies que les « fiat » monnaies nationales<sup>223</sup>, qui devraient servir à fonder un système monétaire international plus sécuritaire, efficace et résilient, suivant un processus d'« *hyper-bitcoinisation* » présidant

---

<sup>221</sup> Bitcoin « est la monnaie la plus saine qui ait jamais existé [...] du point de vue de l'économie autrichienne, des maximalistes\* du bitcoin et de l'économie de la monnaie saine. [Contrairement à] l'euro [dont] les grands risques [...] sont l'émission illimitée de monnaie, l'endettement énorme, l'injection de liquidités dix ans après la crise précédente. » (Antonopoulos Bitcoin Q&A 2018).

<sup>222</sup> L'usage indigène du terme inflation renvoie aux modalités d'émission d'UCN et non à l'augmentation générale du niveau de prix mesuré par l'IPC. Cet usage inclut l'idée du monétariste M. Friedman selon laquelle « l'inflation est partout et toujours un phénomène monétaire », relevant des autorités politiques (Friedman 1973, p. 7). Cette causalité est contestée, l'inflation, comme « processus de hausse cumulative et autoentretenue » des prix ayant diverses causes (Bezbakh 2019, p. 1).

<sup>223</sup> Le terme « *fiat monnaie* », souvent utilisé de manière péjorative, suggère qu'elles n'auraient aucune « valeur intrinsèque » contrairement aux monnaies marchandise. Notre usage est positif : dérivé de « *fiat lux* » (et la lumière fut), il affirme que la monnaie relève d'un acte normatif supérieur. Cela est cohérent avec l'approche nominaliste (encadré n°3) dont nous nous revendiquons. Ce terme représente l'idée d'une monnaie fondée dans la règle, comme soulignée par Aristote dans l'*Éthique à Nicomaque* (« *Numisma* », monnaie en grec, dérive de celui de « *Nomos* », la règle/loi (Favier [1981], cité par Desmedt et Piégay 2007, p. 118).

à une adoption massive de Bitcoin ou d'une autre CM, qu'ils appellent de leurs vœux (« *hyper-crypto-monétisation* » par suite, Ammous 2018, p. 9).

*Coiners*\* et professionnels de l'argent, théoriciens et praticiens de la monnaie se revendiquent du camp de la *règle*. Cette proximité théorique concourt en partie de la dureté du conflit qui les oppose concernant Bitcoin et les CM. Plus « *royalistes que le roi* », les *coiners*\* prétendent avoir dépolitisé la monnaie par un monnayage sain, dont les professionnels de l'argent, encore trop dépendants d'intérêts politiques, sont exclus. Les professionnels de l'argent leur répondent que, au titre de cette absence de gouvernance justement, les CM sont de très mauvaises monnaies et qu'il n'est ni possible, ni désirable de les voir s'imposer massivement. Nous nous inscrivons quant à nous dans le camp de la *discretion* qui renvoie le jugement sur la qualité (bonne ou mauvaise) de la monnaie à l'analyse empirique des usages et de la gouvernance monétaire.

Mais avant de se disputer sur les qualités de ce que nous avons considéré jusqu'ici des monnaies, il importe d'avoir statué au préalable sur ce statut monétaire que l'appellation de CM revendique à concurrence des monnaies traditionnelles. C'est à dessein que nous avons repris cette appellation indigène. Notre thèse défend en effet l'idée que les CM font monnaie et qu'elles en constituent une forme inédite de par leur gouvernance. L'appellation de CM souligne en outre la centralité de la cryptographie\*, nœud\* sociotechnique de leurs protocoles, de leur monnayage, et des arrangements d'usage (la liaison entre l'individu et le collectif s'y jouant, cf. Chap. I). Or ce statut monétaire reste majoritairement contesté par les économistes et les praticiens et n'est reconnu que marginalement, par certains travaux (Yermack 2013; Maurer, Nelms et Swartz 2013; Ali et al. 2013; Böhme et al. 2015; Raskin et Yermack 2016; Dodd 2017; Kindelberger 2017; André Orléan 2019). Affirmer ou infirmer le statut monétaire des CM n'est pas chose aisée, car il faut définir ce qu'est la monnaie, question sans réponse unanime, tant les approches de la monnaie sont plurielles et situées. Les écoles théoriques ont en outre souvent répondu aux questions soulevées par les monnaies de leur temps (Tutin 2009; de Boyer des Roches et Rosales 2003), si bien que les CM, plus récentes, apparaissent comme des objets monétaires non identifiés.

Les éléments ci-dessus expliquent que « *la plupart des analyses sur le Bitcoin ne parviennent pas à se positionner clairement et créent ainsi de faux débats, car elles souffrent précisément d'un vide théorique* » (Desmedt et Lakomski-Laguerre, 2015, p. 5). Historiquement, les innovations monétaires ont entraîné des adaptations institutionnelles et politiques, si bien que les CM sont de formidables outils heuristiques permettant de reconstruire les variations des dispositifs institutionnels de la monnaie et de réinterroger ce que recouvre l'argent conceptuellement et pratiquement<sup>224</sup>. Comme la monnaie de crédit au XIX<sup>e</sup> siècle, l'informatisation des marchés des années 1990 ou les monnaies électroniques des années 2000, Bitcoin et les CM ne correspondent pas aux représentations juridiques et académiques usuelles. Comme les innovations précédentes, les CM suscitent un débat renouvelé sur la monnaie, son statut, son rôle (Tutin 2009; de Boyer des Roches et Rosales 2003; Kindelberger 2004). Les CM, en tant que « *monstres institutionnels* » constituent une « *épreuve d'explication* » (Muniesa, 2017) pour les académiques comme pour les praticiens, mettant en crise la définition

---

<sup>224</sup> Kindelberger (2004) et Minsky (1985) font des innovations financières la clef des crises monétaire et financière : les assouplissements monétaires qu'elles permettent (effet de levier, desserrement des contraintes financières, décloisonnement) concourent tant à la phase d'euphorie qu'à la constitution de bulles, et à l'intensité des conséquences de leurs éclatements : contagion de la panique, dissémination et interdépendance des risques, etc. C'est aussi la démarche de Simmel (2009) dans sa « Philosophie de l'argent » quand il analyse les bouleversements monétaires de son temps, en particulier l'émergence de la monnaie de crédit et des monnaies papier.

de la monnaie et obligeant à expliciter clairement ce qu'elle est et ce qu'elle n'est pas<sup>225</sup>. Les CM peuvent être rapprochées des monnaies parallèles, dont « *la théorie économique tient rarement compte [...] avec difficulté (substitutions de monnaies) ou en liaison avec des phénomènes très spécifiques (hyperinflation) qui ne procèdent que d'une portion du phénomène* » (Blanc 1998a, p. 6). Cette relégation des monnaies alternatives s'explique selon Jérôme Blanc (1998a) par le fait que l'*« analyse économique des phénomènes monétaires [...] repose [...] sur deux modèles distincts [mais] complémentaires et inadéquats* » pour aborder les monnaies alternatives: une « *approche monétaire juridique* » considérant que la monnaie relève uniquement de l'État et une « *approche monétaire marchande* » considérant que la monnaie est une marchandise réduisant les coûts de transaction\* du troc . Le cas des CM pose les mêmes difficultés et interroge la capacité des théories en présence à penser les monnaies dans leur altérité. Les CM seront pour nous l'occasion de remettre en cause les représentations dominantes, en y opposant un institutionnalisme monétaire francophone (IFM) intéressé par les pratiques des acteurs.

Pour démontrer le caractère monétaire des CM, ce chapitre est découpé en 3 sections.

**La première section** (II.1) présente une revue de la littérature des critiques des CM, tout en les résitant au sein de leur corpus théorique et épistémologique respectifs. Derrière la diversité des critiques d'économistes orthodoxes, hétéodoxes ou de praticiens se dessinent deux ensembles motivant la relégation monétaire des CM : l'approche instrumentale et l'approche nominaliste-chataliste.

**La deuxième section** (II.2) sera l'occasion de préciser notre approche inscrite dans l'institutionnalisme monétaire et empruntant à l'ethnographie économique. Nous nous inscrivons ainsi dans un nominalisme non étatiste, qui nous permet d'affirmer que ni les fonctions canoniques de la monnaie (centrales pour les tenants de l'approche instrumentale), ni l'exclusivité étatique (essentielle pour les critiques issues des approches chartalistes) ne peuvent servir à reléguer les CM hors du champ de la monnaie. En effet, à la lumière des pratiques, les CM présentent bien les caractéristiques minimales reconnues de toute monnaie (saisie par le triptyque conceptuel : dettes, confiance, souveraineté) et s'intègrent aisément au phénomène des monnaies parallèles.

**La troisième section** (II.3), poursuivant la tentative de caractérisation des CM dans le champ monétaire, formule une hypothèse opposée à celle qui fonde la dispute entre les *coiners*\* et leurs contemporains autour de la qualité de ces monnaies : si la singularité monétaire des CM est à chercher du côté de leur gouvernance, ce n'est pas parce que cette dernière est absente, neutre ou réduite à leurs codes protocolaires. Comme esquisé par le premier chapitre, les CM et leurs communautés de paiement sont « *multifacette[s], politiquement contestée[s] et sociologiquement riche[s] en fonction et sens* » (Dodd, 2017 p. 4 et 8). À trop discuter les seuls avis des *coiners*\* les plus libertariens et à comparer les CM aux monnaies nationales, les professionnels de l'argent se privent de voir l'hétérogénéité des représentations monétaires des *coiners*\*, les conflits communautaires qu'elle implique, et donc la gouvernance en place pour les réguler. En effet, les communautés de *coiners*\* sont traversées par des controverses concernant le fait de faire évoluer ou non leur CM pour qu'elle soit « meilleure », visibilisant une gouvernance duale et polycentrique, excédant le cadre formel d'interaction qu'établissent leurs codes protocolaires. Ce type de gouvernance explique alors que les CM n'obéissent ni à

---

<sup>225</sup> à l'instar des « *Electronic Communication Network* » qui mirent en crise la définition du marché, et analysés par Muniesa (2017, p. 3) à qui nous reprenons le concept d'épreuve d'explication.

la logique de sceau (des monnaies étatiques), ni à celle de signature (des monnaies privées). Ce point ouvre une voie d'éclaircissement catégoriel dans le champ monétaire.

## II.1 « LES CM NE SONT PAS MONNAIE ! » : ARGUMENTS CONTRE LE CARACTÈRE MONÉTAIRE DES CM

Grâce à une revue critique de la littérature économique et monétaire, cette section vise à présenter les grandes lignes de la controverse entourant le statut monétaire des CM. Nous avons recensé les critiques concourant à ce qu'une majorité d'experts ne considère pas les CM et Bitcoin comme monnaie, puis nous avons cherché à restituer les fondements théoriques et épistémologiques de ces jugements, afin d'en préciser les limites et les angles morts. Ce travail théorique nous est apparu nécessaire à plusieurs titres. Premièrement, ces critiques s'inscrivent toutes dans des fondements épistémologiques, des catégories, des définitions et des représentations différentes, voire antinomiques. Deuxièmement, elles relèvent souvent d'un syncrétisme problématique en termes de cohérence interne et externe : « *force est de constater qu'un manque de clarté, si ce n'est une réelle confusion, règne la plupart du temps dans les études sur le sujet. [...] le constat le plus sévère est à faire au sein de la discipline économique [...] où, la plupart du temps, les commentaires sur le Bitcoin ne s'accompagnent d'aucun éclairage théorique. Est-ce si étonnant, lorsqu'on sait à quel point la monnaie divise les économistes ?* » (Desmedt et Lakomski-Laguerre 2015, p. 2). Comme épreuve d'explicitation, les CM interrogent la capacité des théories dominantes à les intégrer. Rien de surprenant si l'on replace cette dispute dans l'histoire des controverses qui ont toujours succédé aux innovations monétaires. Si chacune des écoles économiques a cherché à répondre à des questions liées aux monnaies de son temps, les CM sont alors de formidables objets pour contribuer à la théorie monétaire.

En tant qu'innovation d'ampleur, il est compréhensible que les CM questionnent et fassent débat. Comme les innovations précédentes, elles entrent difficilement dans les catégories monétaires existantes et leurs spécificités rendent ardue leur appréhension, tant par l'opinion publique que par les économistes et les praticiens – acteurs bancaires et financiers, autorités de régulation, banque centrale et administrations publiques –, d'autant plus qu'il n'existe pas de définition unique et consensuellement acceptée de la monnaie. Celle-ci est définie différemment dans le champ juridique – à travers un écheveau d'articles et de codes différents (sect. II.1.2) - ou dans celui économique - au sein duquel des définitions concurrentes existent (sect. II.1.1 et II.2). Certaines propriétés et certains invariants théoriques font plus ou moins consensus. Ainsi, à la suite d'Aristote, ont été identifiées théoriquement des « fonctions » de la monnaie qui servent de bréviaire pour tout ce qui touche à l'argent : la fonction d'unité de compte, celle d'instrument d'échange, et celle de réserve de valeur. En tant qu'unité de compte, la monnaie sert d'étalon général de la valeur au fondement de tout calcul économique : toute valeur d'échange en dépend, et cette fonction conditionne la fixation de grandeurs nominales qui permettent de rendre commensurables, comparables et échangeables entre eux des biens hétérogènes en quantité et qualité. Comme instrument d'échange, elle joue le rôle d'intermédiaire acceptée et reconnue de tous : la monnaie est un équivalent général échangeable contre toute marchandise. Enfin, en tant que réserve de la valeur, la monnaie peut être un actif de patrimoine et servir à reporter ses achats dans le temps. Bien que communes aux approches monétaires, ces fonctions n'ont cependant pas le même sens, ni la même importance selon les théories : la priorité et le statut donnés à chacune déterminent les différences entre corpus concurrents.

De fait, les CM ne coïncident pas avec les définitions et théories économiques dominantes (J.P Koning 2012; Selgin 2013; Selgin 2014b; Beat Weber 2014a; Desmedt et Lakomski-Laguerre 2015). Le champ monétaire se structure autour de deux grandes approches opposées. Et si, comme Schumpeter le rappelait, il n'y a « *que deux théories de l'argent qui méritent ce nom... la théorie de la marchandise et la théorie de la créance* » (Goodhart 2005, p. 817), aucune ne fait de place aux CM : ces dernières sont reléguées tantôt par les approches instrumentales et substantielles, qui, au cœur de la théorie néoclassique, conçoivent la monnaie comme une marchandise (voir Encadré n°1), tantôt par les approches concurrentes dites nominalistes (ou « *des contraintes légales* », au cœur de l'approche Chartaliste, voir Encadré n°2 ; Orléan 1998, p. 11), qui conçoivent la monnaie comme une dette sociale aux porteurs, produit des restrictions de l'État. D'abord, nous reviendrons sur les critiques d'ordre théorique dans le champ économique.

### **II.1.1 La critique des CM depuis les grands courants de théorie monétaire**

Les connaisseurs de la science économique et de ses professionnels peuvent être surpris de la formation d'un accord consensuel entre écoles de pensée opposées, singulièrement dans le champ monétaire, ce que parviennent pourtant à produire les CM. Une majorité d'auteurs, de toutes obédiences, leur refuse le statut de monnaie. Puisque les analyses de la monnaie, de sa nature, des conditions de son émergence et de ses effets divergent suivant l'appareillage conceptuel mobilisé, il importe de restituer les critiques des CM au sein de leurs cadres théoriques. Nous commencerons par les critiques émanant de l'approche monétaire dite instrumentale, orthodoxe en science économique, où la monnaie est conçue comme une marchandise (« *commodity money* »). Puis, nous présenterons les critiques chartalistes, fondées dans le corpus concurrent qui conçoit la monnaie comme une créance sur l'État (« *claim money* »).

#### **Les critiques instrumentales fondées sur des fonctions monétaires canoniques**

Les approches monétaires instrumentales ou substantielles reposent sur un appareillage théorique complexe qui s'étaye sur une théorie de la valeur utilité / rareté (voir encadré n° 1, ci-dessous). La quasi-totalité des économistes critiquant les CM le fait depuis ce cadre. De ce point de vue, l'objet monnaie (et les CM n'y dérogent pas) doit avoir une valeur « intrinsèque », sise sur des caractéristiques désirables. Les fonctions monétaires canoniques dérivent de ces propriétés recherchées ; elles justifient l'expression d'une demande rationnelle de monnaie, suivant l'utilité procurée par sa « consommation ». Au même titre que les monnaies papier non parfaitement convertibles (les fiat monnaies), l'intégration des CM dans cet appareillage n'est pas aisée : leur « *métallisme digital* » (Maurer et al, 2014 ; Mallard et al, 2018) ne suffit pas à les identifier pleinement aux monnaies métalliques (d'or et d'argent), représentantes idéales typiques de monnaie marchandise pour ce courant. On prête naturellement aux monnaies métalliques une valeur intrinsèque, relevant de leur adossement à des matériaux physiques socioéconomiquement précieux : la valeur de la monnaie est supportée par leur rareté relative et des propriétés physiques singulières et recherchées (malléabilité, inoxidabilité, etc.), qui leur confèrent une valeur de marché non exclusivement monétaire, ouvrant à une utilité de consommation propre et immédiate (la « *valeur substance* » de Simmel 2009). Les CM présentent certes, à la manière de métaux précieux, une offre limitée et les propriétés reconnues de bonne marchandise monétaire que sont la divisibilité, la transportabilité et la conservation dans le temps (Menger 1892, p. 247), mais l'immatérialité de leurs UCN\* empêche pour ces économistes d'y trouver une valeur intrinsèque liée à l'utilité d'une consommation directe.

### Encadré n° 1 : L'approche instrumentale et substantielle de la monnaie marchandise

L'approche monétaire « instrumentale » fonde le cadre de l'économie orthodoxe (théories standard et standard étendue de l'équilibre général). Encrée à la « théorie de la valeur » utilité / rareté, elle vise à penser les liens objectifs entre les activités de production et de consommation et à déduire la valeur réelle (prix relatifs réels hors expression monétaire) de toute marchandise. La théorie quantitative de la monnaie (comme représentée par l'équation de Fisher :  $M * V = P * T$ ) en est un appendice essentiel, établissant un lien entre la quantité de monnaie en circulation (M), la vitesse de circulation de la monnaie (V), le niveau des prix (P) et le volume des transactions\* économiques (T). Pour cette théorie, l'augmentation de M conduit à celle de P, tandis que T reste inchangé : pour importante que soit la monnaie dans la facilitation des échanges, elle n'est qu'un « voile » inessentiel (expression indirecte de valeurs déjà là) par nature neutre : « *les échanges et la production ne sont modifiés ni en niveau ni en structure par des variations de la quantité de monnaie émise. Ils ne dépendent que des données réelles de l'économie, à savoir les ressources utilisables, les technologies disponibles et les goûts des consommateurs.* » (Orléan 1998, p. 9). Dans le cadre marchand d'une concurrence pure et parfaite où les relations économiques sont réduites à une seule logique contractuelle privée, la valeur monétaire et ses fonctions corolaires (en particulier la fonction d'échange) doivent s'expliquer par les caractéristiques substantielles des médiums monétaires : la monnaie doit être une marchandise intégrable à la fonction d'utilité du consommateur. Il faut s'imaginer « *un monde sans asymétrie d'information où les biens sont liquides. Il n'y a ni monnaie ni crédit bancaire. Que des titres !* » (de Boyer des Roches et Rosales 2003, p. 1). Et tout cours d'économie commence par en conter la « fable du troc » : le passage d'échanges en nature incommodes (double coïncidence des besoins) à d'autres médiatisés par la monnaie.

La naissance de la théorie monétaire contemporaine cherche, avec Menger (1892), l'« origine » de la monnaie et les déterminants de sa demande dans les seuls intérêts individuels. Les explications holistes communément avancées qui, depuis « *Platon, Aristote et les juristes romains* », fondent le statut de moyen d'échange sur la « *convention générale ou [...] la loi* » (*Ibid.*, p. 240-241) contreviennent à l'individualisme méthodologique de Menger, pour qui la demande de monnaie doit avoir des fondations micro-économiques. S'il est simple « *de démontrer qu'il est globalement avantageux, au sens parétiien [...] d'utiliser la monnaie* », encore faut-il prouver que cela « *est un choix sensé pour les individus* » (Orléan 1998, p. 12). Menger (1892), cherche l'utilité propre des monnaies dans leur « valeur intrinsèque » conçue comme valeurs d'échange préexistantes, dérivées d'utilité passée (utilité tirée d'usages non monétaires premiers).

Von Mises (1912) en affinera l'approche avec son

« *théorème de régression* » (*Ibid.*, p. 97 à 123). Reste que l'utilité dégagée n'est qu'indirecte, la marchandise monnaie n'est utile qu'en ce qu'elle permet d'obtenir d'autres marchandises à valeur d'usage propre et immédiate. Résultat insatisfaisant, il faut comprendre « *l'utilité de détenir de la monnaie et pas [...] l'utilité de la dépenser* » (Patinkin, cité par A. Orléan 2002, p. 11). L'apparition des « fiat monnaies » se prête mal à une reconnaissance de « *valeur intrinsèque* » même réminiscente. Les « fiat monnaies » étant non « *intrinsèquement utiles* », car inconvertibles et à rendement nul, les questions des déterminants de leur demande et de leur pouvoir d'achat sont redoublées (Hellwig, 1993, cité par Cartelier 2001, p. 994). La question de leur ancrage nominal redevient centrale en l'absence de contrainte exogène d'émission, « *la quantité nominale de monnaie fiduciaire peut être augmentée sans avoir recours à plus de papier et d'encre, simplement en fournissant des coupures plus grosses qu'auparavant, "il n'est pas certain qu'il existe un niveau de prix fini" qui constituera un équilibre* » (Selgin 2013, p. 3). Conséquemment, ces fiat monnaies commandent une offre monopolistique, condition nécessaire de leur « *valeur positive [...] mais la fourniture monopolistique n'est pas suffisante, car un fournisseur monopolistique de monnaie fiduciaire qui maximise ses profits trouverait également profitable d'accroître le stock nominal de cette monnaie à un taux bien supérieur à celui qui est nécessaire pour préserver son pouvoir d'achat* » (*Ibid.*).

Les modélisations économiques contemporaines travaillent à faire ressortir l'utilité/les fonctions des fiat monnaies, au prix d'hypothèses *ad hoc*. Les modèles à générations imbriquées, ou de prospection, concilient intérêt individuel et existence d'une demande, tout en faisant l'économie de références holistes (*Ibid.* ; Orléan, 1998, p. 12-13). Les modèles de prospection avancent sur la question de la fonction d'échange, posant une division du travail qui empêche les agents de consommer leur production ; ils permettent d'inférer « *l'existence d'équilibres avec utilisation d'une monnaie purement fiduciaire dans les transactions\** » (Cartelier 2001, p. 994). Reste que ces modélisations précédentes conservent une fonction de réserve de valeur dérivée du fait que la monnaie est acceptée comme instrument d'échange. La fonction d'unité de compte reste la plus problématique dans cet appareillage. Si Keynes la considérait comme essentielle à toute économie monétaire (Keynes, 1930), soulignant l'existence de règles de monnayage renvoyant à un cadre normatif premier, l'orthodoxie n'a « *jamais pu expliquer comment les maximisateurs d'utilité individuelle s'arrangent] pour n'avoir qu'un numéraire* » (Randall Wray 2010, p. 40). Certains travaux ont récemment tenté d'éclairer cette énigme, partant de relation contractuelle bilatérale, avec risque de prix et coût de rupture des contrats ; ils arrivent à établir que l'établissement et l'usage d'une unité de compte commune et dominante améliorent les résultats économiques globaux (Doepke et al. 2017).

En ce qui concerne la fonction d'unité de compte, un consensus existe pour dire que les CM ne peuvent prétendre à porter cette fonction (Ali et al. 2013, p. 5; Yermack 2013, p. 3 et 7;

Beat Weber 2014a, p. 16). Leurs UCN\* ne seraient en effet pas un étalon général, ne servant pas (ou trop peu) à dénominer la valeur de biens et services. Bien que des prix soient aujourd’hui libellés en UCN\* BTC ou ETH, il ne faudrait pas y voir une utilisation *per se* : selon ces auteurs, les prix affichés en UCN\* cachent une fixation nominale en monnaie nationale (ici, le numéraire premier), dont l’ajustement en temps réel à leur cours boursier est effectué grâce à des services de passerelles\*, offrant aux marchands un service de conversion instantanée des UCN\* reçues en paiement (cf. Chap. I.2.1 ; Ali et al. 2013; Brito et Castillo 2013). Ce manque d’usage en compte se voit particulièrement dans le fait que les coûts supportés par les opérateurs des nœuds\* sont dénominés en fiat monnaie, contre leurs revenus libellés, eux, en UCN\*. Les UCN\* ne seraient ici qu’un véhicule de paiement, non une monnaie.

Les avis concernant la capacité des CM à porter la fonction d’instruments d’échange sont plus nuancés. Certains auteurs leur reconnaissent cette capacité (Yermack 2013, p. 7; Brito et Castillo 2013, p. 34), mais la majorité en nuance la portée (Beat Weber 2014b, p. 2; Beat Weber 2014a, p. 16) : leurs sphères transactionnelles seraient trop faibles. Au nombre relativement mince de marchands acceptant les CM répondrait un nombre tout aussi réduit de transactions\* (Ali et al. 2013, p. 4; Roubini 2018; Bank of International Settlements 2018). En outre, cette fonction serait cantonnée à des activités illégales (Weber 2014b, p. 2; Krugman 2013; Krugman 2018a; Krugman 2018b; Stiglitz 2017; Tirole 2017). Les CM s’avèrent en outre être des « *moyen[s] de paiement lourd[s], lent[s] et coûteux* » (Krugman 2018b) et seraient inefficaces en comparaison des moyens de paiement existants (cartes de paiement, PayPal, etc.). Finalement, leur acceptation en paiement serait réductible à une stratégie de communication de firmes qui en useraient plus comme des « *signaux - regardez-moi, je suis à la pointe du progrès ! - que [pour leur] utilité réelle* » (Krugman 2018a). Du fait de ce manque d’usage, elles seraient bien incapables de tenir la fonction de réserve de valeur. L’ensemble des commentateurs a souligné cette incapacité fonctionnelle, notamment du fait de la grande volatilité de leur cours. Cette volatilité les rendrait, par définition, inaptes à offrir une fonction de réserve de valeur (Ali et al. 2013, p. 4; Yermack 2013, p. 2 et 7; Beat Weber 2014a, p. 16; Beat Weber 2014b, p. 3; Kubát 2015), puisqu’anticiper des baisses de cours n’incite pas à leur détention. À l’inverse, anticiper des hausses brutales n’incite pas à leur dépense et à leur circulation. On comprend que, au prisme d’une approche instrumentale où, « *pour réussir, la monnaie doit être à la fois un moyen d'échange et une réserve de valeur raisonnablement stable* » (Krugman 2013), les CM sortent du cadre.

Au bout du compte, au sein du corpus néoclassique dominant, les CM ne se voient reconnaître ni valeur intrinsèque, ni fonctions monétaires, essentielles à leur qualification monétaire. De ce point de vue, N. Roubini nous donne une conclusion lapidaire : « *Bitcoin n'est PAS une monnaie : ce n'est pas une unité de compte, ce n'est pas un numéraire unique, ce n'est pas un moyen de paiement évolutif, il n'est adossé à aucun actif, il n'a pas cours légal, son prix est fortement manipulé et sa fonction de réserve partielle de valeur ne repose donc sur rien.* »<sup>226</sup>. L’ajout qu’il fait de la référence à la loi, inscrite dans le corpus nominaliste concurrent, illustre le syncrétisme dont il fait montre (comme tant d’autres), et annonce qu’une même disqualification les y attend, suivant des arguments différents.

---

<sup>226</sup> <https://twitter.com/Nouriel/status/1325884383170093056> [consultation au 10/07/2023].

## Une monnaie « créature de l’État » : les critiques nominalistes et chartalistes

Dans le champ des sciences humaines, l’histoire des origines de la monnaie et les concepts clefs de la théorie orthodoxe sont contestés. Ni les historiens, ni les anthropologues, ni certains économistes ne reconnaissent de véracité historique et empirique à ces « mythes » d’une monnaie purement marchande, qui pourtant ne l’est pas primitivement<sup>227</sup> (Aglietta et Orléan 1998; Alary 2009; Wray 2010, p. 39; Cartelier 2013). Le corpus « nominaliste »<sup>228</sup> conteste ce que ses auteurs considèrent comme une *sophistique* économique *aprioriste*, *ahistorique* et *asociale*, qui projette rétrospectivement (et anachroniquement) sur les phénomènes économiques et monétaires des catégories erronées (Chavance 2011, p. xi). Les multiples approches monétaires hétérodoxes qui constituent ce corpus (chartalisme, néochartalisme, post-keynésianisme, institutionnalisme, conventionnalisme, etc.) partagent une vision de la monnaie non marchande (Ingham 2004, p. 24; Aglietta et Orléan 1998) et chaque courant établit des liens (plus ou moins forts) entre la monnaie, l’État et le cadre normatif que ce dernier établit et rend exécutoire (voir encadré n°2 ci-après).

---

<sup>227</sup> Mauss critique Menger et sa recherche d’une origine *ex nihilo* et individuelle de la monnaie, car, à l’opposé du mythe économique du troc, aucune société ne « *fut complètement démunie de notions au moins analogues* » (Mauss, 1914). Les études d’anthropologues et d’historiens prouvent l’antériorité de paiement monétaire non marchand : il suffit d’« *examiner la diversité des formes où le paiement et l’obligation se sont manifestés dans l’histoire économique* » afin de « *retracer une évolution dont l’origine est prééconomique et préjuridique. Le paiement existait avant qu’ait été établie la distinction entre droit civil, droit pénal et droit religieux. [...] Avec l’introduction du système de marché [...], le paiement se présente désormais comme la contrepartie d’un avantage obtenu au cours d’une transaction [...]. L’idée même de l’origine indépendante du paiement est perdue, on a oublié les millénaires de civilisation humaine où le paiement ne provenait pas de transaction économique, mais directement d’obligation religieuse, sociale ou politique* » (Polanyi 2011, p. 175-177). Pour preuve, la tenue de registre\* de créances (monnaie scripturale) et l’évaluation d’obligation non économique (religieuses, coutumières, légales ou fiscales) sont antérieures à l’apparition des monnaies « marchandises » (Randall Wray 2010, p. 40), ce qui illustre la « monnaie meurte » concernant les paiements monétaires d’amende, la « monnaie mariage » concernant les phénomènes de dot, les tributs d’empire, etc. (Aglietta et Orléan 1998).

<sup>228</sup> Cette appellation renvoie à la liaison étymologique entre les mots monnaie et loi (Goodhart, 2005; Ingham, 2004) : l’origine du mot « monnaie » dérive du grec « *nomisma* », preuve « qu’elle tient non pas à la nature, mais à la loi [en grec : *nomos*] (Aristote, 2004, p. 249) » (J. Favier, 1981, cité par Desmedt et Piégay 2007, p. 118).

## Encadré n°2: Les approches nominalistes de la monnaie : une dette sociale au porteur liée à une autorité souveraine.

À l'inverse des approches monétaires orthodoxes, celles dites nominalistes prolongent les réflexions de « *Platon, Aristote et les juristes romains* » sur les liens consubstantiels entre la monnaie et la « *convention générale ou [...] la loi* » que contestait Menger (1892, p. 240-241). Si Menger réussit à imposer ses problématiques de recherche, elles furent au centre de la querelle des méthodes entretenue avec G. Schmoller (la « *Methodenstreit* », Ingham 2004). Ces débats influenceront ses élèves Simmel et Knapp, et se perpétueront dans le champ académique jusqu'à aujourd'hui. Quel que soit le courant, tous partagent une opposition à la théorie de la valeur. Pour eux, la valeur ne préexiste pas à l'échange, mais renvoie ontologiquement à la présence d'une *monnaie de compte* : tout échange, même en troc, relève de dispositifs sociaux au cœur desquels gît la monnaie, le troc étant un cas particulier d'échange monétaire (Simmel 2009). La valeur naît de relations d'échange monétaire tripartite où la monnaie (et ses représentations) joue le rôle de tiers médiateur essentiel (*Ibid.*), en tant que « *principe d'évaluation partagé* » sans lequel pas d'*« échange stable »* (Dequech 2013, p. 257). En outre, ces courants s'opposent à l'épistémologie *aprioriste*, *ahistorique* et *asociale* précédente. La monnaie est indéattachable des relations sociales considérées, s'insérant étroitement dans les systèmes politiques, sociaux et culturels (Polanyi, 1944). Substituant à l'individualisme le holisme méthodologique, la détention de monnaie renvoie de l'articulation de logiques individuelles à d'autres, collectives, relevant moins de « *choix individuels* » que d'une extériorité normative issue d'un collectif institué les conditionnant : l'argent se conçoit comme un cadre préliminaire au marché (et à la logique contractuelle) qu'il est incapable de se fixer lui-même (Cartelier 2001). Ces courants partagent le triptyque conceptuel « dette, confiance et souveraineté », mettant en avant quatre caractéristiques essentielles à la monnaie (Wray 2010) : elle est une dette ; renvoie à l'incertitude radicale et au phénomène de confiance ; a une nature sociale ; et renvoie à de l'autorité (et de la souveraineté).

Une vision de la monnaie non marchande est au fondement des approches nominalistes qui reconnaissent à la monnaie quatre et non trois fonctions canoniques (Ingham 2004, p. 19; Polanyi 2011, p. 163). Est ajoutée une fonction de paiement unilatéral, soulignant la primauté accordée non à la fonction d'échange, mais à celle d'unité de compte, « *logiquement antérieure aux formes et aux fonctions de la monnaie* » (Ingham 2004, p. 22). [L'argent se fait règle, langage métrologique de la valeur économique (Keynes 1930, p. 3, Polanyi 2011) permettant l'évaluation chiffrée d'obligations variées], dont les premières étaient plus sociales et politiques qu'économiques : offrandes, amendes, impôts, tributs. L'argent est simultanément le support de l'expression des relations de dettes et créances sociales tissées au gré de la division sociale et le moyen ultime de leur extinction.

L'argent est ainsi une créance au porteur sur son émetteur, sa détention correspond à être « *un débiteur de biens* » et un créancier « *à l'égard de l'émetteur - monarque, État, banque, etc.* » (Ingham 2004, p. 25). Dans ce cadre, l'acceptation de la monnaie dépend moins de sa matérialité que de l'immatérielle présence de confiance et d'autorité, d'où l'intérêt porté aux liens entre la monnaie, la loi et l'État (Wray 2010, p. 1). Reconnaissant toute l'importance historique du système bancaire hiérarchisé, de l'État et de son rôle dans la stabilité monétaire et économique, les écoles de pensée divergent toutefois sur l'intensité de ces liens.

D'un côté, des approches la conçoivent exclusivement comme une « *créature de la loi* », donc de l'État, suivant « *l'approche juridique des phénomènes monétaires* » de G. F. Knapp (1924, p. 1). Qu'importe la matérialité des médiums monétaires (*hylogénique* ou *autogénique*), l'*« l'unité de compte n'est pas définie techniquement, mais juridiquement »* et l'argent, qu'il soit de coquillage, d'or, d'argent ou de papier, est décrété par l'État, qui « *libère* » les « *moyens de paiement* » de la « *nature réelle de leurs matériaux* » (*Ibid.*, p. 296). Les néo-chartalistes et post-keynésien dominant le corpus prolongent cette « *théorie étatiste de la monnaie* » (André Orléan 1998, p. 13). Les problématiques d'autorité y sont réduites à l'État et aux autorités régulatrices qui l'incarnent (Orléan 1998), « *la monnaie est le produit des restrictions qu'impose l'autorité régulatrice aux intermédiaires financiers privés. Sans cette action étatique, la monnaie n'existerait pas.* » (Orléan 1998, p. 11). Le rôle de l'État se singularise et devient essentiel, suivant deux courants qui relient la monnaie aux contrats ou aux impôts respectivement (Dequech, 2013, p. 251) et ce, à l'aune d'une violence légale et fiscale (Dupré, Ponsot et Servet 2015, p. 13). D'abord, l'État définit l'unité de compte et dote ses moyens de paiement d'un cours légal et forcé, assurant l'exécution des contrats libellés en sa monnaie ; il participe à l'unification du système monétaire. Par ailleurs, déterminant le support « *qu'il accepte aux caisses des percepteurs, [il impose l'utilisation et l'acceptation collective de la monnaie]* » (Desmedt et Piégay 2007, p. 120), qui seule permet d'éteindre ses obligations fiscales. Finalement, hors acceptation en paiement par l'État, pas de monnaie : « *tous les moyens par lesquels un paiement peut être effectué au profit de l'État font partie du système monétaire [...]. Ce n'est pas l'émission, mais l'acceptation qui est décisive* » (*Ibid.*, p. 119).

Contre ces approches unilatérales d'une monnaie « *instrument docile entre les mains de l'État* », d'autres la conçoivent comme une convention (Dequech 2013, p. 260 et 251) qui, bien que renforcée par le rôle de l'État, ne peut s'y réduire : l'argent est « *moins décrété qu'élu* » (Servet, Théret et Yıldırım 2016, p. 30), sa légitimité est [éprouvée] et la monnaie reste « *toujours inachevée* » (Aglietta et Orléan, 2002, pp. 32-33, cité par Dequech 2013, p. 258). C'est de ce courant dont nous nous revendiquons, et que nous éclairerons par la suite.

De nombreuses critiques des CM se fondent sur des arguments empruntant à ce corpus, en particulier les arguments issus des théories étatistes de la monnaie. Si, à l'image des fiat monnaies, les CM ne peuvent se prévaloir d'une quelconque « valeur intrinsèque », leur indépendance à la souveraineté politique nationale et aux autorités monétaires les rendrait inaptes à se voir reconnues comme monnaies. L'argent est conçue comme « *monnaie – institution* » et les fiat monnaies, bien qu'exemptes de « valeur intrinsèque », sont dans ce corpus des créances sur un émetteur jouissant de priviléges exorbitants : l'État, qui, par le cadre formel (normatif et fiscal) imposé par la force et la violence, assure la circulation des UCN\* émises et ce faisant, le bouclage macroéconomique (Dupré, Ponsot et Servet 2015, p. 12-13). À considérer que l'argent, en tant que dette particulière, implique une souveraineté politique étatique (réduite à un légalisme formel), on est conduit à exclure les CM du statut de monnaie. En effet, les CM ne seraient « *pas une créance sur qui que ce soit* » (Ali et al. 2013, p. 3). Puisqu'elles ne sont adossées ni à une marchandise, ni au passif émis par une personnalité tierce (physique ou morale), leur acceptation volontaire, hors coercition d'aucune sorte, n'offrirait aucune garantie d'escompte à leurs détenteurs. Ces critiques considèrent dès lors que les CM ne peuvent dans ces conditions jouer ni le rôle de monnaie de compte, ni celui de moyens de paiement et d'échange permettant d'évaluer et de régler des obligations, notamment celles des mineurs perçus comme émetteurs. L'usage en compte, essentiel pour ce courant, est la marque que la monnaie renvoie à un ordre collectif supérieur : la souveraineté monétaire renvoyant à la capacité de l'émetteur à imposer sa monnaie en compte et en paiement. Que dire face à des CM, pour lesquelles l'expression des coûts et revenus de production des activités de minage est différenciée (les premiers exprimés en monnaie nationale, les seconds en UCN\*) ? « *La plupart, voire la totalité, des coûts, même pour les producteurs de l'économie des bitcoins, sont libellés dans des devises différentes (...) [Dans la mesure où] les revenus des bitcoins ont une valeur volatile en termes de devises nécessaires pour payer les intrants, il ne serait pas économique d'adopter les bitcoins comme unité de compte, c'est-à-dire d'afficher les prix en bitcoins* » (Beat Weber 2014a, p. 16). Cet argument, déjà mobilisé par les tenants d'une approche instrumentale, est ici interprété comme la marque d'une absence de souveraineté monétaire propre, privant les CM du statut de créance au porteur, donc de monnaie. Puisqu'« *une chose ne peut être émise sous forme d'argent que si elle est capable d'annuler toute dette contractée par l'émetteur* » (Ingham 2004, p. 25) et considérant (à tort, selon nous) que l'émission d'UCN\* est le fait des mineurs et non du protocole, pour ces auteurs, les CM n'en sont pas.

Les auteurs de ce courant soulignent que les contraintes légales garantissant la demande et la circulation de monnaie ne se limitent plus aujourd'hui aux seules réglementations fiscales. S'y ajoutent les actions régulatrices portées par les autorités monétaires et, plus largement, par les pouvoirs publics. Historiquement, les autorités monétaires ont pris une position centrale dans le système hiérarchique et joué un rôle essentiel, tant sur la stabilité de l'unité de compte que sur celle du système de paiement<sup>229</sup> (Velde 2013, p. 3; Beat Weber 2014b, p. 3; Krugman 2018a; J.P Koning 2018f). Fournissant en dernier ressort crédit et liquidité à la société (Dupré, Ponsot et Servet 2015, p. 19), le monnayage de la monnaie est devenu un outil essentiel à la sphère économique en tant qu'outil de politiques contra-cycliques (Tirole 2017; Varoufakis 2013; Varoufakis 2020). Bitcoin et les CM n'offriraient pas ces leviers, avec leur monnayage fixé à l'avance et indépendamment des conditions économiques réelles. Synthétiquement, la

---

<sup>229</sup> Les autorités monétaires, dont le rôle est de réguler l'offre de monnaie, ont développé pour ce faire différents types d'instruments. Ils fixent les taux d'intérêt directeurs, le niveau attendu de réserves obligatoires et/ou peuvent engager des politiques d'*open market*, suivant les cibles d'inflation définies et annoncées à l'avance. À cela s'ajoutent différentes politiques prudentielles (micro et macro) comme divers monitorings, ou, à l'extrême, les actions de prêt en dernier ressort.

critique de ce courant explique que « *le bitcoin ne repose ni sur un système bancaire hiérarchisé chapeauté par une banque centrale, ni sur un système de compensation permettant d'assurer la pérennité des paiements. Complètement décentralisé, il n'est pas en mesure d'assurer la liquidité nécessaire aux besoins du circuit économique de la production de biens et services par des avances pour le financement de l'économie réelle. En cas de fléchissement des activités économiques, il est incapable de permettre des actions publiques de relance. L'hypervolatilité de son cours en fait un instrument monétaire peu propice à ancrer les anticipations et pérenniser les paiements.* » (Ponsot 2021, p. 3). Finalement, les CM ne seraient en rien comparables aux monnaies nationales, n'offrant « *pas les amortisseurs nécessaires pour empêcher les crises capitalistes* » (Varoufakis 2020). À l'aune de cette comparaison (qui n'est pas raison selon nous, cf. section II.3.2), l'autonomie relative des CM vis-à-vis de l'État, en particulier l'inélasticité de l'émission de leur UCN\*, finit de les reléguer en dehors du champ de la monnaie.

Ainsi, quelle que soit l'inscription théorique des critiques, toutes conviennent que les CM ne sauraient être des monnaies. Nous présenterons maintenant les critiques avancées par les autorités monétaires qui, mêlant les différents arguments déjà recensés, concluent à un même refus catégorique.

### **II.1.2 Les CM comme épreuve d'explicitation de l'argent : des « monstres monétaires » difficilement qualifiables**

La monnaie n'est pas que l'objet de débats théoriques abstraits, elle est aussi une construction pratique très concrète : l'ordre monétaire et financier est d'abord défini formellement par la loi et par la pratique des autorités monétaires. Avec les CM, les législateurs et les régulateurs doivent d'abord, comme pour toute innovation monétaire et financière, s'interroger sur leur statut juridique. Or, leur singularité rend la qualification juridique ardue dans la mesure où ils ne correspondent ni aux définitions juridiques existantes, ni à celles développées empiriquement par les autorités monétaires et leurs administrations. Les CM soumettent la monnaie à une « *épreuve d'explicitation* » similaire à celle provoquée par l'informatisation et l'émergence des « *Electronic Communication Network* » des années 1990. Ces réseaux\*, qualifiés de « *monstres institutionnels* », ont mis « *en crise la définition du marché* », obligeant les praticiens à clarifier « *ce qu'est un marché (...) et ce qu'il n'est pas* » (Muniesa 2007, p. 3). De la même manière, les CM s'apparentent à des « *monstres monétaires* », forçant les praticiens à reconsiderer leurs catégories et leurs contenus et à préciser ce qu'est ou non une monnaie. La citation suivante d'E. Assouan (2018) de la Banque de France offre un bon condensé de la relégation des CM effectuée par les professionnels de l'argent : « *les crypto-actifs\*, parfois nommés à tort cryptomonnaies\*, ou monnaies virtuelles, désignent le Bitcoin et d'autres jetons virtuels utilisés pour spéculer et pour réaliser certains achats [...]. La Banque de France préfère parler de crypto-actifs\* plutôt que de monnaie. Une véritable monnaie, comme l'euro, est une unité de compte universelle et est acceptée par tous les commerçants, car sa valeur est garantie. À l'inverse personne ne garantit la valeur de Bitcoin, qui ne cesse de fluctuer, et personne n'est obligé de l'accepter en paiement. Les crypto-actifs\* ne sont pas plus illégaux que des jetons de casino par exemple, mais comme ils offrent un total anonymat à leurs détenteurs, ils peuvent être utilisés de façon privilégiée pour financer des activités illégales* » (Assouan 2018).

#### **Des objets non couverts par les catégories juridiques et empiriques de la monnaie**

Les espaces monétaires nationaux sont aujourd'hui des espaces juridictionnels souverains, qui se sont structurés sur le temps long, à la fois hiérarchiquement et territorialement, concomitamment aux développements des États-nations (Cohen 1998; Emily Gilbert et

Helleiner 1999; Helleiner 2003). Les catégories réglementaires de la monnaie et de ses formes (fiduciaire, scripturale, électronique, publique/privée, etc.) sont explicites et formelles, et relèvent de cette souveraineté. L'articulation des monnaies étrangères au niveau international et la question des relations entre autorités monétaires dépendent d'une activité très encadrée, qui s'est internationalisée (sur la construction historique de l'"*International Central Banking*", voir Feiertag et Margairaz 2012). Cette activité repose sur des accords et mécanismes de coopération multi ou bilatéraux (mécanisme de *swap*, etc.) et vise à renforcer leurs relations et expertise, afin de contribuer à la stabilité monétaire et financière mondiale. Ce cadre juridique et administratif, complexe et hiérarchisé, établit d'un même coup le périmètre des objets, des acteurs et des comportements que les autorités monétaires visent à réguler, comme les fins et moyens de cette régulation. Ici Bitcoin, Ethereum et leurs UCN\* n'entrent définitivement pas dans le cadre retenu par la majorité des États et de leurs administrations.

Dans l'Eurosystème dont relève la France, la monnaie *au sens étroit* correspond à la base monétaire (ou *High PoW\*er Money*) émise par la Banque centrale, à laquelle s'ajoutent les dépôts à vue émis par les banques de second rang (European Central Bank 2015a). La base monétaire contient les monnaies dites fiduciaires (les pièces et billets<sup>230</sup>), pour nous moyens de paiement manuels<sup>231</sup>, et des formes scripturales (cf. les réserves détenues par les institutions financières et monétaires – IFM - auprès de la Banque centrale). Les monnaies manuelles, émises par l'autorité souveraine et ses représentants (la Banque centrale et le réseau\* des banques centrales nationales au sein de l'UEM), jouissent d'un statut particulier bénéficiant d'un cours légal et forcé : elles ne peuvent être refusées<sup>232</sup>. À cette base monétaire s'ajoutent les monnaies scripturales et la monnaie électronique, dernières formes à avoir été reconnue<sup>233</sup>. Les monnaies scripturales inscrites dans les registres bancaires reposent sur des émetteurs privés reconnus, surveillés et régulés. Leur circulation est assurée par des moyens de paiement comme les virements ou les chèques. Ces monnaies scripturales et électroniques ne bénéficient pas du cours légal et forcé, et sont acceptées par choix. Ces formes prises ensemble constituent

<sup>230</sup> Les montants maxima fixés pour un paiement dans la zone euro sont : cinquante pièces (quelles que soient leurs valeurs) et jusqu'à 1 000 euros pour les billets (European Central Bank 2015b, p. 22).

<sup>231</sup> Cette catégorie des monnaies manuelles qualifie les moyens de paiement qui circulent de main en main. Comme Blanc (2009a, p. 1), nous la préférons à celles communément mobilisées des monnaies fiduciaires et divisionnaires, car toute monnaie est par essence fiduciaire, imposant de ne pas réduire la fiduciarité à certains types de moyen de paiement puisqu'aucun n'en est dénué.

<sup>232</sup> En France, l'article R642-3 du Code pénal prévoit une sanction en cas de refus d'acceptation de pièce et billet libellés en monnaie légale. Des exceptions existent pour les billets de valeur faciale importante : le débiteur a l'obligation de faire l'appoint (article L. 112.5 du Code monétaire et financier) et le commerçant peut refuser, si tant est que ce refus soit fondé sur un « principe de bonne foi » (il ne dispose pas d'espèces suffisantes, par exemple, Journal Officiel de l'Union Européenne 2010).

<sup>233</sup> Les « monnaies électroniques » apparues en 1990, dont Monéo en France (aujourd'hui suspendue), sont les dernières innovations monétaires à avoir été reconnues légalement, au prix d'une épreuve d'explicitation au long cours (cf. section II.3.1) : ni matérielles (comme les monnaies manuelles), ni dépendantes « d'un compte de dépôts, lors de leur usage courant (hors recharge) [et d']écriture des opérations individuelles sur un compte courant » (comme la monnaie scripturale), elles ont soulevé « des questions économiques, fiscales, sociétales... » nécessitant « une réglementation particulière » (Sitruk 2008, p. 2). La BCE reconnaît que « la réglementation est en retard de quelques années sur les développements technologiques [comme ce fut] le cas [pour les] systèmes de monnaie virtuelle (du moins sous leur forme actuelle) » (European Central Bank 2015b, p. 44). Les monnaies électroniques seront finalement définies par l'article L315-1 du Code monétaire et financier transposant l'article 2.2 de la directive 2009/110/CE : monnaies stockées sous forme électronique, y compris magnétique ; représentant une créance sur un émetteur reconnu, les établissements de monnaie électronique (dont le statut est créé pour l'occasion) ; elles doivent être acceptées par une personne physique ou morale autre que l'émetteur (Ibid. ; Sitruk 2008). Émises contre remise de fonds aux fins d'opérations de paiement de faible montant, elles sont circonscrites à l'espace national (Sitruk 2008, p. 2 et 6).

formellement l'euro<sup>234</sup>. Le cours légal et forcé est le privilège des monnaies relevant de l'émetteur public souverain et de ses représentants ; les monnaies scripturales et électroniques relèvent d'entités privées à statuts spécifiques. Ces entités sont juridiquement reconnues, encadrées et supervisées par les autorités monétaires compétentes. Les monnaies nationales reposent sur une architecture bancaire et financière hiérarchique, au sommet de laquelle la Banque centrale, suivant une institutionnalisation lente et heurtée (Cohen 1998; Emily Gilbert et Helleiner 1999; Helleiner 2003; Feiertag et Margairaz 2012). Au prisme de ces définitions, les CM apparaissent d'abord comme des monstruosités monétaires. De fait, leurs *UCN\** ne sont pas de la monnaie nationale, mais elles ne sont pas non plus des devises étrangères : ni des dépôts, ni des créances détenues sur une personnalité tierce (physique ou morale)<sup>235</sup>. Dès lors, aucun banquier central avec qui négocier.

### **Statut réglementaire des CM : non-qualification, disqualification et requalification**

À côté de ces définitions légales, les autorités monétaires en ont développé d'autres, empiriques et statistiques, dans lesquelles les CM s'intègrent également difficilement (Kubát 2015, p.411). Ces éléments définitionnels, mélanges pratiques d'arguments empruntant aux corpus monétaires instrumental et nominaliste précédents, visent à leur permettre de suivre et de réguler des relations entre l'évolution quantitative de la monnaie (représentées sous forme d'agrégats monétaires) et certaines variables macroéconomiques considérées comme importantes (voir encadré n°3 suivant).

---

<sup>234</sup> Les pièces et billets, la monnaie scripturale et la monnaie électronique sont des « fonds » comme définis par l'article 4.15 de la directive 2007/64/EC (European Central Bank 2015, p.24 note 55).

<sup>235</sup> La BCE (2015, p. 43-45) reconnaît que les CM n'entrent ni dans la directive sur la monnaie électronique (2009/110/EC), ni dans celle sur les services de paiement (2007/64/CE) puisqu'elles n'offrent ni contrepartie sous forme de dépôt, ni émetteur reconnu et qu'elles excèdent l'espace national.

### Encadrés n°3 : Définition empirique et conventionnelle de la monnaie et ses agrégats.

Les autorités monétaires doivent analyser l'évolution quantitative de la monnaie et des instruments de crédit en circulation afin d'estimer et de réguler leurs effets sur certaines variables macroéconomiques (l'inflation, la croissance, etc.). Pratiquement, elles distinguent les actifs monétaires en circulation des autres actifs financiers (au sein d'agrégats monétaires) suivant un critère de liquidité, où l'étalon de la liquidité parfaite est joué par la monnaie légale, elle dont la circulation est garantie par le statut public et souverain de l'émetteur. Le concept de masse monétaire (au sens large) saisit ce qui relève de « la monnaie » et contient les actifs réputés les plus liquides (en rouge dans le schéma). En sont exclues les « créances » financières dont le degré de liquidité est plus faible (cf. immobilisation à moyen ou long terme, en bleu). Cette séparation conventionnelle reste dépendante du degré de proximité à la fongibilité absolue retenue : avec l'apparition d'innovations, la forme et les caractéristiques des actifs financiers ou moyens de paiement évoluent. Certains objets voient leur liquidité s'accroître et la ligne de démarcation entre les moyens de paiement et les actifs financiers est poreuse, particulièrement lors de phénomènes d'euphorie financière où le nombre de produits d'investissement facilement convertibles en moyens de paiement liquides augmente (Kindelberger 2004, p. 65). D'où des définitions différentes d'agrégats monétaires, suivant un éventail d'outils et d'instruments évolutifs (les hachures de M3 soulignent que la définition et l'inclusion dans la masse monétaire au sens large diffèrent suivant la BC considérée).

Le bilan consolidé du secteur des *Institutions Financières Monétaires* est au fondement de la définition des agrégats monétaires de la zone euro. Il relève de convention et, comme le rappelle la Banque centrale européenne, « les définitions de la BCE des agrégats monétaires de la zone euro sont basées sur une définition harmonisée du secteur émetteur de monnaie et du secteur détenteur de monnaie, ainsi que sur des catégories harmonisées d'engagements des IFM. Le secteur émetteur de monnaie comprend les IFM résidant dans la zone euro. Le secteur détenteur de monnaie comprend toutes les non-IFM résidentes de la zone euro à l'exclusion du secteur de l'administration centrale » (European Central Bank 2015).

Au niveau européen, la masse monétaire est mesurée par M3, ce qui recouvre :

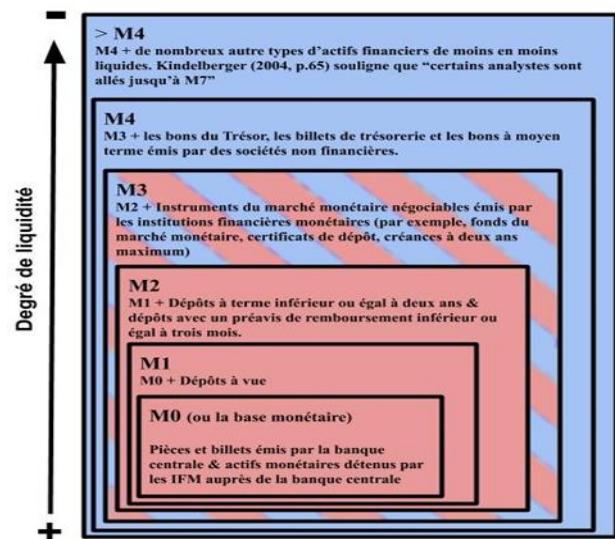
- M0 : contient la « base monétaire », soit les pièces et les billets émis par la banque centrale et les réserves détenues par les IFM auprès de la banque centrale. Elle correspond aux formes monétaires les plus liquides.

- M1 : La monnaie au sens étroit pour l'Eurosystème, elle contient, en plus de M0, les dépôts à vue dans les banques de second rang, et est immédiatement convertible en monnaie.

- M2 : Contient, en plus de M1, les dépôts à termes d'une durée inférieure ou égale à deux ans ou remboursables avec un préavis inférieur ou égal à trois mois. Si ces dépôts peuvent être convertis en composantes de monnaie au sens étroit, certaines restrictions existent (notification préalable, pénalités et frais divers) impliquant certains degrés d'illiquidité.

- M3 : Contient, en plus de M2, certains instruments négociables émis par les *Institutions Financières Monétaires* résidentes, dont la durée est inférieure ou égale à deux ans (ex. titres d'OPCVM monétaires, titres de créance, etc.). Comme pour M2, ces actifs, plus illiquides que ceux contenus dans la monnaie au sens étroit, disposent cependant d'un degré élevé de liquidité et d'une certaine stabilité de prix, qui en fait de proches substituts des dépôts.

Le schéma ci-dessous synthétise les différents agrégats monétaires, en séparant : **(i) en rouge, les actifs monétaires et (ii) en bleu, les actifs financiers**. L'agrégat M3 est hachuré afin de souligner que d'une banque centrale à l'autre, ce ne sont pas les mêmes agrégats monétaires qui sont retenus pour évaluer et réguler l'évolution de la masse monétaire.



Source : Rolland Maël

Les CM s'intègrent difficilement dans un tel cadre. En son sein, les UCN\* des CM sont considérées comme des titres renvoyant à des émetteurs privés et en aucun cas comme de la monnaie renvoyant, elle, à un émetteur public souverain. Pourtant, d'un autre côté, leurs UCN\* jouissent d'un degré de liquidité bien plus important que beaucoup de produits financiers : elles

peuvent être utilisées en propre pour des paiements « rapides » chez des acteurs économiques qui les acceptent (à la manière des moyens de paiement contenus dans M1) ou de manière indirecte, pour être converties en monnaie nationale, au prix de délais courts et du paiement de frais de transaction\* relativement modiques, sur des places d'échange ouvertes 24h/24, 7jours/7 et 365 jours par an (s'approchant ici des moyens de paiement contenus dans M2). En outre, par leur conception, les CM apparaissent comme à l'opposé de la gestion qu'opèrent ordinairement les acteurs du système hiérarchisé. Outre le fait que le monnayage programmatiquement inélastique ne laisse que peu de place aux activités quotidiennes réalisées par les banques centrales afin d'adapter leurs politiques monétaires, Kubát (2015, p.411) souligne d'autres étrangetés : si la masse monétaire en circulation est facilement auditable, cela ne signifie pas que toutes les UCN\* visibles dans le registre\* soient actives et dépensables, puisqu'un certain nombre d'entre elles est à jamais irrécupérable<sup>236</sup> (donc hors circulation) du fait de perte d'accès (destruction/perte de clefs privées). Une telle situation est inconcevable dans le système monétaire où la banque centrale est censée avoir la maîtrise des canaux monétaires et financiers. Dans ce sens, les banquiers centraux ont à leur charge de renouveler les monnaies manuelles perdues et détériorées, et l'accès à un compte courant peut être réclamé (en cas de décès du propriétaire, par exemple), ainsi l'argent détenu n'est jamais vraiment inactif (*Ibid.*). Mais à cette différence s'en ajoute une autre : si l'*« on ne peut pas dire combien de bitcoins sont réellement utilisables dans l'économie »* (*Ibid.*), la transparence des registres\* facilite l'évaluation, tant des montants d'UCN\* perdus que de la vitesse de circulation de celles qui se meuvent, là où, pour la monnaie légale, ces évaluations sont plus délicates à effectuer.

Les difficultés à intégrer les CM dans les définitions et catégories existantes furent tôt reconnues par les autorités monétaires, bancaires et financières - particulièrement les banques centrales – comme par certaines administrations. Leurs caractéristiques questionnent : « *s'il semble admis qu'il ne s'agit pas d'une monnaie au sens du code monétaire et financier, s'agit-il : d'un bien (comme de l'or) ? d'un service ? Dans ce cas, s'agit-il d'un service régulé, comme un service de paiement ou de monnaie électronique, ou d'un service d'investissement ?* » (Mariani et Marc 2014, p. 28). Relevant d'infrastructures et d'objets-frontières, elles induisent différents points de vue suivant la position relative de l'observateur (Star 1999; Trompette et Vinck 2009), expliquant la visibilité de l'épreuve d'explicitation qu'elles imposent aux différentes autorités monétaires. Suivant les acteurs (BC, autorité de régulation des marchés, administration fiscale, etc.) et « *faute de réglementation actuellement plus précise* », « *la qualification des monnaies virtuelles peut être considérée au regard de différentes branches du droit qui peuvent entrer en conflit* » (Mariani et Marc 2014, p. 28). Les CM obligent ces autorités à établir des qualifications et des appellations *ad hoc* (non forcément congruentes) afin d'adapter leurs régulations. Tôt intéressées par l'émergence des CM, ces autorités ont développé une littérature grise sous la forme de rapports ou notes d'information<sup>237</sup>. Ce n'est que tardivement qu'elles ont amorcé un processus (encore en cours) de requalification réglementaire de ces objets. Initialement, leurs prises de position étaient ballotées entre, d'un

<sup>236</sup> Kubát (2015, p. 411) mobilise l'exemple célèbre de James Howells qui cherche à retrouver un disque dur, contenant son portefeuille\* utilisé pour miner un grand nombre de BTC, dans une décharge publique depuis 2013 et ce, par tous les moyens possible (Steven Morris 2021). Nombreux sont les exemples de ce type (Sedgwick 2019m) et, pour Bitcoin, certaines évaluations qui ont été réalisées établissent qu'environ 3,7 millions de BTC, soit près de 20% du total, auraient été à jamais perdus (Chainalysis Team 2018; Chainalysis Team 2020).

<sup>237</sup> Voir pour la France et l'Eurosystème : ministère de l'Économie et des Finances (2011) ; European Central Bank (2012) ; Banque de France (2013) ; Mariani et Marc (2014) ; ministère de l'Économie et des finances (2017); ministère de l'Économie et des Finances (2019a); ministère de l'Économie et des Finances (2019b). Pour les États-Unis, Department of the Treasury (2013); The Internal Revenue Service (2014). Les premiers papiers de recherche, publiés au sein des pôles recherche des banques centrales (Ali et al. 2013; Lo et Wang 2014; Velde 2013), ont été rangés dans la littérature académique suivant ce statut particulier.

côté, une absence de qualification (soulignant leurs incertitudes et les difficultés à les rapporter à leurs catégories monétaires) et, de l'autre, une disqualification pure et simple (pour non-congruence aux catégories existantes). Au départ, les publications des autorités monétaires se limitaient à donner des informations générales sur Bitcoin et les CM, insistant sur leurs risques. Elles étaient l'occasion de conseils et d'appels à la prudence lancés aux utilisateurs – existants et potentiels. Ces informations furent suivies d'une reconnaissance explicite du fait que les CM ne correspondaient (sauf exception légale) « à aucune qualification au regard de la réglementation bancaire et financière en vigueur » : « il ne s'agit pas d'instruments de paiement au sens du c) de l'article L. 133-4 du Code monétaire et financier ; - de même, la qualification de monnaie électronique ne saurait être retenue, les monnaies virtuelles ne représentant pas une créance sur l'émetteur et n'étant pas émises contre la remise de fonds, au sens de l'article L.315-1 du Code monétaire et financier ; - ces monnaies virtuelles ne rentrent pas, enfin, dans la catégorie des instruments financiers dont la liste est définie à l'article L. 211-1 du Code monétaire et financier (à cet égard, il est à noter que l'Allemagne a (...) rangé les monnaies virtuelles parmi les instruments financiers ; il s'agit de la seule juridiction à l'avoir fait à notre connaissance). » (*Ibid.*, p. 29). De nos jours, plus de dix ans après leur apparition, les CM « n'ont [toujours] pas (...) de statut légal explicite et leur encadrement par les pouvoirs publics reste embryonnaire » (Bercy Infos 2020) et parfois contradictoire, comme le souligne le cas allemand. Au niveau européen, la Banque centrale européenne a qualifié primitivement les CM de « Virtual Currency Scheme » (VCS, European Central Bank 2012, 2015) et les a définies négativement comme « des représentations de valeur, non émises par une banque centrale, une institution bancaire ou un institut d'émission de monnaie électronique, et qui, dans certaines circonstances, peuvent être utilisées comme des alternatives à la monnaie » (Banque centrale européenne, 2015). Ce qualificatif n'est ni unique, ni partagé par les différentes administrations participant à l'écheveau institutionnel du système monétaire traditionnel. Elles peuvent être regroupées sous l'appellation de « crypto-actif\* », de « monnaie digitale\* » ou « virtuelle », voire dernièrement de « cyber-monnaie » (appellation conseillée par l'État français, au travers de la commission pour l'enrichissement de la langue en 2017). Ces appellations disparates renvoient à des classifications hétérogènes et contradictoires. Après les avoir considérées comme des biens, les autorités monétaires les traitent aujourd'hui comme des actifs financiers, alors même que la Cour de Justice de l'Union Européenne (2015) leur a reconnu le statut de moyen de paiement<sup>238</sup>. Sur le plan fiscal, si les CM entrent dans le champ de la déclaration et l'imposition des plus-values spéculatives, les administrations peinent à

<sup>238</sup> Suivant un différend entre l'autorité fiscale suédoise et la bourse d'échange « Bitcoin.se », la Cour de Justice de l'Union européenne a statué (arrêt de principe du 22/10/2015) que cette activité relevait de l'exonération de la TVA au titre de l'Article 135, § 1 de la directive 2006/112 encadrant les opérations de change, reconnaissant ainsi aux UCN BTC le statut de monnaie (voir <https://bitcoin.fr/le-bitcoin-exonere-de-tva/> [consultation au 05/12/2016]). Avant, les UCN de CM pouvaient être considérées à la fois comme : « une unité de mesure monétaire [...] sous forme électronique [circulant] au sein d'une communauté d'acteurs » ; « Au regard du droit civil [...] comme un bien meuble incorporel valorisable, utilisé comme outil spéculatif, plus précisément d'un bien meuble par détermination de la loi, car il ne peut rentrer dans la catégorie des biens immeubles définie aux articles 517 à 526 du Code civil » ; mais « au regard de certaines dispositions législatives, les monnaies virtuelles ne paraissent pas pouvoir être assimilées à une marchandise ou à une matière première [...]. La DGDDI relève qu'il serait intéressant de considérer certaines de ces monnaies virtuelles [...] comme un bien similaire à l'or, ce qui permettrait à la douane d'être compétente en termes de contrôle des transferts de capitaux ou de les classer sous une même appellation d'"instrument de paiement" [...]. Toutefois, cette seconde option risquerait d'entraîner une confusion avec les moyens de paiement encadrés par le code monétaire et financier » ; à une « mesure financière » – au sens de l'article D.211-1 A 1 du code monétaire et financier – pouvant servir de support à des contrats financiers ; à « un bien assimilable à un « bien divers » au sens de l'article L.550-1 du code monétaire et financier ; « à des « indices » au sens de l'article L. 465-2-1 du code monétaire et financier, ce qui conférerait à l'AMF une compétence en termes de sanction vis-à-vis d'éventuelles manipulations de marché » (Mariani et Marc 2014, p. 28-30).

établir un cadre précis, homogène et stabilisé (voir Direction Générale des Finances Publiques 2014; Ministère de l’Économie et des Finances 2019). Depuis 2019, les CM ne relèvent plus du régime des cessions des biens meubles (article 150 UA ; Légifrance 2018) et sont dorénavant soumises à un régime propre (article 150 VH bis ; Légifrance 2019). L’élaboration de ces cadres légaux est un processus dynamique et négocié, non encore achevé<sup>239</sup>. Les autorités compétentes ont encore à préciser le statut qu’elles donnent à ses objets, et ce faisant, les réglementations et régulations qui pèseraient sur eux, comme sur les acteurs qui en usent<sup>240</sup>.

Les corpus théoriques sur lesquels prennent appui les critiques recensées, par-delà leurs différences, partagent un fond commun : l’argent et la monnaie y sont conçus comme homogènes, unitaires et exclusifs. Notre thèse est qu’il est possible de relâcher l’une et l’autre de ces caractéristiques conventionnelles (relevant d’hypostases situées) tout en conservant la qualification de monnaie. À ce titre, nous affirmerons contre ces vues que les CM sont monnaie.

## II.2 « POURTANT, ELLES FONT MONNAIE » ! À L’AUNE D’UN NOMINALISME « NON ÉTATISTE » ATTENTIF AUX USAGES

De notre point de vue, l’un des obstacles à la reconnaissance du statut monétaire des CM tient à « *l’incapacité des analystes à s’abstraire de ce qu’ils connaissent déjà : la monnaie bancaire, unitaire et centralisée, garantie en dernier ressort par l’État. Or, Internet et les cryptomonnaies\* remettent en cause cette conception traditionnelle de la monnaie et interrogent la théorie sur sa capacité à penser leur spécificité.* » (Desmedt et Lakomski-Laguerre 2015, p. 2-3). En ce sens, ni la théorie instrumentale et substantielle de la monnaie, ni l’approche « chartaliste » ne permettent de cerner pleinement le phénomène des CM. Elles partagent un même tropisme qui fait des caractéristiques de la monnaie moderne le fondement indépassable de leur définition de la monnaie. Elles ont en commun de penser l’argent au prisme de sa capacité à porter parfaitement les fonctions monétaires canoniques, et ce, au sein d’un espace économique conçu comme unitaire et exclusif grâce à un centre souverain réifié. Mais ces approches ne sont pas indépassables et continuent d’être controversées dans le champ monétaire. Partir de l’unicité et de l’exclusivité des phénomènes monétaires repose sur deux hypostases imbriquées : l’une conçoit la monnaie du point de vue des systèmes monétaires contemporains et de la centralité que jouent les banques centrales (et de l’État) et l’autre postule que cela produit automatiquement unicité et l’homogénéité. Ces hypostases aux fondements

---

<sup>239</sup> Il y a quelques années, les États s’étant emparés de cette question se divisaient entre : ceux qui cherchaient à les intégrer et à les réglementer (Allemagne, France, Lettonie, Lituanie, États-Unis) et ceux qui souhaitaient les interdire. Au sein de ce deuxième groupe, qui comptait la Russie ou la Chine, des législations sont venues doter les CM de statuts légaux (Huang 2020; Partz 2020a). Parmi les premières tentatives d’intégration réglementaire, citons l’Allemagne qui a reconnu le statut de monnaie privée à Bitcoin afin d’en soumettre les transactions à l’impôt. En septembre 2015, par l’intermédiaire du régulateur des bourses du commerce américain (le CFTC), les États-Unis reconnaissaient à leur tour le Bitcoin. Voir <http://fr.euronews.com/2015/09/18/le-bitcoin-officiellement-considere-comme-un-marchandise/> et <http://www.cftc.gov/index.html> [consultation au 19/12/2016]. La Suisse, qui concentre des entreprises de l’écosystème des CM, apparaît pionnière dans la volonté de développer un cadre réglementaire incitatif. Le Canton de Zoug a d’ailleurs été le premier au monde à accepter le paiement des impôts locaux en bitcoin (cf. Chap. I). Le Japon qui, dans une loi entrée en vigueur le 1er avril 2017, a reconnu le bitcoin et d’autres CM comme des moyens de paiement légaux, tout en renforçant les exigences de transparence et de solidité financière des opérateurs du marché local (AFP 2018).

<sup>240</sup> Par exemple, en France, la dernière loi en date du 22 mai 2019 (Loi 2019-486, art. 86), dite « PACTE », a créé, dans le Titre IV du Livre V du Code monétaire et financier, le Chapitre X, qui définit les « Prestataires de services sur actifs numériques ». Cette loi pose les jalons d’une réglementation concernant les « actifs numériques » et les acteurs de cet écosystème (Abraham 2020).

des critiques des CM relèvent d'un présentisme *ahistorique* contrefactuel, au mépris d'une histoire passée et présente : cette situation contemporaine, résituée dans le temps long, n'est pas tant la règle que l'exception (Cohen 1998; Emily Gilbert et Helleiner 1999; Helleiner 2003; Blanc 1998a; Viviana A. Zelizer 1999; Steiner 2007; Polanyi 2011; Doepeke et Schneider 2017). Aucun instrument, d'hier ou d'aujourd'hui, ne porte parfaitement les fonctions canoniques de la monnaie, et l'exclusivité cache toujours une pluralité de monnaies et de communautés de paiement/groupes monétaires qui, grâce à ces monnaies, peuvent se relier et échanger. Il existe aussi des monnaies en dehors du giron étatique. Les difficultés rencontrées pour qualifier les CM rappellent celles soulevées par les monnaies parallèles (Blanc 1998a). Aux approches instrumentale et chartaliste, on peut opposer des cadres théoriques et méthodologiques plus hétérodoxes, qui permettent de reconnaître aux CM une dimension proprement monétaire. Des courants plus libéraux (libertarianisme, *free banking*, etc.), malgré leur adhésion à la vision marchande et instrumentale de la monnaie, théorisent ainsi que la présence de l'État est moins nécessaire que superflue (quand elle n'est pas le problème monétaire premier). D'autres courants nominalistes « non étatiques », comme l'institutionnalisme monétaire francophone dans lequel nous nous inscrivons<sup>241</sup>, permettent ainsi de penser la monnaie autrement. Ce dernier courant conserve la vision d'une monnaie fondée dans la règle, par nature collective et politique, mais n'envisage pas l'État comme toujours essentiel, ni ne considère que l'argent a porté, partout et toujours, les fonctions monétaires canoniques. Il est ainsi possible de voir dans les CM une chimère monétaire, mi-monnaie marchandise, mi-monnaie dette (J.P Koning 2012; Selgin 2013; Andri Olafsson 2014; Beat Weber 2014b), et de considérer que cette hybridité n'est plus rédhibitoire à leur qualification de monnaie : au contraire, elle permet de conceptualiser une nouvelle catégorie.

Nous verrons qu'il est possible de mobiliser différemment les critères monétaires dominants tout en émancipant la monnaie du critère d'exclusivité étatique (II.2.1). Ensuite, nous expliciterons les grandes lignes, les concepts et arguments clefs de l'institutionnalisme monétaire qui nous permettent d'affirmer que rien ne s'oppose à ce que les CM soient reconnues comme des monnaies (II.2.2). Une fois posé ce décor théorique, il deviendra possible d'y intégrer nos objets pratiques et de contester tant l'exclusivité monétaire postulée par les critiques chartalistes que l'unicité des critiques instrumentales (II.2.3).

### **II.2.1 Des chimères monétaires inédites, reléguées à des usages spéculatifs**

Des auteurs venant d'écoles et de corpus théoriques pourtant concurrents ont souligné le caractère hybride des CM (Koning 2012; Ali et al. 2013; Selgin 2013; Andolfatto 2013; J.P Koning 2019c). Plutôt que de chercher à les fondre dans des catégories existantes mal taillées pour elles, ces approches ont conduit à mettre à jour des dimensions proprement monétaires des CM et d'établir les contours d'une catégorie monétaire inédite. Néanmoins, pour ces auteurs, elles n'en sont pas moins conçues comme relevant de « mauvaises » monnaies<sup>242</sup> (Andolfatto 2013; Selgin 2014b; Koning 2018a). Ces analyses franchissent toutefois une étape vers la reconnaissance du statut monétaire des CM, puisqu'il faut « *que ce soit de la monnaie*

<sup>241</sup> Précisons que si, comme nous, certains auteurs affirment le caractère monétaire des CM depuis un même positionnement institutionnaliste (De Filippi et Loveluck 2016; Dodd 2017; Orléan 2019), cela n'a rien d'automatique, comme nous l'ont prouvé les mises en garde théoriques (Dupré, Ponsot et Servet 2015) et pratiques (lors de certains colloques, introduction générale) déjà évoquées. Le conflit normatif et symbolique qui oppose les *coiners*\* aux économistes a échaudé tout le monde, et pourrait d'ailleurs recouvrir en partie des animosités plus personnelles consécutives à des face-à-face, plus que houleux, entre certains de ces auteurs et des *bitcoiners*\* [Entretien SuperAnon, Annexe n° IV.4].

<sup>242</sup> Référence au titre du billet d'Andolfatto (2013) intitulé « Why gold and bitcoin make lousy money ».

*pour que ce soit de la mauvaise monnaie* »<sup>243</sup> (Knapp 1924, p. 1). Elles rejoignent cependant le concert de critiques qui n'y voient finalement que des actifs financiers spéculatifs.

### Les CM : des chimères monétaires inédites... de mauvais aloi

Les théoriciens contemporains du *free banking* G. Selgin (2013; 2014) et L. H. White (White 2018; White 2020) comptent parmi les auteurs libéraux s'étant intéressés aux CM. Nous avons déjà croisé ces auteurs, car ils participèrent à la liste de diffusion « *Libtech-1* », créée par Szabo en 1994 (McCormack et Szabo 2019; Lars 2020; cf. Chronologie 1, Chap. I.1.1). Selgin part du constat de l'hybridité inédite des CM : celles-ci, en effet, « *impliquent des caractéristiques à la fois de la monnaie marchandise et de la monnaie fiduciaire, telles qu'elles sont généralement définies, sans correspondre à la définition conventionnelle de l'un ou l'autre type* »<sup>244</sup>. Les CM empruntent selon lui aux premières leur « rareté absolue », mais s'en distinguent par leur absence d'usage non monétaire et leurs coûts moindres relativement aux monnaies métalliques (Selgin 2012, p. 4). Cette dernière caractéristique les rapproche des fiat monnaies, alors même que leur rareté absolue les y oppose (Selgin 2014b, p. 5-6). Ces caractéristiques hybrides définissent une nouvelle catégorie monétaire : celle de « *monnaie marchandise synthétique* »<sup>245</sup>.

Malgré cette reconnaissance, les CM sont jugées comme n'étant pas « *idéales* », car trop imparfaites. Au grand dam de *coiners\**, qui faisaient du *free banking* leur étandard théorique et qui voyaient en Selgin « *la drogue idéale pour accéder à Bitcoin* » (« *the perfect gateway drug to Bitcoin* », Farrington 2021), voilà que ce dernier, comme l'ensemble des autres commentateurs, voit l'inélasticité du monnayage des CM comme Bitcoin être fondamentalement problématique. S'il suggère « *qu'un régime monétaire synthétique de matières premières pourrait être plus performant que les régimes de monnaie fiduciaire existants* », cela renvoie à un système où l'offre monétaire reste élastique (Selgin 2014b). L'erreur des *bitcoiners\** c'est de « *compar[er] le bitcoin à l'or en tant qu'actif d'investissement* », là où « *les économistes, en revanche, s'intéressent davantage à la comparaison entre un système monétaire basé sur le bitcoin et un système monétaire basé sur l'étalement-or.* » (White 2018). Des « *similitudes et [d]es différences entre le système bitcoin et l'étalement-or* », ces auteurs retiennent surtout les « *différences [de] mécanismes d'approvisionnement* » qui à l'instar des *bitcoiners\** sont peu appréciés, puisqu'ils impliquent une dynamique déflationniste problématique (*Ibid.* ; Selgin 2014b). Si les CM s'imposaient comme système monétaire, leur dynamique d'offre limitée, couplée à une demande et à une vitesse de circulation des UCN\* très volatile, conduirait à une instabilité du niveau général des prix comme du niveau de dépenses nominales, avec un phénomène de thésaurisation incité par l'appréciation de leur prix (Selgin 2014b; Selgin 2014a; White 2018). Finalement, de leur point de vue et contrairement à celui des *coiners\**, les CM peineront à jouer le rôle d'instrument de

---

<sup>243</sup> Dès l'introduction de son ouvrage célèbre, Knapp (1924, p. 1) rappelle que, même à voir les papiers monnaies comme de « *mauvaises monnaies* », toute théorie monétaire se doit de les intégrer, car, « *Money it must be, in order to be bad money* ».

<sup>244</sup> La distinction établie par Selgin entre les monnaies marchandises et les fiat monnaies relève de deux critères : le premier, dans la lignée des théories instrumentales, renvoie à l'existence ou non d'usage non monétaire ; le second renvoie à la rareté (« *scarcity* ») qui peut être « *absolue et naturelle* » comme pour les matières premières, ou contingente. (Selgin 2013, p. 5). Dans ce sens, « *contrairement aux formes de monnaie couramment utilisées [...], les monnaies numériques ne constituent pas une créance sur qui que ce soit [et] peuvent donc être considérées comme un type de marchandise*. Mais à la différence des marchandises physiques comme l'or, elles sont aussi des actifs intangibles, ou des marchandises numériques » (Ali et al. 2013, p. 3).

<sup>245</sup> Entre son article de 2012 et celui de 2014, qui est une réédition légèrement modifiée, Selgin passe de l'appellation « *Quasi-commodity money* » à celle de « *Synthetic commodity money* ».

réserve de valeur du fait de leur instabilité : les CM ne seront « *pas susceptible[s] de remplacer le dollar* », car « *un système monétaire basé sur le bitcoin pourrait s'avérer incompatible avec la stabilité macroéconomique* » et il est « *peu probable* » « *que le bitcoin devienne un jour un moyen généralement accepté et largement utilisé pour les paiements quotidiens, c'est-à-dire de l'"argent"* » ou « *une "monnaie"* » (Selgin 2013, p. 23-24)<sup>246</sup>.

### Des critiques paradoxales et syncrétiques, confinant les CM au rôle d'actif financier

Force est de constater que les critiques précédentes « *manque[nt] de clarté* », voire entretiennent « *une réelle confusion* » sur les CM, en particulier « *au sein de la discipline économique* » (Desmedt et Lakomski-Laguerre 2015, p. 2). La dimension paradoxale des critiques précédentes pointe selon nous les limites des appareillages théoriques qui les fondent. En l'absence de valeur « *intrinsèque* » – n'étant adossées à aucune marchandise –, les CM ne seraient pas des monnaies, à l'image des monnaies de papier qui, à l'époque de leur émergence, susciteront la méfiance de nombreux analystes qui y voyaient une pure « *escroquerie puisque cela ne repose sur rien* » ((J Adams cité par John Kenneth Galbraith 1976, p. 58). Mais ces raisonnements inscrits dans les visions « *substantielles* » de l'argent ne sont pas satisfaisants, car ils pourraient exclure les monnaies modernes de crédit, non convertibles en métal, et il n'est pas sûr que les auteurs mobilisant cette critique soient satisfaits de côtoyer des « *gold bugs* », qui condamnent l'apparition des fiat monnaies et la remise en cause des convertibilités or des monnaies nationales, au XIX<sup>e</sup> siècle ou après l'effondrement du système de Bretton Woods dans les années 1970. Au prix d'un syncrétisme problématique, certains acteurs, comme Krugman (2018b), parlent des fiat monnaies en mobilisant le concept de valeur intrinsèque, qui recouvre chez eux les régulations et garanties étatiques là où, historiquement, les visions substantielistes s'en servaient pour opposer en nature les « *monnaies marchandises* » aux « *monnaies dettes* », à l'encontre des approches nominalistes qui en défendaient le statut monétaire (de Boyer des Roches et Rosales 2003). Dans un grand écart théorique, l'argument se lie aux arguments « *nominalistes* » dans leur version « *chartaliste* ». De leur « *métallisme digital* » (Maurer et al, 2014 ; Mallard et al, 2018) reposant sur un monnayage déconnecté du crédit et des États, les CM ne seraient pas en mesure de se prévaloir du statut monétaire. Cet argument doit affronter le cas des systèmes métalliques : peut-on en effet soutenir que les monnaies parfaitement convertibles n'étaient pas de l'argent, puisqu'elles n'étaient pas directement liées à l'émission de crédit pur<sup>247</sup>? Ou bien que, hors monopolisation de l'émission monétaire par une banque centrale nationale, point de monnaie ? De nombreuses expériences monétaires en dehors du cadre de l'État-nation et de leur représentant élu ont existé dans le passé (banques centrales et État-nation ne sont que des construits modernes), mais aussi dans le présent (l'euro avec une banque centrale indépendante des États membres, le phénomène de monnaie parallèle, la dollarisation en Amérique latine, le dinar suisse irakien<sup>248</sup>...). Devrait-on en déduire que les moyens de paiement en circulation ne sont pas en monnaie ? Là encore, il n'est pas sûr que les auteurs ayant mobilisé ces arguments chartalistes accepteraient ces conséquences.

---

<sup>246</sup> Voir le fil twitter original : <https://twitter.com/GeorgeSelgin/status/1391723283788308487> [consultation au 03/09/2023].

<sup>247</sup> Cartelier (1996), dans sa théorisation de la monnaie comme système de paiement, pose trois idéaux types de systèmes de paiement à monnayage différent ayant historiquement existé : le « *monnayage métallique pur* », le monnayage « *métallique avec crédit* » (papier-monnaie) et le système contemporain fondé sur le « *crédit pur* » (monnaie papier).

<sup>248</sup> Pour une analyses des limites des approches néo-chartalistes, voir Desmedt et Piégay (2007); sur l'expérience contemporaine du dinar suisse irakien, voir Selgin (2013, p. 13).

Ces différents auteurs critiques venant de courants opposés s'accordent néanmoins sur un argument : les CM constituerait une nouvelle classe d'actifs financiers à haut risque et hautement spéculative. Selon eux, se rejouerait avec les CM une euphorie spéculative à la manière de la « Tulipomania » du XVII<sup>e</sup> siècle<sup>249</sup>. Les CM ne seraient que « *Bulle, fraude et trouble* » (Krugman 2018b), « *une chaîne de Ponzi naturelle* » (Shiller, cité par Krugman 2018b) dont le « *prix tombera à zéro si la confiance disparaît* » (rejoint ici par Shiller, 2018). Il faudrait protéger les investisseurs, car « *cela finira mal, et plus vite ce sera fait, mieux ce sera* » (Krugman 2018b), d'où Stiglitz de proposer d'en précipiter la fin en les interdisant purement et simplement (Stiglitz, 2017). Le chapitre I a montré comment l'usage spéculatif des CM avait été essentiel pour stimuler leur développement infrastructurel. Et il est certain que les CM sont de parfaits « *objets de spéculation* » (Kindelberger 2004, p. 50) : objets innovants ; taux de change flottant soumis aux seules forces du marché ; offre limitée, tant du fait de l'émission protocolaire que de leur degré élevé de thésaurisation et de concentration ; et une demande en croissance constante<sup>250</sup>. Tous les ingrédients sont réunis pour qu'elles fassent l'objet de polarisation mimétique dans la pure logique autoréférentielle d'un « *concours de beauté keynésien* » (André Orléan 1989; Koning 2018b). Mais ces arguments sont-ils rédhibitoires à leur qualification en termes de monnaie ? Même le critique Tirole (2017) le reconnaît : aucune monnaie n'est exempte ni de dimension spéculative (d'où des marchés « *forex* »), ni de dimension autoréférentielle (la monnaie peut être conçue comme objet autoréférentiel par excellence, voir André Orléan 1998; Ingham 2007), ni de volatilité (dont le degré sert de critères pour caractériser les crises économiques et monétaires, cf. inflation, voire hyper-inflation)<sup>251</sup>.

Partant de la dimension spéculative et ludique, élément dont dérive une part importante de leur demande, Koning (2018b; 2018e; 2018c; 2018a; 2019c; 2019a; 2020b) offre une qualification plus fine et nuancée : les CM, Bitcoin en tête, seraient pour partie un nouveau « *type de jeu de paris financiers* », un « *early bird game* » profitant aux premiers entrants (Koning 2019c). Les CM s'opposeraient aux titres financiers traditionnels ou aux moyens de paiement monétaires, qu'il fait entrer dans la famille des jeux à somme positive (« *win-win opportunity* ») auxquels est reconnue une dimension productive : les actifs concernés permettent aux entreprises émettrices de dégager plus de ressources que ce à quoi les détenteurs de titres ont contribué à l'origine, d'où le fait qu'ils génèrent des revenus (dividende ou intérêt). À l'inverse, les CM sont décrétées non productives et sont rangées dans « *la catégorie des paris et des couvertures* », des jeux à somme nulle (pour tout gagnant, il y a un perdant) au même titre que « *les assurances, les contrats à terme et les options, ainsi que divers jeux de hasard comme les loteries* » (Koning 2019c). Il n'empêche qu'une telle demande spéculative n'est pas près de se tarir puisqu'il existerait « *une demande constante de ponzis de la part d'individus volontaires et informés* » (Koning 2018a), ainsi que le prouve l'engouement pour les jeux

---

<sup>249</sup> Il serait difficile de faire une liste exhaustive des articles de presse où de telles critiques ont été formulées, tant par des commentateurs économiques, des praticiens que des économistes. On trouve plus de 2 millions de pages référencées sur Google liant Bitcoin et tulipe (voir <https://www.google.fr/search?q=bitcoin+tulip>). Jacques Javier - membre fondateur du Cercle du Coin, association francophone qui vise, suivant ses statuts, « à l'étude et à la promotion » de Bitcoin et des crypto-monnaies (Le cercle du Coin 2016) – conteste, à raison, la pertinence d'une telle analogie (Favier 2017). Pour s'en moquer, il référence certains grands noms qui mobilisent cet exemple et leur décerne « le prix tulipe » (Favier 2018) [consultation au 11/03/2022].

<sup>250</sup> Nous reviendrons sur les caractéristiques transactionnelles de Bitcoin et d'Ethereum dans notre section II.2.2.

<sup>251</sup> Si, pour Tirole, « *la question de la soutenabilité* » implique de voir Bitcoin comme une bulle et un actif sans valeur intrinsèque, il reconnaît qu'il « *existe indéniablement des bulles qui réussissent et qui durent : l'or (dont la valeur dépasse largement le prix qu'il atteindrait s'il était traité comme une matière première et utilisé à des fins industrielles ou décoratives), ou même le dollar, la livre ou l'euro. [...] Personne ne peut affirmer avec certitude que le bitcoin va s'effondrer. Il pourrait devenir le nouvel or. Mais je ne parierais pas mes économies dessus, et je ne voudrais pas que des banques réglementées jouent sur sa valeur.* » (Tirole 2017)

d'argent de toutes sortes. Cet auteur souligne néanmoins des différences notables avec les pyramides de Ponzi et des « *chain letters* »<sup>252</sup> : l'absence de centralisation caractéristique des pyramides de Ponzi et l'impossibilité de profiter du schème par falsification qui se retrouve dans les *chain letters* avec, pour leurs utilisateurs, une transparence quant à leur règle et leur fonctionnement bien supérieure à ces deux systèmes (*Ibid.*).

Considérer les CM comme actifs financiers n'est certes pas erroné : une monnaie peut tenir le rôle de devise. Son essence monétaire s'évapore alors et elle devient un actif de portefeuille comme un autre. Mais cet usage est réducteur et les confine à un statut qui ne leur est ni premier, ni exclusif. Cette question nous ramène à la prise en compte du degré de liquidité au cœur de la définition empirique de la masse monétaire retenue par les autorités. Un actif qui connaît successivement euphorie et panique voit rarement sa liquidité subsister, comme en témoigne l'épisode des tulipes. Les CM sur ce point apparaissent donc comme des actifs singuliers. La question reste entière : l'inadéquation des CM aux théories monétaires dominantes prouve-t-elle qu'elles ne peuvent prétendre à faire monnaie ? Ou leur existence même ne remet-elle pas en cause la capacité de ces théories à analyser les phénomènes monétaires dans toutes leurs dimensions ? Comme d'autres auteurs qui appellent à renouveler l'approche, nous considérons comme vraie la seconde hypothèse : « *le bitcoin remet en question [les] théories monétaires populaires* » qui « *traitent l'argent comme un nom, et non comme un adjectif* » (Koning 2012). À ce titre, les travaux de Koning (2012; 2013; 2018f; 2018a; 2018b; 2018e; 2019c; 2019a; 2020b) sont intéressants par leur ambivalence. Ils illustrent d'un côté les positions monétaires que nous critiquons mais, d'un autre, ils déploient une approche en termes de « monétisation » parente de la nôtre : l'argent est conçu moins comme une chose renvoyant à des objets que comme un état qualifiant ceux-ci suivant leur degré de monétisation, c'est-à-dire de liquidité<sup>253</sup>. Cet intérêt pour la « monétisation » ouvre sur nos propres problématiques puisqu'il est au cœur de l'institutionnalisme monétaire francophone que nous mobilisons. Présenté en introduction, il nous revient à présent d'en préciser les contours et d'expliquer les deux ensembles argumentatifs qui, transposés aux CM, permettent selon nous de dépasser les critiques précédentes.

## II.2.2 L'Institutionnalisme Monétaire Francophone : un nominalisme non étatique, apte à contenir les CM

Au-delà de leurs socles théoriques différents, les critiques recensées partagent le fait de penser l'argent et la monnaie (quelles que soient leurs formes) comme homogènes, unitaires, centralisés et exclusifs. En cela, elles démontrent une même « *incapacité [...] à s'abstraire de [...] la monnaie bancaire, unitaire et centralisée, garantie en dernier ressort par l'État*une véritable monnaie, comme l'euro, est une unité de compte universelle et est acceptée par tous les commerçants, car sa valeur est garantie », quand le second exige qu'une monnaie soit « *moyen de paiement généralement*

---

<sup>252</sup> Les « *chain letters* », comme les ponzi, correspondent à « *un jeu de lève-tôt, un type de jeu à somme nulle qui utilise l'ordre d'entrée comme règle de redistribution [et comme eux] ils sont illégaux.* » (Koning 2018d)

<sup>253</sup> Koning, auteur iconoclaste aux références hétéroclites, publie sur les CM depuis 2012 sur son blog intitulé « *moneyness* ». Difficilement classable dans les familles d'approches précédentes, il reconnaît explicitement le caractère monétaire des CM au titre de son approche en termes de monétisation. Mais on retrouve dans ses écrits des critiques assez similaires à celles déjà recensées. Conçues univoquement comme actifs financiers de « *type de jeu de paris financiers* » au même titre qu'un « *ticket de loterie* », les UCN des CM peuvent difficilement devenir monnaie, « *ce n'est qu'un jeu* » (Koning 2018c) : « *les bitcoins d'un propriétaire de bitcoin [...] ils sont un rêve, une lambo, un billet de sortie de la corvée. Les dépenser chez un détaillant à leur seule valeur marchande serait du gaspillage, car leur "destin" est de décrocher la lune* » (Koning 2018a)

accepté » sans préciser le périmètre de cette acceptation universelle / générale, ni le comment, ni le par qui il est défini. Et les auteurs qui partent de l'hybridité des CM, bien qu'ils leur octroient un « *certain degré d'argent* », elles sont à leurs yeux de « *mauvais moyens d'échange et [de] réserve de valeur* » (Koning 2018e), selon les fonctions monétaires classiques. Ces critiques, par leur fonctionnalisme, ressassent des représentations instrumentales et marchandes de la monnaie, dont témoignent les références récurrentes aux fonctions monétaires, et la primauté donnée à « *la fonction d'instrument d'échange [...] guidée par la vision d'une monnaie marchandise* » (Courbis, Froment et Servet 1990, p. 13). Ce que traduit l'appellation « *monnaie marchandise synthétique* » de Selgin. Ces critiques convergent sur des visions réifiantes, *aprioristes, ahistoriques et asociales*, au sein desquelles les qualités de « bonne » ou « mauvaise » monnaie sont préjugées de manière exogène, en surplomb des acteurs. Cependant, d'après nous, répondre à la question de « *comment penser l'argent* »<sup>254</sup> impose de se décentrer de la conception classique de la monnaie et de l'étude des caractéristiques fonctionnelles et marchandes des médiums monétaires, qui ne sont ni premières, ni suffisantes. Avec Knapp (1924), nous pensons que se focaliser sur la matérialité de l'objet monnaie relève d'*« une grave erreur »* et ceux qui le font, comme le « *numismate ne [peuvent apprendre grand-chose sur] la monnaie, car [ils n'ont] affaire qu'à son cadavre* » (Knapp 1924, p. 1)<sup>255</sup>. Cet intérêt de « *médecin légiste* », que partagent les critiques précédentes, est incomplet, partiel et partial du point de vue de l'IMF et du nominalisme pur dont il est issu (cf. encadré n°2). D'un autre côté, nous préfèrons à l'approche de Knapp celles de Simmel<sup>256</sup> (2009) ou de Polanyi selon lesquels ni la loi (formelle), ni l'État (qui l'établit) ne constituent les germes uniques et exclusifs de la monnaie. À la manière de Koning, le terme monnaie (et liquidité, dont elle est la forme ultime) est moins pour nous un nom se référant à une chose, qu'un adjectif qui la qualifie : d'où l'usage du terme monétisation. Selon ce prisme, comment ne pas voir que « *les bitcoins ont toujours été une monnaie. Un certain degré d'argent y était attaché dès l'instant où le premier utilisateur de bitcoin a réalisé que ses bitcoins pouvaient être échangés avec un autre utilisateur contre quelque chose d'autre. [...] Si vous traitez l'argent comme un adjectif, le théorème de régression et la théorie des chartes ne sont pas pertinents. Que l'argent soit attaché à un jeton émis par le gouvernement pour acquitter les impôts, ou qu'il soit attaché à un objet précieux à des fins religieuses ou industrielles, est sans importance. Le degré de liquidité - ou de monétarisation - est la variable de l'intérêt* » (Koning 2012). Aucun objet n'est monétaire en lui-même et tout objet peut, dans une situation appropriée, jouer le rôle de monnaie : les caractéristiques matérielles de l'objet monnaie importent moins que les situations où il est utilisé comme tel et pourquoi il l'est.

<sup>254</sup> Titre de l'ouvrage collectif et interdisciplinaire de 1992, auquel participent les auteurs autour desquels se formera le courant de l'IMF et qui participa au renouveau théorique des années 1980-90 dans le champ de la monnaie en France (Blanc 2009b, p. 1).

<sup>255</sup> En rupture avec la conception métalliste et substantielle de la valeur de la monnaie, Knapp établit que, au sein d'une même « *monnaie chartale (les moyens de paiements proclamés)* [on trouve des formes pouvant être] *hylogéniques (monnaie-métal) ou autogéniques (papier-monnaie)* » (Desmedt et Piégay 2007, p. 118) : « *la monnaie n'est pas liée à l'utilisation de métal, [elle est] une création du droit et, en dernier ressort, elle peut continuer à exister même sans métaux* » (Knapp 1924, p. 296). Ainsi, la validité des moyens de paiement est « *indépendante du contenu de la pièce* » puisque « *les dettes exprimées en unité de compte peuvent être acquittées par des pièces gravées, pièces de monnaie ou billets, qui ont, selon la loi, une certaine validité en unité de compte* ». Dans ce cadre, la monnaie relève de la loi et la loi de l'État, donc la monnaie est une institution de l'État (*Ibid.*, p.25 et suivantes).

<sup>256</sup> Schmoller, dont Simmel et Knapp étaient les élèves, était plus proche de la démarche empirique du premier que du second, qui « *construit sa théorie a priori* » procédant « *plus par la logique que par les faits* », postulant d'emblée que « *l'argent [est] une créature de l'État* » (Ehnts 2019, p. 14). Outre « *le compte rendu très positif de Schmoller* » sur l'ouvrage phare de Simmel, Knapp lui-même « *a qualifié le livre [...] de "tissage d'or dans la tapisserie de la vie* » (Frisby 1978, p. xvi-xvii).

## Au-delà de la monnaie, l'argent : questionner la monétisation à l'aune des usages

Ce décentrement marque le renouveau programmatique des années 1980 dans le champ monétaire, impliquant des sociologues, des historiens, des anthropologues, des ethnographes et les économistes institutionnalistes du courant de l'IMF. Ce renouveau, « *concomitant du reflux des théories économiques de la valeur, qui prétendaient expliquer la formation des valeurs économiques par des critères non monétaires* », émerge de la volonté de dépasser les limites de cette approche classique de la monnaie (Blanc 2009b, p. 3) et de son « sens étroit »<sup>257</sup>. À partir d'une même base ethnographique intéressée aux usages et pratiques, ces travaux cherchent à comprendre « *les significations sociales de l'argent, les variations dans les modes et l'étendue de ses usages, ainsi que celles des frontières et des formes de la monnaie par laquelle l'argent existe* » comme « *lien social* » (Blanc 2009a, p. 1). Cette approche théorique remplace la théorie orthodoxe de la valeur utilité / rareté contre une théorie de la valeur monnaie, où la monnaie est essentielle aux coordinations économiques décentralisées, car aucune valeur intrinsèque ne préexiste aux échanges : la médiation monétaire est consubstantielle à l'un et à l'autre et toute valeur est monétaire (et extrinsèque). La monnaie devient cruciale pour comprendre le marché, liant les transactions\* décentralisées (déséquilibres micro) et leurs interdépendances (équilibre macro) dans un contexte d'incertitude radicale et de défaut de paiement (absent de la théorie de la valeur). Ainsi, l'IMF traite l'argent comme un « *fait social total* »<sup>258</sup>, produit d'un enchevêtrement institutionnel mouvant, « *non seulement de la monnaie, mais aussi des relations individuelles médiatisées par* » elle (Blanc 2009a, p. 3-4).

Comprendre l'argent dans toutes ses dimensions nécessite d'aller au-delà de l'étude des caractéristiques génériques des médiums, car il s'agit moins d'*« un fait matériel et physique, [que d']un fait social »*, *« d'une institution, d'une foi »* (Mauss 1914, p. 3-4). L'IFM, suivant la « *démarche unificatrice proposée par Dufy et Weber (2007)* » et par l'analyse des usages de l'argent, vise à rendre compte des significations sociales de l'argent, de la pluralité des instruments monétaires et des modalités de leurs usages et de leurs articulations (Blanc 2009a, p. 2). Il faut privilégier la compréhension des pratiques et usages de l'argent, en reconnaissant l'importance à la fois des représentations (individuelles) et des arrangements institutionnels (collectifs) qui s'articulent dans tout phénomène monétaire. À travers ce prisme et puisque la monnaie apparaît d'abord comme un « *ensemble spécifique de relations prenant diverses formes – symboliques (unité de compte, sceau, signature), matérielles (moyens de paiement : pièces, billets, écritures), institutionnelles (règles de compte, de paiement, d'émission, de change)* » (Théret 2008, p. 7), l'argent ne saurait se réduire « *à la monnaie* » conçue comme « *un médium socialement, si ce n'est économiquement, neutre apte à mesurer, intermédiaire et conserver la richesse* » (Blanc 2009b, p. 1). En découle une distinction conceptuelle entre l'argent, comme abstraction sociale de la valeur, et la monnaie, renvoyant aux « *moyens de paiement manuels* » sur lesquels cette valeur s'adosse par monétisation (*Ibid.*). Il s'agit alors d'éviter plusieurs écueils. Tout d'abord, celui d'intégrer la monnaie à la sphère des biens, à laquelle elle s'oppose par définition (Simmel 2009) ; ensuite, celui d'amalgamer l'absence de médium monétaire à l'existence de société non monétaire ; enfin, celui de mobiliser l'hypostase

---

<sup>257</sup> M. Mauss (1923, p. 30, note 5) qualifie ainsi les critiques qui lui avaient été faites par Malinowski et Simiand, pour qui le terme de monnaie devait être réservé aux seuls objets porteurs des fonctions d'échange / paiement ET d'éton de valeur.

<sup>258</sup> Selon Mauss ([1924] cité par Blanc 2009, p. 3-4), « *un fait social total est un fait qui met “en branle dans certains cas la totalité de la société et de ses institutions” et “dans d’autres cas, seulement un très grand nombre d’institutions”* ».

de la monnaie tout usage, portant idéellement les fonctions monétaires canoniques (cf. section II.2.3 suivante).

À contre-courant du mythe économique du troc, nous considérons avec d'autres qu'aucune société ne « *fut complètement démunie* » de la notion d'argent et ce, même en l'absence de système de marché. Si l'argent tient une fonction, c'est primitivement celle d'être un opérateur d'appartenance sociale. Il est un rapport construit à la totalité sociale toujours située, dans lequel s'expriment et se confortent (ou non) les valeurs de la société considérée. De ce point de vue, il est vain de chercher, comme Menger (1892), l'« origine » de la monnaie dans les caractéristiques des médiums et les seuls intérêts individuels. Penser l'argent oblige à s'intéresser moins à *ce qui circule* qu'au *comment cela circule*. La matérialité des moyens de paiement importe moins que l'« état monétaire »<sup>259</sup> qui leur est donné, par *fusion*, suivant des usages prenant place dans un environnement économique, social et politique situé. D'où le fait que, si l'acception monnaie des économistes « *renvoie d'abord à un problème de quantité, l'argent [renvoie d'abord à] un ensemble de qualités* » (Blanc 2009b, p. 1). Notre objet de recherche n'est pas tant la monnaie que l'argent, conçu comme processus de *monétisation*, dynamique et multidimensionnelle, articulant les deux. Réussir « *le test de la "monétisation" dépend de la satisfaction de deux conditions* » transfigurant la monnaie en institution, suivant un processus d'assignation moins économique que socio-politique : s'ériger « *en tant que mesure de la valeur abstraite (monnaie de compte)* (Keynes 1930 ; Grierson 1977 ; Hicks 1989 ; Hoover 1996) ; et *en tant que moyen de stockage et de transport de cette valeur abstraite* » (Ingham 2004, p. 70). L'argent comme relation sociale et mesure de celle-ci construit un espace institutionnel « unifié », une communauté. S'y définit collectivement le commensurable, le comparable et le payable (et, en négatif, l'incommensurable, le non comparable et le non payable), suivant des dispositifs et des arrangements institutionnels.

### **La monnaie comme système de paiement : monétisation et liquidité de dettes hétérogènes**

De ce qui précède, l'IMF reconnaît que la monnaie ne se réduit pas à *une institution*, puisque, empiriquement, elle est « *tout à la fois système de signes (langage), système d'objets (matérialité) et système de règles (institution)* » (Théret 2008, p. 2). Pour saisir la complexité du phénomène de monétisation, l'IMF a forgé une boîte conceptuelle centrée sur les concepts de dette, de confiance et de souveraineté (communs à l'hétérodoxie monétaire, cf. encadré n° 3). D'abord, trois modes de présence au monde simultanés de la monnaie (qualifiés d'états) dont il est impérieux d'analyser l'articulation, sont distingués. Les critiques précédentes, arc-boutées sur leur bréviaire fonctionnaliste, marchand et unitaire de la monnaie, ne disent rien de cette articulation. Ces dernières se focalisent sur le seul « *état objectivé* », « *repérable dans les instruments monétaires qui servent de moyens de paiement* » et occultent l'essentiel : l'« *état incorporé [...] où elle apparaît comme étalon de valeur et confiance [et l'] état institutionnalisé, soit les diverses règles et régulations qui unifient un espace monétaire régi par un système de compte et constituant une communauté de paiement.* » (*Ibid.*, p. 16). Aussi, l'argent est plus communément conçu comme système de paiement, dont trois caractéristiques suffisent à garantir la présence (Cartelier, 1996, p.76-77) : d'abord, la fixation d'une unité de compte nominale ; ensuite, l'existence d'un « monnayage », c'est-à-dire d'un ensemble de règles déterminant la manière par laquelle les UCN\* sont mises en circulation (cf. modalités d'accès aux moyens de paiement hors recette provenant d'autrui) ; enfin, la présence d'un cadre

---

<sup>259</sup> En physique, la liquidité renvoie à l'état d'une matière dépendant de conditions environnementales et de son processus de fusion. Les états liquide et solide sont relatifs, avec des états intermédiaires dits « mésomorphes ».

de résolution des soldes, puisque la présence de soldes non nuls implique des restructurations du support de monnayage susceptible de restaurer l'équilibre des paiements.

Au centre de cet appareillage, on retrouve une unité de compte nominale qui permet la mesure préalable de la valeur économique sans laquelle les échanges n'auraient de termes à honorer. On affirme la primauté (historique et logique<sup>260</sup>) de cet usage en *monnaie de compte* : de lui dérive l'usage en paiement/échange. Ces usages (et non fonctions), considérés comme « *des concepts premiers dans une théorie de la monnaie* » (Keynes cité par *Ibid.*, p. 8), constituent les « *propriétés génériques (et fonctionnelles)* » de l'argent, distinctes d'*« usages non monétaires* », comme la fonction de réserve (*Ibid.*, p. 2). L'unité de compte intègre la monnaie dans la métrologie, se présentant comme un « *système sémantique, semblable [...] au langage, à l'écriture ou aux poids et mesure* » (Polanyi 2011, p. 163-164), structurant le langage de la valeur économique et permettant d'évaluer quantitativement des relations de dettes et créances hétérogènes, nouées entre membres participants à la division du travail au sein de la société considérée (Cartelier 1996; Aglietta et Cartelier 1998). Ce langage médiatisant des relations de dettes et créances diverses<sup>261</sup> renvoie irréductiblement à une dimension collective et holiste (la fixation d'un langage comme système de règles et de signes reconnu par une communauté ne peut se réduire à une logique individuelle). L'espace socialement reconnu du commensurable, de l'échangeable et du payable se fonde dans l'argent et son UCN\*, qui sont au fondement de notre rapport à nous, en tant que sujet économique, et à autrui. À ce titre et puisque qu'aucun linguiste n'affirmerait qu'une langue n'existe du seul fait de la présence d'institutions en charge d'en fixer formellement le cadre d'usage, la monnaie vit d'abord par ceux qui l'emploient, parfois en dehors de ce cadre. On touche à l'*« état incorporé »*, niveau le plus individuel et micro de l'analyse, où la monnaie « *est d'abord une activité mentale* » structurant « *la personne même de ses utilisateurs, [faisant] partie de leur habitus, [qui] est inscrite dans leur système de disposition* » (Théret 2008, p. 16). La monnaie est une croyance collective, résultante d'un accord entre les membres du groupe, reflétant les liens perçus ou réels des individus avec la société, chacun devant y voir une expression légitime de la valeur (Orléan 2005).

La diversité des relations d'endettement que médiatise l'argent met en évidence la question de la qualité des créances et des incertitudes (cf. défaut de paiement et risque systémique, Théret 2008, p. 16), donc de liquidité. Y répond la question des palliatifs institutionnels de réglementations, de hiérarchie et d'autorité (pouvant se faire pouvoir<sup>262</sup>), vecteurs de confiance, de sécurité et de stabilité (pointant nos autres états monétaires). L'argent signe relève d'un *signifié* et nécessite des objets *signifiants* à investir, en tant que symbole tangible (« *état objectivé* »). Quels que soient les moyens de paiement, leur monétisation repose sur l'évaluation de leur liquidité par différents acteurs, liquidité conçue comme « *désirabilité (et donc acceptabilité) aux yeux d'autrui* » (Dequech 2013, p. 255). Elle est supportée par la confiance que tous ont dans cette acceptation future et dans les qualités perçues qui la

---

<sup>260</sup> Simmel (2009, chapitre 1) démontre l'antériorité logique de l'unité de compte abstraite. Les travaux d'histoire et d'anthropologie confirment la préséance des monnaies scripturales (Aglietta et Orléan 1998; Théret 2008; Cartelier 1996; Ingham 2004).

<sup>261</sup> Face à des rapports d'endettement nombreux, nous n'amalgamons pas toute obligation sociale à une dette, et notre intérêt se porte sur les obligations monétaires, médiatisées en UCN et réglées en moyens de paiement (Théret 2009; Polanyi 2011).

<sup>262</sup> Nous suivons la distinction wébérienne opposant le pouvoir - comme capacité d'imposer sa volonté contre toute résistance – à l'autorité - comme capacité d'imposer une décision grâce à la reconnaissance de sa légitimité par ceux qui obéissent.

garantissent<sup>263</sup>. C'est à ces conditions que l'argent devient l'opérateur de « *la comptabilisation et [du] règlement des dettes* » et qu'il est permis aux instruments de paiement qui s'y adosSENT de se comporter *de facto* comme tel (Ingham 2004, p. 25). Les symboles d'autorité politique chers aux chartalistes qui s'y trouvent apposés ou l'acceptation en règlement des obligations fiscales témoignent de cette confiance à construire entre tous et de l'« état institutionnalisé » où la monnaie se donne comme forme politique d'une communauté. Mais rien ne dit qu'aucune communauté humaine et ce faisant, qu'aucune monnaie, ne puisse s'instituer hors du giron exclusif des États-nations, proposition aussi réifiante qu'anachronique et contrefactuelle.

### **La monnaie à l'épreuve : quand dettes, confiance et souveraineté se confrontent**

Notre conception de la monnaie, d'abord comme un ensemble de règles donnant forme à une monnaie de compte et ses représentations matérielles, induit une série de problématiques relatives aux autorités qui énoncent les règles, en vérifient l'application, en sanctionnent les manquements et émettent les représentations matérielles de la monnaie de compte, ainsi qu'à la confiance et à la légitimité qui sont octroyées aux autorités, aux règles et à la monnaie. Nous revendiquons un nominalisme « non étatique » dont le conventionnalisme s'oppose au chartalisme (Dequech 2013, p. 252-253), ce qui nous conduit à des analyses démontrant « *tantôt d'un point de vue empirique* [cf. section I.2.3], *tantôt d'un point de vue doctrinal* [cette section], que la dimension étatique de la souveraineté ne saurait annexer la notion de souveraineté monétaire. » (Blanc 2009b, p. 6). Certes, l'« *argent doit être émis. Et quelque chose ne peut être émis en tant que monnaie que s'il est capable d'annuler toute dette contractée par l'émetteur* » (Ingham 2004, p. 25). L'espace institutionnel que recouvre l'argent contient un enchevêtrement d'une diversité de formes de créances, relevant d'émetteurs et de sphères de circulation hétérogènes questionnant la confiance qu'on leur prête, selon la qualité des signatures ou des sceaux qui y sont apposés, de leur intrication et des défauts qu'implique la répudiation de certaines. De là, et selon la personnalité des émetteurs et la qualité de leurs créances, sont distinguées les monnaies publiques des monnaies et titres privés, et, comme explicité, pourquoi chacune ne peut assurer la même confiance (Orléan 1998, repris par Scialom 2003). Les monnaies privées comme les titres financiers reposent sur une logique de signature, à base contractuelle (de droit privé), ce qui par nature les rend fragiles : la qualité de la signature et ce faisant, la confiance dans la monnaie qu'elle garantit, renvoie à « *une évaluation locale des risques spécifiques attachés à telle ou telle dette* », soit à la crédibilité et la solvabilité – réelle ou anticipée – d'émetteurs, qui peuvent brutalement être remises en cause (cf. défaut de paiement ; André Orléan 1998, p. 8). À l'opposé, les monnaies publiques reposent sur une logique de sceaux, à base purement fiduciaire, qui les dote de qualités et d'une liquidité supérieure : l'émetteur relève d'un représentant souverain (de droit public) dont la qualité de la signature n'a pas d'égal. La confiance en la validité pérenne de cette créance repose sur des garanties collective, publique et institutionnelle et, en dernière instance, sur la permanence des États et de leurs systèmes fiscaux, permettant de garder désirable la monnaie émise par l'État ou ses représentants. On retrouve cette logique de sceau au fondement de la monnaie centrale, dite de premier rang dans les systèmes hiérarchisés contemporains. Nous-mêmes reconnaissions à l'État un rôle clef dans les phénomènes monétaires modernes, ses administrations établissant et régulant la monnaie nationale et les modalités de conversion avec les autres devises (Emily Gilbert et Helleiner 1999, p. 11). Pour autant, le phénomène monétaire ne n'y réduit pas. L'argent est « *moins décrété qu'élu* » (Jean Michel Servet, Théret et Yildirim 2016, p. 30),

---

<sup>263</sup> L'importance prise par la matérialité des objets monétaires serait faite d'un renversement : si « *l'objet élu [...] peut être a priori n'importe quoi* », sa reconnaissance sociale « *conduit les agents à penser que l'élection d'un objet particulier comme monnaie est due à ses qualités intrinsèques, et non au mimétisme* » (Aglietta et Orléan 2002, p. 83; Dequech 2013, p. 258).

puisque la monétisation est moins un fait du prince qu’« *un processus collectif d’élection par lequel un groupe de producteurs et d’échangistes de marchandises construit sa cohésion en faisant émerger une représentation commune de la valeur unanimement admise [...] ; c'est l'accord unanime du groupe qui est au fondement de l'institution monétaire.* » (André Orléan 2019, p. 1) On comprend dès lors que toute souveraineté incarnée ait toujours à faire face « *d'une façon ou d'une autre [à] la souveraineté des utilisateurs de monnaie* » (Courbis, Froment et Servet 1990, reprenant le concept de J. Rueff, p. 23). La légitimité de l’État et de ses lois est éprouvée et contestée, de manière endogène (via la renégociation des règles de monnayage et de règlements de solde) ou exogène (comme avec le phénomène des monnaies parallèles). La monnaie apparaît comme *ambivalente* : il s'y joue une dialectique entre les individus et le collectif, irréductiblement politique. Preuve que « *la monnaie n'appartient pas à l'État* » : même la coercition la plus radicale (la peine de mort) n’arrive à garantir le cours légal et forcé effectif des « *assignats révolutionnaires* » (Orléan 2002, p. 27).

Partir de la confiance inhérente au fait monétaire, comme le fait l’IMF, permet de comprendre qu’aucune confiance n’est jamais imposée d’en haut. Elle vient d’en bas et ceux qui l’octroient ne la confient que pour un temps, conservant le pouvoir de la retirer aussi vite qu’ils l’avaient donnée : le pendant négatif qu’est la défiance apparaît. La confiance (et son inverse) relève d’un phénomène multidimensionnel reposant sur une diversité d’acteurs, d’arrangements institutionnels, de relations et de représentations sociales. Cette idée d’un écheveau institutionnel produisant ou non de la confiance est au cœur des travaux de l’IMF. Simmel (2009) l’avait formulé au travers de sa théorisation d’un *continuum* monétaire infini (évolutif, mais non univoque, allant du « troc » à l’échange monétaire « pur »), reposant sur de la confiance dont les ressorts connaissent des basculements qui la font passer de garanties plus individuelles (confiance « centrifuge ») à d’autres, plus collectives et institutionnelles (confiance « centripète »)<sup>264</sup>. Si l’argent est un construit collectif, la confiance se joue d’abord en chaque individu : y git un désir de liquidité autoréférentiel et mimétique, cristallisation d’une tension entre les individus et le(s) collectif(s) dans lesquels ils sont insérés (André Orléan 1998; Aglietta et Orléan 2002). L’autoréférentialité fonde le statut de liquidité ultime et de créance au porteur sur la totalité sociale. La disposition d’argent comme promesse sociale, si elle se rapporte toujours au collectif, se mue simultanément en un pouvoir individuel sur la circulation économique (ou thésaurisation) dessinant une « ambivalence » de l’argent (et de la liquidité qui l’incarne<sup>265</sup>, Aglietta 1988). Cette multidimensionnalité du phénomène de confiance est saisie aussi par la distinction de trois niveaux, d’ordres différents, qui s’articulent de manière singulière dans tout système monétaire (Aglietta et Orléan 1998; Théret 2008; Desmedt et Lakomski-Laguerre 2015; Blanc et Fare 2017). Le niveau le plus individuel relève d’une confiance dite *méthodique*, renvoyant à ces conditions d’usage et au mimétisme des comportements individuels, de l’ordre d’une croyance routinière dans l’acceptation collective des moyens de paiement. La confiance *hiérarchique* renvoie au fait que la monnaie est toujours

<sup>264</sup> La confiance dite centrifuge serait tournée vers l’individu et la satisfaction de ses propres besoins, renvoyant aux monnaies marchandises (les « produits de base » de Polanyi par exemple, 2011), là où la confiance centripète est sise sur des symboles purs tournés vers l’extérieur. Les fiat monnaies illustrent ce décentrement du sujet vers le groupe, puisqu’elles n’offrent aucune consommation en propre, informant du fait que, en dernière instance, c’est la société qui en garantit le pouvoir libératoire. Les monnaies métalliques opéraient déjà ce décentrement par rapport au produit de base : la parure, sa dimension symbolique et ostentatoire ne sont compréhensibles qu’en relation avec le groupe (Simmel, 2009).

<sup>265</sup> Cette ambivalence repose sur l’usage en réserve de valeur permettant de s’extraire individuellement de la circulation marchande, au prix de la formation de déséquilibre collectif. On retrouve la « *préférence pour la liquidité* » de Keynes, dont dérive la demande de monnaie : les moyens de paiement et leur thésaurisation se muent en une protection et un pouvoir privé assurant à leur détenteur l’éventail de choix le plus large, capacité de choix désirable face à l’incertitude radicale (Aglietta et Orléan, 2002).

garantie par une ou plusieurs autorités souveraines, d'où des hiérarchies entre les émetteurs et les moyens de paiement. La confiance *éthique*, enfin, met en branle l'autorité du système normatif (normes et valeurs) et induit que la régulation monétaire assure la reproduction de la société dans le respect de ses valeurs constitutives. Les analyses précédentes semblent myopes à cette dernière dimension pourtant essentielle. Pour qu'existe une foi dans la stabilité de la monnaie comme système de compte, ces trois dimensions doivent s'articuler hiérarchiquement et de manière cohérente aux yeux non seulement de l'état et de ses représentants, mais des citoyens (Aglietta et Orléan, 1998 ; Théret, 2008 ; Desmedt et Lakomski-Laguerre 2015). Sans cela, la défiance prime.

Interroger la liquidité des moyens de paiement, quelles que soient leurs formes, révèle la nature sociale et le lien à la souveraineté politique, ainsi que le rapport dialectique entre les logiques individuelles et collectives, et entre les autorités et la légitimité accordée par les membres de la société, qui se jouent dans la monétisation. Dans son *Traité des monnaies* de 1360, Nicolas Oresme mettait en garde contre le fait de plaquer toute entière la souveraineté monétaire sur le fait du prince et la personne qui l'incarne : car « *quoique, pour l'utilité commune* », il lui revient d'apposer « *sa marque sur la pièce de monnaie* », il n'en devient pas pour autant « *le maître ou propriétaire* » ! En tant qu'« *éalon de la permutation des richesses naturelles ; elle est donc la possession de ceux auxquels appartenaient ces richesses* », ceux-là mêmes que le prince ne fait que représenter (Oresme, p. 54 cité par Desmedt et Piégay 2007, p. 130). Oresme questionne cette tension et le contenu de la gouvernance de la monnaie : chez lui, si la diminution du numéraire des monnaies était légitime, cela pose la question de savoir si un tel pouvoir devait raisonnablement être confié au seul prince (Tutin 2009, p. 10). Considérer la monnaie comme « un lien social » impose d'être conséquent, puisque cela suppose l'existence d'un espace relationnel (non univoque) que la monnaie participe à former, ce « *dont témoigne avec force le fait qu'elle se présente toujours adossée à une communauté de paiement.* » (André Orléan 2019, p. 1) Conceptualisée par Knapp dès 1905, une communauté de paiement qualifie l'ensemble des acteurs qui s'identifient au système monétaire national, suivant qu'ils partagent la même unité de compte, les mêmes principes de monnayage et de résolution des dettes (Blanc 1998a, p. 7). À toute communauté de paiement s'attache un « *univers symbolique* », un « *espace homogène de représentations caractérisé par une hiérarchie en valeurs et des normes* », qui « *s'impose aux acteurs par la définition du cadre dans lequel leurs pratiques prennent place et les formes monétaires prennent sens* » (Blanc 2009b, p. 12). Cette communauté de paiement relève d'une « *souveraineté propre, dont sont investies des personnes ou des institutions spécifiques* », qui n'est jamais donnée, puisqu'elle se construit, s'étoffe et s'éprouve dynamiquement, suivant qu'elle est traversée d'intérêts différents (*Ibid.*). On peut ainsi distinguer des « groupes monétaires » conçus comme des « *sous-ensembles hiérarchiquement insérés dans la communauté de paiement* » qui, s'ils « *en respectent les principes* » communs, n'en réprouvent pas moins certains, d'où le fait que leurs membres puissent « *refuser d'employer certains instruments monétaires au profit d'autres qui leur sont spécifiques* » (*Ibid.*). Chaque groupe monétaire relève d'un univers symbolique propre, qui définit pour lui et ses membres des limites et oriente les usages sociaux de la monnaie. Cette pluralité interroge du même coup les conditions d'articulation des systèmes entre eux via l'établissement de procédures de conversation (*Ibid.*).

Le cadre précédent, à visée universelle, englobe toutes les monnaies, qu'elles soient métalliques ou fiat, sans les opposer. Il permet, par l'analyse de leur monnayage et des régulations en place, de décrire et d'analyser la diversité des médiums ainsi que l'évolution des normes monétaires et des arrangements institutionnels. Dès lors qu'on se situe au sein de l'IMF, nous allons voir que les deux grands corps d'arguments mobilisés contre les CM - l'unicité

synchronique des fonctions canoniques et l'exclusivité juridictionnelle de la monnaie - ne tiennent pas.

### **II.2.3 Au-delà des critiques instrumentales et chartalistes : des CM ni unitaires, ni exclusives**

Ainsi, nous contestons les définitions de la monnaie « *par ce qu'elle fait* » mobilisées par les contempteurs des CM, considérant que « *la monnaie doit a priori être considérée comme une entité à définir non pas par des fonctions vis-à-vis d'un extérieur à elle-même, mais par des propriétés constitutives propres* » (Théret 2008, p. 6). Tout à la fois signifiant et signifié primordial fondant une communauté de paiement, c'est seulement à l'aune des propriétés respectives de Bitcoin et d'Ethereum, donc du point de vue de leurs usagers, qu'il est permis d'évaluer leurs dimensions monétaires et les qualités qui leur sont prêtées. C'est ce que permet d'affirmer aussi la démarche ethnographique : analyser la monnaie comme système à la fois idéal et matériel passe par l'analyse d'usages situés, où s'enchevêtrent un ensemble d'acteurs, de groupes, de dispositifs et arrangements institutionnels, de valeurs et de représentations, plus ou moins homogènes (Dufy et Weber 2007). Et ce, en cohérence avec l'une des thèses centrales du chapitre I : on ne peut qu'amputer le phénomène des CM, si on le réduit à leur seul protocole *sans tenir compte de la dynamique relationnelle et carnavalesque propre à leur monétisation*. Matériellement, cela reviendrait à oublier l'ensemble composite d'arrangements sociotechniques hors protocoles qui en soutiennent l'usage et les acteurs qui y prennent part. Idéellement, cela revient à imposer les représentations des analystes contre celles de ces mêmes acteurs, faisant fi du même coup de leurs attendus monétaires propres. La controverse qui traverse le champ monétaire n'a pas besoin de la crise pour se faire jour : l'analyse systématique des pratiques démontre que toutes les sociétés connaissent la présence synchrone d'usages et ce faisant, de monnaies particulières, au sein et à côté des systèmes de paiement traditionnels (Viviana A . Zelizer 1989; Viviana A . Zelizer 2005; Blanc 1998a; Blanc 2009b). Une conflictualité « en pratique » s'exprime dans les formes (plus ou moins formelles) de différenciation ou d'indifférenciation *des monnaies* en circulation, qui participent à imposer (ou non) des modalités de conversion. Il s'y joue les conditions mêmes de la circulation, comme de la reproduction d'une confiance partagée dans la stabilité et la pérennité du système de paiement. Cette pluralité des pratiques démontre la diversité des univers symboliques, autour desquels peuvent se constituer des groupes monétaires disparates.

Finalement, l'hétérogénéité des pratiques monétaires contraste avec les caractéristiques d'unicité, d'exclusivité et de pleine synchronicité des fonctions monétaires canoniques aujourd'hui axiomatisées en théorie et en pratique. En libérant l'argent des carcans réifiants, il est possible d'interroger les conditions institutionnelles, collectives et politiques qui président (ou non) au maintien dynamique de l'unicité et de la stabilité du système monétaire considéré. À revers des critiques focalisées sur la présence synchronique des fonctions monétaires, nous verrons que les monnaies nationales sont elles-mêmes moins homogènes qu'elles n'y paraissent quand, dans le même temps et à côté d'elles, une diversité de monnaies parallèles existe. De ces constats et des pratiques des *coiners*\*, il devient possible de dégager des usages en compte, en paiement et en réserve de valeur.

### **L'irréductible hétérogénéité des monnaies d'hier et d'aujourd'hui**

Quand on s'intéresse aux usages effectifs de l'argent - d'hier et d'aujourd'hui –, la monnaie apparaît « *fragmentaire sous l'aspect des instruments* », n'apparaissant homogène et unitaire que « *sous l'aspect du système* » (Blanc 2008, p. 11) : la seule règle monétaire universellement valable est que les usages de l'argent mobilisent, partout et toujours, une multiplicité d'objets (non parfaitement homogènes, ni fongibles entre eux), relevant d'usages et

fonctions différencierées. On retrouve la centralité accordée à la monétisation, puisque l'unicité systémique entre une multiplicité de monnaies n'est pas donnée, mais se construit, s'institutionnalise, sans qu'il soit possible d'en exclure le phénomène des CM.

On doit à Polanyi (2011) d'avoir systématiquement contesté l'hypostase d'un argent partout et toujours « tout usage » (« *All Purpose Money* » ou « APM », portant parfaitement les fonctions monétaires canoniques, *Ibid.*, p. 9). Il distinguait les systèmes monétaires dits « *primitifs et archaïques* » des systèmes « *modernes* ». Les premiers relevaient de « *Special Purpose Money* » (SPM), suivant la coprésence d'une diversité d'objets monétaires couvrant des fonctions différencierées, structurant des espaces économiques pluriels et cloisonnés. Les travaux d'historiens, d'anthropologues ou d'ethnographes le confirment : nombreux sont les « *exemples où les fonctions de moyen d'échange et d'unité de compte ne coïncident pas* [, comme] dans l'Europe médiévale, [où] la séparation des différentes fonctions de la monnaie était la règle plutôt que l'exception» (référence à Spufford (1988) et Kindleberger (1993), Doepke et Schneider 2017, p. 1-2). Historiquement, les fonctions monétaires n'étaient portées qu'incomplètement par une diversité de médiums hétérogènes plus ou moins convertibles entre eux, relevant d'usages monétaires, d'acteurs, de normes et de canaux de circulation monétaire spécifiques (cf. la séparation entre « trésor » et « produit de base », Polanyi 2011, Chap. 9). Au sein de l'espace national, une concurrence forte existait entre la monnaie nationale et d'autres types de monnaie en circulation, comme des monnaies sous-nationales (émises par des entités privées ou infra-étatiques) et des monnaies étrangères. Il était moins facile de se défaire de cette concurrence que de s'en accommoder, aussi les autorités politiques avaient intérêt « à attirer le plus de monnaies étrangères sur leur territoire », « tolérer ces espèces, voire [à] leur donner cours légal » tant « la prohibition des espèces illicites [et] étrangères, était illusoire », alors « que la monnaie locale demeurait insuffisante en quantité ». [Et ce] même lorsque les structures de l'État sont relativement fortes, le monopole ne peut s'établir sur la circulation monétaire (Favier 1981, p. 177) [quand le] souverain ne possédait pas le privilège du prélèvement, car il existait de nombreux circuits para-fiscaux non étatiques » (Desmedt et Piégay 2007, p. 124).

Néanmoins, pour Polanyi (1944; 2011), les monnaies « modernes », suivant la « grande transformation », seraient devenues de pures APM, unitaires et intégrées, portant parfaitement les fonctions monétaires canoniques, à la différence des SPM conçues comme coûteuses et inefficaces. Cette distinction entre SPM et APM démontre déjà le caractère partiel et situé des définitions de la monnaie, compte tenu de la prévalence historique des systèmes de SPM. Ces éléments rendent dès lors impossible d'exclure du champ monétaire les formes monétaires « imparfaites » à l'aune d'APM situées historiquement et qui n'en représentent qu'une part congrue. Polanyi postulait que l'hétérogénéité et la non-synchronicité des fonctions monétaires relèvent d'un passé révolu, et que les SPM avaient définitivement laissé la place à des APM. Et c'est de cet étalon des APM que s'écartent trop les CM. Les recherches contemporaines démontrent cependant que la vision en termes d'APM relève aussi d'une hypostase : pour modernes qu'elles soient, nos fiat monnaies contemporaines sont moins unitaires qu'elles n'y paraissent (Melitz [1970] cité par Blanc 2009, p. 11; Zelizer 1989; 1999; 2000; 2005). Malgré leur haut degré d'unicité et d'intégration, les monnaies modernes sont l'objet de « marquages sociaux » émanant de trois sources, qui dépendent de l'identité du détenteur (organisation ou individu, genre, activité et communauté d'appartenance) et s'opèrent à différents moments de

la séquence des opérations monétaires (Blanc 2009a, p. 13-15)<sup>266</sup>. À cette hétérogénéité endogène au sein de la monnaie nationale s'ajoute encore le phénomène des monnaies parallèles (cf. sous-section suivante). La monnaie est hétérogène de toutes parts, ce qui renouvelle la question des modalités de conversion et des acteurs qui l'opèrent (agrément officiel dans le cas des banques et établissements financiers, hôtel des monnaies en système métallique, mais aussi changeurs à la sauvette).

Finalement et comme par le passé, dollar et euro sont assignés dans leurs usages à des contrôles et restrictions qui limitent leur liquidité et leur fongibilité. Les différenciations qualitatives que ces marquages produisent remettent en cause leur pleine capacité à porter synchroniquement les fonctions canoniques. Dès lors, la monnaie, ou plus exactement les monnaies (les « *monies* » de Zelizer, 1989), sont partout et toujours des *SPM*. Il devient alors impossible d'affirmer, à charge contre les CM, que l'« *euro est universellement accepté* » comme le fait E. Assouan (2018). L'universalité de l'euro est relative, comme pour toute monnaie. Déjà, l'Union européenne n'est pas l'univers et l'euro, à l'instar du dollar, n'a pas le statut de monnaie internationale, quand sa circulation européenne est cantonnée aux pays engagés dans l'union monétaire seulement. Et même au sein de l'union monétaire, peut-on vraiment dire que tout euro est « *accepté par tous* » ? Comme nous l'avons vu dans la section 1, le cours légal et forcé est soumis à des exceptions : comme l'obligation de faire l'appoint ou la possibilité de refus des commerçants soumis au principe de « bonne foi » (article L. 112.5 du Code monétaire et financier). Juridiquement, l'« *euro* » contient les monnaies scripturales privées, dont l'acceptation, nous l'avons vu, n'a rien d'universel puisqu'elles ne jouissent pas du cours légal et forcé dont bénéficient les monnaies manuelles émises par l'autorité centrale. Aussi, l'argent, qu'il soit dollar ou euro, a bien « une odeur », particulièrement quand il est « sale », marqué du sceau de l'« illégalité » (exemple du marquage à l'encre des billets volés dans un distributeur, Koning 2018d), nécessitant d'être « blanchi » suivant des procédures et dispositifs particuliers, afin de ne pas perdre son pouvoir libératoire (Blanc 2008, p. 19).

### **Monnaies nationales et monnaies parallèles, un espace monétaire toujours contesté**

L'exclusivité de leur circulation sur l'espace juridictionnel étatique n'est pas pleine et entière. La remise en cause de SPM ne s'est pas faite en un jour, mais relève plutôt d'un processus d'homogénéisation difficile, long, heurté et jamais achevé : consubstantiel à la constitution des États-nations, elle relève de conflits et négociations politiques dont s'éprouve la légitimité (pensons au « *National Banking Act* » de 1863 et l'apparition controversée des « *green backs* », Zelizer 1989). Au début du processus étatsunien, ce sont près de 5000 monnaies qui circulent (hors contrefaçons) relevant d'émetteurs différents et, aujourd'hui encore, si ce nombre a diminué, l'hétérogénéité persiste : ce qu'illustre la diversité des billets

---

<sup>266</sup> Les sources de ces marquages sont : (1) les règles comptables, jouant sur les modes de comptabilisation des avoirs et les modes de mise en réserve, ils orientent les usages monétaires (en particulier ceux des organisations et des administrations), ce qui explique pourquoi leur évolution suit des débats politiques et sociaux conflictuels, produits de négociations : pensons aux réglementations fiscales, définissant les types de revenus (cadeau, allocation, salaire), leur assiette et leur taux, ou plus proches de Zelizer (2000), les rapports sexuels et leurs qualifications suivant l'établissement du caractère professionnel ou non de la relation ; (2) les facteurs cognitifs, qui renvoient aux pratiques des personnes en situation de stress budgétaire qui procèdent des cloisonnements dans leurs usages monétaires, associés à la constitution de routines et de hiérarchies claires dans les paiements à réaliser ; (3) enfin, les ordres moraux, puisqu'une dimension morale et affective est associée aux revenus en fonction de leur provenance, induisant là encore des limitations qui peuvent perdurer jusqu'à l'usage final de l'objet monétaire. Ces marquages des monnaies peuvent avoir lieu à différents moments, allant de leurs origines à leurs usages finaux, en passant par leur mode de comptabilisation et leur modes de mise en réserve (matérielle, comme des boîtes et enveloppes, ou scripturale, dans divers comptes, placements sur titres,...), présidant à ce que certaines formes de monnaies servent ou non à certains au paiement. Voir (Blanc 2008, p. 13-15).

et « *promesses* » qui y sont portées (Koning 2017)<sup>267</sup> ou le fait que toute monnaie légale n'a pas de cours fixe (comme la carte bancaire, le chèque, certaines grosses coupures, cf. section II.1.2).

Les espaces nationaux voient aujourd’hui encore coexister de nombreux instruments monétaires parallèles, souvent lors de crises, mais aussi dans d’autres contextes (Blanc 1998, 2006, 2009b). Blanc (1998b, p. 4) en recense 465 à travers le monde sur la période 1988-1996. Ce terme générique recouvre une réalité polymorphe. Ce phénomène renvoie à l’usage en paiement et/ou en compte d’unités de compte et de moyens de paiement différents de ceux du système monétaire national, et pose d’ailleurs des problèmes de typologie, du fait d’expériences situées qui suivent un double mouvement d’extension et de diversification (Blanc et Fare 2013, p. 54-56). Ces monnaies parallèles peuvent être classées selon l’identité des émetteurs (Blanc 1998b), l’inscription territoriale ou localisme (Blanc 2002), les objectifs du projet (Blanc 2011) ou des critères chronologiques (Blanc et Fare 2013)<sup>268</sup>.

Dans tous les cas, derrière cette grande diversité de systèmes monétaires *ad hoc*, à unité de compte propre et construits autour d’acteurs, de communautés et d’objets spécifiques, on retrouve une même volonté de questionner le monnayage national. Ces systèmes monétaires émergent en réaction à des enjeux situés dont une partie des réponses réside justement dans le fait d’instituer par la monnaie des cloisonnements/décloisonnements entre les personnes, les biens, les services et les territoires. Les contraintes et ressources organisationnelles de ces systèmes monétaires relèvent d’une question d’échelle et des objectifs visés, qui peuvent être expliqués par quatre rationalités différentes s’articulant différemment : la captation de revenus de seigneurage au profit de l’entité émettrice ; la protection de l’espace social contre les fuites de revenus et les interférences extérieures ; la dynamisation de l’activité locale ; et la transformation de la nature des échanges. Articulées entre elles, ces rationalités forment la base d’une multitude de monnaies qui, à divers degrés, contestent et cherchent à améliorer le système monétaire existant. Et comme pour les CM, les médiums monétaires utilisés portent souvent mal les trois fonctions monétaires, soit par choix (comme pour les monnaies fondantes à la Gesell, par exemple), soit du fait des caractéristiques de leur design et des contraintes de leur organisation (sphère de circulation volontairement restreinte, gestion de la *double dépense*\* avec la présence de contrefaçons, etc., Blanc 2009b ; Ali et al. 2013, p. 3). Ces monnaies parallèles, dont les CM apparaissent comme une nouvelle itération, soulignent que la structuration de l’espace monétaire est le fait d’une diversité d’instruments qui ne portent pas pleinement l’ensemble des fonctions canoniques de l’argent.

---

<sup>267</sup> Sur les billets de banque de la Réserve fédérale qui coexistent pratiquement figurent des promesses différentes, traces de l’évolution tant de la diversité des émetteurs, que des monnayages en présence. Par exemple, la série de 1914 comportait quatre promesses : l’acceptation par les banques du système de la Réserve fédérale, l’acceptation pour le paiement des impôts, le remboursement en or et le remboursement en « monnaie légale » (Koning 2017).

<sup>268</sup> Blanc (1998b, p. 5) distingue quatre groupes de monnaies parallèles selon l’identité des émetteurs : les instruments émis par une collectivité territoriale, par une organisation commerciale ou administrative, par des collectivités de personnes à vocation non commerciale, et ceux d’origine non spécifiquement monétaire. Un groupe transversal, les *paramonnaies*, se caractérise par une circulation volontairement restreinte. En termes de localisme territorial, « *sa forme la plus connue et visible* » est le « *localisme territorial étatique* » (monnaies nationales à cours légal), qui coexiste avec un « *localisme territorial infra-étatique* » (monnaies propres à des sous-espaces nationaux) et un « *localisme communautaire* » (basé sur des communautés de relation) (Blanc 2002, p. 6). Blanc (2011) identifie aussi quatre rationalités derrière les objectifs des projets, voir ci-après. Chronologiquement, quatre générations sont dessinées : les premières, fermées sur elles-mêmes sans dispositif de conversion, et les nouvelles, de plus en plus intégrées au système monétaire national avec des passerelles\*, et l’implication d’acteurs publics et bancaires (Blanc et Fare 2013).

Quand on s'intéresse aux questions entourant les conditions institutionnelles qui permettent d'articuler cette diversité, les enjeux et conflits qui traversent toujours tout espace monétaire, sa communauté de paiement et ses groupes monétaires se révèlent crûment. Ces monnaies sont l'expression pratique d'une tension en valeur, en confiance et en souveraineté. L'hétérogénéité qu'elles impliquent et qu'elles revendiquent contraste avec les caractéristiques d'unicité et d'exclusivité monétaire aujourd'hui axiomatisées, tant en théorie qu'en pratique. La contrainte que fait porter la synchronicité des fonctions dans la qualification de monnaie se relâche, tout en conservant cohérence interne et externe. Selon le prisme de ce qui précède, nous considérons que le phénomène des CM s'inscrit parfaitement dans le mouvement plus large des monnaies parallèles, particulièrement dynamique ces dernières décennies (Blanc, 1998 ; Lietaer, 2009). Transposons maintenant ce qui précède au cas de Bitcoin et à Ethereum.

### Des cryptomonnaies parallèles : usages monétaires des UCN BTC et ETH

Ce qui précède nous a conduit à préciser les caractéristiques que nous retenons comme essentielles : les usages en compte et en paiement d'UCN\*. Si les lecteurs ont déjà perçu comment cet éclairage théorique met en perspective la dimension proprement monétaire de Bitcoin et d'Ethereum, il nous reste à en réaliser une transposition plus systématique. L'ensemble de ce qui fait monnaie et participe à la monétisation est présent dans les CM. Pour le cerner, encore faut-il partir des usages. L'administration de la preuve repose sur notre enquête de terrain : les usages (observés et/ou pratiqués), en compte et en paiement, au sein de communautés du même nom ne font aucun doute, en particulier concernant un type de transaction\* que les critiques précédentes font mine d'ignorer. Il apparaît d'emblée que Bitcoin et Ethereum correspondent à de la monnaie conçue comme système de paiement puisqu'elles en présentent toutes les *caractéristiques typiques* : émission et encadrement de la circulation d'une UCN\* suivant l'établissement de règles de monnayage (Desmedt et Lakomski-Laguerre 2015, p. 3 et p. 6). Nous reviendrons d'abord sur la dimension générique et fonctionnelle de l'unité de compte où l'argent se fait tout à la fois opérateur abstrait (« état incorporé ») incarné concrètement (cf. moyen de paiement à l'« état objectivé »), institutionnalisant un espace de commensurabilité et d'échangeabilité au sein de la communauté de paiement (« état institutionnalisé »).

#### *L'impérieuse mise en forme des UCN BTC et ETH*

Nous l'avons vu, l'argent est une abstraction et se présente simultanément comme un *signifié*, qui requiert des objets *signifiants* et des symboles tangibles à investir (« état objectivé »). Malgré leurs apparences singulières, les CM relèvent de nos universaux monétaires. Historiquement, le « *choix des formes d'unité de compte* » conduit à les faire exister « *sous la forme d'un nom* », suivant deux configurations « *selon que [ce nom] se confond ou pas avec celui du moyen de paiement* » (Servet, Courbis et Froment 1991, p. 333) : s'il y a dissociation, l'ontologie sociale et abstraite de l'argent comme signifié devient évidente, ce que saisit le concept de « *monnaies imaginaires* » ou de « *monnaie fantôme* »<sup>269</sup>. Quant au « *choix*

---

<sup>269</sup> Dans la France de l'Ancien Régime, la « livre tournois [...] a servi d'unité de compte pendant des siècles au cours de la période médiévale et au début des temps modernes, même lorsque la pièce de monnaie n'était plus en circulation. La valeur d'une pièce utilisée comme monnaie de compte peut également être différente de celle de la même pièce en circulation, un phénomène appelé "monnaie fantôme" par Cipolla (1956) et "monnaie imaginaire" par Einaudi (1937, 1953) » (Doepke et Schneider 2017, p. 1-2). Dans ce sens, « l'emploi de l'écu [et de l'euro] comme monnaie de compte » a dû être introduit « progressivement dans les pratiques commerciales et financières [...] [afin] qu'il devienne une réalité sociale », avec des mises en place ciblées et par étape : les organisations précèdent les ménages, notamment (voir Servet, Courbis et Froment 1991, p. 337-338).

*des noms* », « la faible variété des termes employés » répond à la « faible capacité d'innovation des états » : cette « quasi-stabilité [...] en dépit des changements politiques ou des révolutions » souligne, s'il le fallait encore, l'incapacité du « pouvoir [à] faire abstraction de la société civile », l'importance prise par le poids des habitudes, des routines vis-à-vis d'un signifié incarnant la cohésion sociale, et donc les risques de la remise en cause du nom (*Ibid.*, p. 333-334). C'est pourquoi les termes employés renvoient souvent à des noms de monnaies anciennes - le dollar, la couronne, le franc, le florin, etc. - ou à des unités de poids - la livre, le shilling ou encore la peseta -, comme s'ils participaient d'une « mémoire commune » « dans laquelle les peuples puisent » leurs représentations monétaires. Du côté du signifiant, la frappe permet de redoubler matériellement l'objectivation de cette mesure abstraite, par apposition de symboles représentant l'autorité émettrice ou tout autre symbole d'appartenance à la société et à ses valeurs (Aglietta et Orléan 1998; Aglietta et Orléan 2002; A. Orléan 2002). Ainsi, pour ce qui est des monnaies nationales, la recherche de stabilité domine, expliquant qu'« une différenciation par le nom de la monnaie de compte est rare » (*Servet, Courbis et Froment 1991*, p. 334). Il n'en va pas de même pour les CM, qui restent néanmoins des ruptures dans la continuité.

Inscrits dans un « localisme communautaire » plutôt qu'« étatique » ou « infra-étatique », Bitcoin comme Ethereum illustrent comment, malgré le caractère numérique et immatériel de leur UCN\*, le choix de leur nom et de leur représentation témoigne d'une volonté de créer et renforcer une identité collective et un sentiment d'appartenance, en s'appuyant sur des références historiques, culturelles ou politiques propres à leur communauté. Le nom bitcoin est formé à partir des mots anglais « bit » (unité d'information binaire de base) et « coin » (pièce de monnaie), à la manière des projets de Bitgold de Szabo et de B-money de Dai, que Nakamoto avait pour référence (cf. Chap. I, sect. I). Pour l'ether d'Ethereum, Buterin souhaitait s'inspirer de la science-fiction. Le nom ether est choisi en référence à la conception scientifique médiévale qui le concevait comme un fluide hypothétique censé remplir l'univers et permettre la propagation de la lumière et des ondes électromagnétiques (Russo 2020, p. 55) : avec l'ether, l'UCN\* s'inscrit dans l'histoire des sciences, suggérant son rôle essentiel et universel dans le fonctionnement de l'« ordinateur mondial » que promeuvent les concepteurs d'Ethereum. Ces UCN\* doivent encore être dotées de symboles propres et facilement reconnaissables, et être intégrées à un système de comptabilité. Cela suppose l'établissement (i) d'un logo qui, fixé à l'origine, peut évoluer à la suite de propositions communautaires (comme pour Bitcoin<sup>270</sup>, Sedgwick 2018f ; Milano 2020); (ii) d'un « Ticker » boursier (BTC ou XBT pour Bitcoin et ETH pour Ethereum) ; (iii) d'un symbole inspiré de l'imagerie des monnaies nationales (« ₿ » pour BTC ; «Ξ» pour ETH)<sup>271</sup> et (iv) d'un système de comptabilisation (voir Annexe n°II.1

---

<sup>270</sup> En 2010, l'utilisateur (« bitboy ») propose un premier visuel pour l'UCN BTC, voir <https://bitcointalk.org/index.php?topic=1631.0;all> [consultation au 16/02/2022].

<sup>271</sup> La question du ticker est intéressante. Les codes symboliques des devises sont définis par la norme ISO 4217, mais ni le BTC, ni l'ETH n'y figurent encore (voir la liste ici : <https://www.iso.org/fr/iso-4217-currency-codes.html> [consultation au 18/02/2022]). Bien que BTC soit le symbole boursier dominant pour Bitcoin, il n'est pas conforme aux normes internationales. Certaines bourses préfèrent le ticker XBT, qui respecte la norme ISO 4217:2015. Bitcoin, n'ayant pas de pays d'origine, utilise le préfixe X pour les actifs supranationaux, suivi des deux caractères de la devise.

pour bitcoin et n°III.1 pour l'ether) : c'est la décimalisation<sup>272</sup> qui a été choisie, ce qui rapproche les UCN\* des CM de celles des monnaies fiats actuelles. Mais elles s'en démarquent par l'amplitude des plages de paiement qu'elles visent à couvrir : Bitcoin dispose de 8 décimales après la virgule ( $10^{-8}$  BTC) et l'Ether de 18 décimales ( $10^{-18}$  ETH). Cette grande divisibilité doit pallier aux offres monétaires limitées qui « peuvent sembler insuffisant[e]s pour une population mondiale de 7 milliards de personnes » : pour Bitcoin, puisqu'il y a « 100 millions de satoshis dans un seul bitcoin, [...] l'offre maximale de 21 millions de BTC [est] égale à 2,1 quadrillions de satoshis ou [...] à 2 100 trillions de satoshis. » (Champagne 2014, p. 2). En outre, cela offre une grande granularité dans les paiements. De gros montants peuvent circuler en l'absence de plafond autre que la limite de l'offre elle-même, là où le plancher qu'offre leur décimalisation fine doit faciliter les micro-paiements que les monnaies nationales rendraient difficiles (Nakamoto 2008, épigraphe Chap. I). Néanmoins, ce plancher s'établit protocolairement, mais surtout économiquement, via des frais de transaction\* (cf. Chap. I, section I.2.1). Étant donné l'augmentation continue du prix unitaire des UCN\* BTC et ETH et la prévalence des transactions\* fractionnaires (témoignant d'un usage en compte majoritaire des fiat monnaies ; cf. changement opéré dès la phase de concept, Chap. I, section 2.1), des dénominations fractionnaires propres ont été établies (voir Annexe n°II.1 et n°III.1, pour Bitcoin et Ethereum). Ces dénominations sont aussi cruciales que pour les monnaies nationales : outre la granularité des paiements offerte par leur grande divisibilité, ces fractions doivent faciliter la comptabilité mentale. L'objectif est d'ériger « *un point de Schelling sur ce qu'il faut utiliser pour les petites coupures afin que les gens puissent facilement parler de quantités variables d'Ether, que le prix [...] soit de 0,01 \$, 10 \$ ou 100 000 \$.* » (Buterin 2016f). Le choix d'un nom est délicat : « *avec Bitcoin, la communauté a du mal à s'entendre sur une dénomination plus petite [...]. « Millibitcoin » est difficile à prononcer d'une manière que “finney” ne l'est pas (aussi, voulez-vous vraiment dire à un caissier d'une banque que vous voulez acheter « cinq cents mETH » ?)* » (Ibid.). Ainsi, pour le Bitcoin plus encore que pour l'Ether, les noms choisis – le Satoshi, le Finey, le Szabo, le Lovelace, etc. – font référence à des figures et symboliques clefs de leur communauté (notamment des figures cypherpunks et crypto-anarchistes, cf. Chap. I). Les UCN\* BTC et ETH possèdent toutes les caractéristiques formelles d'unités de compte et sont même davantage divisibles. Mais remplissent-elles pour autant le rôle de monnaie de compte et de paiement ?

### *Usage en compte et en paiement*

Répondons aux critiques pour lesquelles les CM ne sont pas des unités de compte en soi, suivant que leur usage ne serait pas propre : les prix nominaux seraient toujours primitivement établis en fiat monnaies, pour des biens et services accessibles en paiement trop peu nombreux, surtout inutiles ou illégaux.

---

<sup>272</sup> La décimalisation renvoie à l'institutionnalisation d'un système de conversion monétaire, en unité compatible avec un système décimal (puissance de 10). De tels systèmes sont anciens et remontent aux premières monnaies métalliques. Selon « *certaines épopées hindoues* », il est « *possible que des pièces de monnaie – et une division décimale – aient, en fait, existé en Inde* » des centaines d'années avant les pièces frappées du roi de Lydie, dans la seconde moitié du XVIII<sup>e</sup> siècle av. J.-C. (John Kenneth Galbraith 1976, p. 25). Dans ces systèmes, toutes les sous-unités sont basées sur un facteur 10 de l'unité principale. En France, la décimalisation a été réalisée par l'introduction du franc le 17 germinal An XI, remplaçant la livre tournois et son système qui « *avait l'inconvénient d'être duodécimal, tant pour la monnaie de compte que pour la monnaie réelle. La livre, la monnaie de compte, était divisée en 20 sous, chaque sou correspondant à 12 deniers [...]. Les abus comme les inconvénients du système furent dénoncés par Mirabeau [en] décembre 1790 dans un Mémoire distribué à l'Assemblée Constituante dont les conclusions [prévoient] la décimalité des monnaies d'or et d'argent* » (Baltazard 1956, p. 175).

On pourrait répondre que l'existence d'un usage exclusivement en compte dérivé, comme le décrivent les critiques, n'est pas rédhibitoire : le phénomène des monnaies imaginaires a illustré de quelle façon un système monétaire peut contenir différentes UC, dont certaines n'existent matériellement qu'au travers de taux, consignés dans des tables de conversion formelle ou non. D'un point de vue ethnographique, qu'importe que le paiement implique ou non une conversion des UCN\* BTC ou ETH reçues (différées ou en temps réel) puisqu'il reste des traces d'un usage en compte des UCN\* à côté des fiat monnaies. Ces traces, tant *on chain\** qu'*off chain\**, qu'imposent les transferts d'UCN\* entre usagers intéressent d'ailleurs ces derniers et de nombreuses organisations et administrations (les opérateurs de passerelles\* à qui s'imposent des réglementations en termes de *Know Your Consumer* et d'*Anti Money Laundering*, ou l'administration fiscale, qui attend que cette comptabilité lui soit déclarée). En ce sens, notre retour historicisé sur le développement infrastructurel de Bitcoin et d'Ethereum, réalisé dans le chapitre I, contribue à démontrer comment le bitcoin et l'ether ont pu jouer, chacun à leur manière, des rôles de monnaie de compte et de paiement. Ces infrastructures et leur UCN\* ont trouvé des utilisateurs et des usages, fussent-ils illégaux ou portés par la spéculation. S'il est difficile d'évaluer le nombre total de vendeurs, leur localisation, tout comme les types de biens et services concernés, on peut toutefois affirmer qu'on a assisté à un accroissement important et tendanciel : de la quantité demandée d'espace d'enregistrement, du nombre de transactions\* (Annexes n° II.4, II.5 pour Bitcoin et Annexes n°III.4 et III.5 pour Ethereum) et de celui des utilisateurs d'une des bourses les plus importantes, Coinbase (Annexes n°I.3). Pour ce qui est de la plage de paiement des UCN\* bitcoin et ether, si l'on retrouve effectivement les usages visés par leurs décimalisations (gros montant et micro-paiement), l'augmentation des frais de transaction\* tend à privilégier les opérations de gros montants (quand le développement des couches de layer 2 doivent absorber la demande de micro-paiement) : ce que permet d'observer la taille moyenne et la taille médiane (comme l'écart entre les deux) des transferts en UCN\* et USD quotidiens (Annexes n°II.7 et II.8, pour Bitcoin et n°III.7 et III.8 pour Ethereum). Par ailleurs, des entreprises les acceptent en paiement, comme c'est le cas de Wikipedia, Microsoft, AT&T, Subway, Dell, Bloomberg, Google, PayPal, etc<sup>273</sup>. Le développement infrastructurel a même conduit à ce qu'il ne soit plus nécessaire à l'usager d'attendre que les commerçants les acceptent puisque, désormais, les services de paiement et des passerelles\* permettent de dépenser les CM via des cartes de paiement. Nos observations de terrain confirment ces usages : si les « *coiners\** » aiment à théauriser leurs CM, ils les utilisent aussi en bien des occasions, que ce soit de manière cérémonielle et festive, ou contrainte et forcée dans le cadre d'une crypto-finance « *vivrière* » (Allard 2018)<sup>274</sup>. L'accroissement incontestable de leur usage explique que leurs communautés rencontrent des problèmes structurants de mise à l'échelle\* (cf. Chap. I) qui conduiront Bitcoin à une dispute communautaire révélant une gouvernance sur l'infrastructure aux enjeux très politiques (le « Scaling Debate », section II.3 suivante). Aussi, quand les analystes critiquent

<sup>273</sup> Voir <https://bitpay.com/> et <https://www.coinbase.com/clients> [consultation au 15/05/2015] ou de manière plus actuelle, <https://99bitcoins.com/bitcoin/who-accepts/> [consultation au 04/03/2021].

<sup>274</sup> Le bar accueillant les Meet-up Bitcoin parisiens accepte les UCN BTC et ETH. Il est courant que les consommations soient réglées en UCN, soit directement au tenancier, soit entre les participants, l'un réglant en fiat monnaie et les autres remboursant en CM. Nos observations ont révélé de nombreux usages en paiement. Les CM s'adressent aussi aux « *exclus du système bancaire, qui vivent grâce à cette monnaie en la minant, en l'échangeant* » (Allard 2017). Certains, en grande précarité, non bancarisés, ne survivent que grâce au minage ou au trading, payant leur loyer en échangeant leur BTC à la maison du Bitcoin, illustrant le concept de « *finance vivrière* » (Allard 2018). Nos entretiens montrent que, à côté d'une théaurisation anticipant une appréciation future, ils utilisent aussi les UCN pour des paiements, tant légaux qu'illégaux, certains partageant leurs expériences sur le « *Darknet* » sous forme de révélation. Nous-mêmes avons utilisé des CM pour des biens et services : vente et achat de NFT, chargement de carte de paiement via CM lors d'un voyage, souscription à des associations comme le « Cercle du coin » et Asseth, et achat de « *goodies* » lors de la conférence ETHCC 2019.

les CM comme inefficaces du fait de frais de transaction\* « trop » importants, ils ne disent pas autre chose que *Bitcoin et Ethereum ne seraient pas utilisables... car ils sont trop utilisés !* Cette proposition est paradoxale pour des économistes, qui devraient savoir que les frais de transaction\* indiquent en creux le consentement à payer des usagers et l'utilité qu'ils en retirent... contredisant par là même l'inutilité de ces infrastructures postulée par ces économistes. Enfin, certains États et administrations, comme le Japon (McCombie 2018) ou la Suisse (Métille 2014), ont reconnu légalement le statut de moyen de paiement à ces UCN\* : un comble pour les chartalistes, des collectivités territoriales les acceptent en paiement de leurs impôts locaux<sup>275</sup>!

Affirmer que les CM n'en sont pas, car elles ne seraient l'équivalent général que de trop peu de choses, comparées aux monnaies nationales en circulation, n'a pas de sens pour nous. Fondé sur un *localisme communautaire*, le périmètre de leur circulation est plus restreint, et les CM s'intègrent à moins d'activités quotidiennes relativement à celles du localisme étatique. Cependant, ni le statut de monnaie, ni la qualité de « bonne » ou de « mauvaise » monnaie ne dépendent de la taille de leur sphère d'usage, ni de la quantité et/ou de la qualité de personnes ou de biens et services accessibles grâce à elles. Analyser la monétisation implique, pour chaque système de paiement, de porter son intérêt sur sa sphère de circulation propre, comme espace singulier d'expression de la valeur des choses en une UCN\* élue par les membres d'une communauté de paiement. Libre aux professionnels de l'argent de considérer que des cigarettes ou des boîtes de poisson ne sont pas de la monnaie, encore moins de la « bonne » ! Ce point de vue souligne l'extériorité depuis laquelle il est affirmé : du point de vue des prisonniers qui en usent, ces monnaies ne peuvent être que relativement « bonnes » comparées aux autres formes qui leur sont difficilement accessibles, car hautement régulées. De ce fait, ces monnaies visent moins à se substituer à la monnaie légale qu'à la compléter. À ce titre, il suffit qu'un bien ou service soit uniquement exprimable et payable dans leur UCN\* pour que les BTC et l'ETH jouent un rôle de monnaie de compte et de paiement sans que ce rôle soit considéré comme dérivé et secondaire. Les analystes précédents semblent avoir ignoré l'usage premier de ces UCN\*, décrit dans notre premier chapitre : être les monnaies endogènes de leur protocole, à la manière des jetons de compagnie de chemin de fer ou des monnaies émises par des collectivités territoriales, dont le pouvoir libératoire est limité à l'espace des biens et services offerts par leurs émetteurs (Blanc 1998a; Blanc 1998b). Oui, dans une pure logique nominaliste, la monnaie est émise et ce faisant, elle représente une créance ou un crédit à l'encontre de l'émetteur qui l'accepte en règlement (Goodhart 2005, p. 818). Ici, les critiques précédentes qui voient les mineurs comme émetteurs se méprennent : les seuls émetteurs sont les protocoles Bitcoin et Ethereum. Les interactions *au sein de la chaîne*, qu'elles relèvent d'usage monétaire ou non, ne connaissent qu'une monnaie de compte : leurs UCN\* respectives. Utiliser lesdits protocoles impose d'user pratiquement des UCN\* qu'ils ont émises, seules capables d'évaluer et d'éteindre les dettes contractées envers leurs représentants mineurs. BTC et ETH sont les seules monnaies de compte et de paiement liant ensemble l'offre et la demande d'enregistrement : elles permettront d'exprimer et d'acquitter les frais de transaction\* afférents aux traitements réalisés (cf. Chap. I, coûts computationnels et de stockages payés en satoshi/bit pour Bitcoin et en gwei/quantité de « gas » utilisé pour Ethereum). Or, ces deux protocoles voient une augmentation du nombre de transactions\* traitées (Annexe n°II.5 et n°III.5), comme du montant - total, moyen et médian, en UCN\* et USD quotidiens - des frais versés par transaction\* (Annexes n°II.9, n°II.10 pour Bitcoin et n°III.9 et III.10 pour Ethereum). Outre la tendance haussière, depuis le lancement respectif des deux protocoles, ce sont en cumulé près

---

<sup>275</sup> Le canton de Zoug a adopté cette mesure dès 2016, avec un plafond de paiement de 200 CHF (swissinfo.ch 2016). En 2021, la municipalité a étendu cette décision à l'ether et a augmenté le plafond à 100 000 CHF (Khatri 2021). En 2020, la ville de Zermatt a suivi cet exemple (Partz 2020b).

de 240 346 BTC (pour une valeur de près de 1 654 410 52 \$) qui ont été réglés aux mineurs Bitcoin ; près de 2 833 184 ETH (pour une valeur de près de 1 914 945 993 \$) à ceux d’Ethereum (Annexe n°II.11 et n°III.11). Coûts pour les utilisateurs, ces frais de transaction\* sont un revenu pour les opérateurs du traitement des transactions\*. Ces frais s’ajoutent aux récompenses d’émission perçues et s’élèvent en valeur cumulée à près de 23 711 736 998 \$ pour Bitcoin et à près de 11 018 696 543 \$ pour Ethereum. Alors que les coûts de minages sont exprimés en monnaie nationale, les recettes du minage (récompense d’émission et frais de transaction\*) sont dénommées et payées en UCN\*. Celles-ci devront être vendues pour couvrir les premiers, le tout étant consigné dans une comptabilité qui doit faire la place aux différentes unités de compte présentes. En outre, l’augmentation pour Bitcoin et Ethereum de la difficulté moyenne de l’activité de minage, comme des taux de *hash*\* cumulés, souligne leur capacité à recruter des opérateurs pour assurer leur fonctionnement et leur sécurité (Annexes n°II.12 et III.12). La consommation globale d’électricité évaluée pour le réseau\* Bitcoin (allant actuellement de 40.68 TWh à 447.17TWh, suivant le scénario retenu) augmente aussi continuellement (Annexes n°II.13) comme celle, beaucoup plus difficile à estimer, du réseau\* Ethereum<sup>276</sup>.

Bitcoin et Ethereum ont leur sphère d’activité propre, où leurs UCN\* offrent des prestations monétaires de paiement et de règlement exclusives, évoluant dynamiquement avec les renégociations d’acteurs. Ces usages en compte et en paiement, qu’ils soient en propre ou « dérivés », confèrent aux CM le statut de monnaie, car, comme le souligne Knapp, « *ce n'est pas l'émission, mais l'acceptation qui est décisive* » (Desmedt et Piégay 2007, p. 119). La monnaie représente une « "créance" ou un "crédit" [...] constitué par des relations sociales [qui] existent indépendamment de la production et de l'échange de marchandises » (Ingham 2004, p. 25). L’acceptation en paiement par les *coiners*\*, qu’ils soient nombreux ou non, est ce qui importe. Cette acceptation volontaire (et non forcée), bien qu’induisant un pouvoir libératoire plus « limité » que les monnaies nationales, les rapproche des expériences de monnaies parallèles. Il reste alors à examiner la fonction de réserve de valeur.

#### *De l’usage - non monétaire - en réserve de valeur*

Notre intérêt pour cette troisième fonction est ambivalent. D’un côté, celle-ci est exclue de notre définition de la monnaie, ainsi que de celle de nombreux économistes. Comme l’ont souligné Wicksell ou Hicks, elle est secondaire à la monnaie (Courbis, Froment et Servet 1990, p. 11) : au strict « *niveau définitionnel, on peut mettre de côté la fonction de réserve, car [elle est] une fonction non autonome des deux fonctions fondamentales que sont le compte et le paiement, et non spécifiquement monétaire* [ :] tout bien peut constituer une réserve de richesse, mais n’en constitue pas pour autant un instrument monétaire » (Blanc 1998a, p. 4 et 17). D’un autre côté, les croyances, représentations et attentes monétaires de la communauté de paiement restent essentielles à notre conception de la monnaie.

Déjà, le contenu de cette fonction de réserve ne va pas de soi et reste discuté (Courbis, Froment et Servet 1990, p. 12; Andolfatto 2013) : faut-il y voir une certitude quant à la

---

<sup>276</sup> Pour la méthodologie suivie, voir <https://cbeci.or> [consultation au 04/03/2021]. L’algorithme de consensus d’Ethereum, conçu pour rendre difficile la construction de machine de minage dédiée, fait que les ASIC conçus pour Ethereum ont une efficacité énergétique proche des cartes graphiques (GPU) qui restent compétitives. D’où une estimation plus difficile du fait de l’hétérogénéité des machines impliquées et de leurs rendements variés. Swanson (2021) a estimé pour 2021 une consommation basse (avec un réseau uniquement constitué des machines les plus performantes) de 8,2TWh/an, un scénario intermédiaire de 9.1 TWh/an (GPU de dernière génération) et une limite haute de près de 21TWh/an (réseau constitué uniquement de vieilles machines peu efficaces).

conservation d'un pouvoir d'achat dans le temps ou une certitude quant aux grandeurs nominales des instruments monétaires<sup>277</sup> ? C'est le premier sens que retient contre les CM la majorité des économistes et praticiens suivant la volatilité de leurs cours (Annexes n°II.14 et n°III.13). Mais doit-on alors refuser le statut de monnaie à nombre de monnaies modernes lors de perturbations monétaires ? En cas d'inflation ou d'hyperinflation, la monnaie disparaît-elle ? Les fiat monnaies permettent-elles en tout temps et tout lieu un maintien parfait de leur pouvoir d'achat suivant que leur économie connaît des taux d'inflation nuls de manière constante<sup>278</sup> ? Les réponses sont bien entendu négatives, et même le dollar ici ne serait plus monnaie (Courbis, Froment et Servet 1990, p. 12). Le second sens est également problématique, car il conduit à « repérer toute une série d'actifs financiers sûrs (quant à leur valeur nominale future), mais dont certains seulement peuvent servir de moyens de paiement [ce qui fait prendre le risque] de perdre de vue la Monnaie, de confondre monnaie et actifs liquides » (*Ibid.*). Cette perspective de conservation est inessentielle à la monnaie et relative à différents horizons temporels. Qu'importe qu'« un instrument monétaire conserve sa valeur sur de longues périodes », on attend de l'argent « qu'il conserve sa valeur pendant de courtes périodes [,] après tout, [il] n'est pas censé être une réserve de valeur à long terme. Une fois que vous avez reçu votre salaire, vous êtes libre d'acheter de l'or, des bitcoins ou tout autre bien que vous souhaitez » (Andolfatto 2013). Dans le cadre de cette fonction de réserve, BTC et ETH se distinguent néanmoins des titres financiers de par leur grande liquidité et la rapidité que cela offre aux conversions en devise nationale (la séquence Fiat -> CM -> Fiat peut être réalisée en tout instant). En outre, le second sens s'oppose au premier, en mettant au centre de son analyse la sphère de règlement propre en UCN\* au BTC et à l'ETH. Évaluer la conservation de la valeur des instruments monétaire vis-à-vis de ceux d'autres communautés de paiement place l'analyse dans le monde des titres. À l'aune de prix relatif, la monnaie est devise, un actif de patrimoines détenu dans des logiques de portefeuille. Et là où l'argent s'échange contre de l'argent (le prêt ou le change), l'argent acquiert la relativité des choses particulières, perdant ainsi son essence d'unité de compte : « la relativité, [l'argent] est voué à l'être et non l'avoir » (Simmel 2009, chap.1, section III). Ce second sens, où il importe que les instruments monétaires soient « définis de façon stable en unité de compte [...] offrant une certitude quant [à leurs] valeurs nominales » (Courbis, Froment et Servet 1990, p. 12), les *bitcoiners*\* le saisissent aussi, avec une parfaite ironie. Ils répètent à ceux qui leur parlent de volatilité que le « *prix de la pièce n'a pas vraiment d'importance* » car, partout et toujours, « 1 BTC = 1 BTC » (Hajric 2022) !

Notons cependant que cette fonction de conservation, avec son sens premier, est mobilisée par les acteurs eux-mêmes, qui en font une des propriétés désirables de leur UCN\*. Chez les *coiners*\*, cette fonction prend une place particulière dans leurs représentations et s'y lie aux récits entourant l'immortalité de leur monnayage, à leur émission monétaire limitée et décroissante qui pousserait à ce que leurs UCN\* s'apprécient, incitant à leur détention et, finalement, à leur monétisation. Pour beaucoup de *coiners*\*, les CM seraient des paris sur

<sup>277</sup> Ainsi, « l'histoire a montré que de telles "monnaies" pouvaient connaître une forte instabilité de leur valeur et donc ne plus assurer la fonction de réserve de valeur, sans pour autant perdre automatiquement leurs qualités d'instrument de paiement et d'unité de compte, donc leur caractère monétaire ». De plus, « l'emploi d'instruments définis de façon stable en unité de compte ne garantit en aucun cas aux utilisateurs une conservation du pouvoir d'achat. En revanche, et par définition, il leur donne une certitude quant aux valeurs nominales des instruments » (Courbis, Froment et Servet 1990, p. 12)

<sup>278</sup> Comme le fait remarquer sur twitter un « *coiner*\* » : « Sur les plateaux télé Fr j'entends tjs les "experts" dire qu'une vraie monnaie doit être une réserve de valeur. Si j'invite ces mêmes "experts" pour parler du franc Congolais (qui a perdu près de 200k% sur 20 ans), c'est tjs d'une monnaie qu'on va parler ou je ne comprends rien ? » <https://twitter.com/GloireKW/status/1368244762256498688> [consultation au 03/11/2023].

l'avenir<sup>279</sup>, voire des « valeurs refuges » vers lesquelles se précipiter « *en période de mauvaise conjoncture ou d'incertitude économique* » (Andolfatto 2016; exemple de la crise chypriote mobilisées par la Banque de France 2013, p. 3-4). Que les CM soient une classe particulière d'actifs d'investissement ou de spéculation ne fait aucun doute. Là où cette activité spéculative importe pour leur qualification de monnaie, c'est qu'elles fournissent des preuves des usages en compte et en paiement évoqués et qu'elles contribuent à une demande et à une liquidité de marché importante. On l'a vu, l'un des reproches faits aux CM est qu'elles sont de purs objets spéculatifs ; or, cet usage implique nécessairement une commensurabilité : devises et actifs s'échangent les uns contre les autres, suivant la fixation de « paires » de trading. S'y établissent des taux de change bilatéraux posant la question des UCN\* dominantes choisies comme pivot dans la définition des prix relatifs (BTC/USD, ETH/BTC, etc.). Les paires de trading disponibles varient d'une bourse à l'autre, et restent à la discréption des opérateurs de bourse d'échange (P. Noizat, Entretien n°24). Il en ressort que les « *coiners\** » font plus facilement référence à des cotations « à l'incertain » qu'« au certain »<sup>280</sup>, dénotant une comptabilité mentale effectuée en UCN\* (BTC ou ETH) dans l'évaluation qu'ils font de leurs portefeuilles\* d'actifs. Notre propre expérience en témoigne, et le cas des NFT est idéal typique : objets *on chain\** dont la production et la consommation passent nécessairement par la dépense d'UCN\*, leurs prix, comme les pertes et profits, sont majoritairement calculés en UCN\*. Comme vu au Chapitre I, les premières bourses ne permettaient que des échanges CM/CM, et l'UCN\* BTC jouait ce rôle d'UCN\* pivot (Carter 2020). Avec l'introduction des « stable coins », la situation a évolué, et de plus en plus d'échanges et de paires de trading sont exprimés en « jetons USD ». Cette « *dollarisation de Bitcoin* » cache une « *Tetherisation* » des CM, où « *l'USDT* [émise par l'entreprise Tether] » s'érige en « *principale paire de négociation* », en « *principal actif de règlement* » en remplacement « *de Bitcoin dans cette fonction* » (*Ibid.*) : néanmoins pour que ces jetons Tether (ou tout *stable coin*) existent et circulent au sein de ces protocoles de registre\* distribué, ils doivent s'acquitter de frais de transaction\* exprimés en UCN\*<sup>281</sup>. D'ailleurs, tous ne relèvent pas des mêmes logiques d'émission. Alors que Tether ou USDC (un *stable coin* émis par l'entreprise Circle dont les parts de marché augmentent rapidement) sont émis de manière centralisée et adossés à des « fiat monnaies » du système financier traditionnel, il n'en pas automatiquement de même au sein de l'écosystème d'Ethereum. Avec le développement du secteur de l' « open finance »/« DEFI », l'UCN\* ETH s'est vue dotée d'une pluralité de rôles, dont l'un des principaux est de servir de collatéral à l'émission de crédit en « *stable coin* » *ad hoc* (c'est le cas du DAI, où près de 55% des 2 535 286 576 \$ de DAI en circulation sont adossés à l'UCN\* Ether<sup>282</sup>). En outre, les *coiners\** voient moins la volatilité des UCN\* BTC et ETH comme un problème que comme une propriété recherchée, d'autant plus que la tendance de leur cours est historiquement haussière. Les *coiners\** spéculent au sens premier du terme, anticipant que les UCN\* détenues prendront encore de la valeur ; ils ne s'en servent pas en paiement à toute occasion : ils valorisent la thésaurisation, comme en témoignent les slogans

<sup>279</sup> Une part importante des acteurs interrogés mobilise le registre\* du pari et du jeu pour parler de leurs acquisitions de CM, espérant avoir « *misé sur le bon cheval* ».

<sup>280</sup> Dans la terminologie financière, il existe deux façons de présenter le taux de change. La cotation « à l'incertain » exprime le taux de change nominal d'une monnaie étrangère en monnaie nationale (1 USD = X euros), tandis que la cotation « au certain » exprime le change nominal d'une monnaie nationale en monnaie étrangère (1 Euro = X USD) (Généreux 1991, liv. 3, p.12).

<sup>281</sup> Les premiers « Tether » étaient émis via le méta-protocole Omni/Mastercoin et utilisaient primitivement le BTC et l'UCN omni. Aujourd'hui diversifiée, l'activité de Tether s'étend à d'autres protocoles de registre\* distribué et l'offre d'USDT en circulation se répartit entre les protocoles Ethereum (près 20 milliards de dollars), Tron (près de 16 milliards de dollars) et Bitcoin (près de 1,3 milliard de dollars), voir <https://www.theblockcrypto.com/data/decentralized-finance/stablecoins> [consultation au 04/03/2021].

<sup>282</sup> Respectivement 53,33% pour les DAI émis suivant la collatéralisation de type « ETH-A » et 1,97% pour ceux de type « ETH-B », voir <https://daistats.com/#/> [consultation au 04/03/2021].

du « Hodl »<sup>283</sup>, du « staking Sat » ou du « buy the dip » (visant à accumuler toujours plus d'UCN\*) ou la mise en œuvre lors de pratiques rituelles, comme le jour de la « Preuve de clef » pour les *bitcoiners*<sup>284</sup>.

Que ces acteurs préfèrent les BTC ou l'ETH à la monnaie fiduciaire comme actif de patrimoine n'est pas pour nous crucial à la qualification des CM comme monnaie. Cela nous amène moins à les considérer comme irrationnels qu'à expliciter la rationalité qui est la leur. Le chapitre I l'a rappelé : selon de nombreux *coiners*<sup>\*</sup>, les protocoles de CM seraient immunisés contre la gouvernance humaine du fait de leur nature technique, d'où leur capacité à offrir un argent « *protégé contre l'inflation* », « *sous le contrôle de [leur] propriétaire et qui est susceptible de conserver sa valeur à long terme* » (Ammous 2018, p. 202). Pour les *coiners*<sup>\*</sup>, la question de savoir si les cryptomonnaies<sup>\*</sup> (CM) sont de « bonnes » ou de « mauvaises » monnaies est centrale. Ils ne sont pas les seuls. À la réponse affirmative qu'ils y donnent, les détracteurs des CM répondent par la négative : elles en sont de mauvaises. Selon notre conception de la monnaie (et de la monétisation), fait monnaie tout objet usé en compte et en paiement, et ces qualifications de « bonne » ou « mauvaise » soulignent d'emblée un avis normatif situé. Reprocher aux CM leur faible capacité à porter pleinement les fonctions canoniques, c'est oublier que l'apparente unicité de l'argent n'est ni spontanée, ni donnée une fois pour toutes, mais se construit et se maintient en dynamique grâce à l'existence d'agencements institutionnels et d'acteurs les produisant. Ces usages toujours situés président à ce que tout instrument monétaire se présente comme *Special Purpose Money* : comme l'explique Blanc (1998a), si du point de vue des instruments monétaires, rares sont les objets monétaires à la fois « *employés en compte, en paiement et comme réserve de richesse* », c'est « *entendu comme système, [que l'argent] rassemble nécessairement le principe du compte et du paiement, et celui de la conservation de la richesse lui est aussi accolé dès lors que ce système est viable et perdure* » (*Ibid.* p. 17). Pour Bitcoin et Ethereum, ces différents usages existent et s'articulent aux normes et valeurs des membres de leurs communautés. Quelques éclaircissements restent nécessaires pour savoir s'il s'agit de bonne ou de mauvaise monnaie, et ils ouvriront finalement à la question de leur gouvernance.

### II.3 AU-DELÀ DE LA REVENDICATION D'UNE ABSENCE DE GOUVERNANCE !

Cette dernière section poursuit notre tentative de caractérisation des CM, que sont Bitcoin et Ethereum, dans le champ de la monnaie. Conclusive du chapitre II, elle ouvrira sur les problématiques centrales du chapitre III à venir. C'est qu'à rechercher ce qui distingue les CM des autres formes de monnaie connues, nous serons conduit à l'hypothèse que c'est leur gouvernance qui fait leur singularité monétaire. Si, pour nous, les CM font bien monnaie, ce n'est ni dans le sens des experts monétaires, ni dans celui des *coiners*<sup>\*</sup> vocaux ! Sortir des

---

<sup>283</sup> Le terme « HODL » est né d'une faute de frappe d'un utilisateur du forum Bitcointalk en 2013. L'utilisateur, sous le pseudonyme GameKyuubi, a écrit « I AM HODLING » au lieu de « I AM HOLDING » dans un message où il expliquait sa décision de conserver ses Bitcoins malgré la volatilité du marché. Véritable « *signe de ralliement de la communauté Bitcoin* », cette formule est devenue un symbole de patience et de conviction malgré les fluctuations de prix (Cryptoast 2022).

<sup>284</sup> Ce « *Proof of Key day* », conduit chaque 3 janvier en célébration du lancement de Bitcoin, correspond à un retrait coordonné des fonds des bourses et passerelles<sup>\*</sup> par les participants. Ce faisant, ils clamant la propriété souveraine de leurs fonds, vérifient la solvabilité des tiers à qui ils font confiance et réduisent d'autant la liquidité disponible à la vente : « *les HODLers of Last Resort* » « *en prenant possession de tous les bitcoins détenus par des tiers de confiance en leur nom [...] apprendront très vite avec la preuve de la blockchain\* s'ils font partie de l'élite des HODLers ou non. Proof of Keys est l'initiation annuelle des HODLers* », voir <https://www.proofofkeys.com/> [consultation au 06/12/2023].

cadres réifiants précédents n'implique pas seulement que les CM peuvent (et doivent) être intégrées dans le champ de la monnaie sans être rabattues sur des catégories monétaires existantes, mal taillées pour elles, fussent-elles dominantes. Puisque notre point de départ n'est pas d'axiomatiser des fonctions abstraites « pures » et désincarnées que porteraient plus ou moins naturellement certaines marchandises, point d'autres désaccords. Nous contestons la perspective adoptée concernant l'existence d'une « bonne » monnaie en soi, dont l'*« essence »* sera d'être un instrument marchand unitaire, homogène et exclusif : elle renvoie à une absolutisation de qualités présupposées, fondée normativement de manière externe et en surplomb des acteurs qui en usent. De même, nous questionnerons les propositions afférentes qui croient saisir la monnaie et les CM au prisme d'une seule *concurrence* entre « bonne » et « mauvaise », envisagée comme un simple phénomène de substitution. Toutes ces propositions renvoient au même fond épistémologique que nous avons déjà critiqué et que certains *coiners*\* partagent avec leurs contemporains.

D'abord, nous reviendrons sur la polysémie et les controverses suscitées par le concept de gouvernance dans le champ académique, et préciserons l'acception positive que nous mobiliserons (I.3.1). Ensuite, nous verrons comment les ambitions libérales technicistes des *coiners*\* – selon lesquels une absence de gouvernance humaine caractériserait les CM –, réactivent une controverse monétaire ancienne sur la question de la bonne monnaie et de la gouvernance qui la garantit (I.3.2). Ensuite, partant de ce que les professionnels de l'argent négligent, l'hétérogénéité des représentations monétaires parmi les *coiners*\* et les conflits communautaires qui en découlent, nous mettrons au jour une gouvernance de type particulière mise en place pour les réguler. Nous formulerais l'hypothèse que la singularité monétaire des CM réside dans une gouvernance polycentrique dont la caractérisation relève d'enjeux primordiaux tant pratiques – cela permet d'opérer une clarification catégorielle au sein du champ des actifs numériques et de la monnaie – que théoriques. Il nous semble que seule une analyse empirique endogène devrait permettre de juger de la qualité d'une monnaie pour les membres de sa communauté de paiement (I.3.3). Finalement, cette analyse permettra de mettre en évidence l'originalité de la gouvernance des CM, que nous explorerons au chapitre III.

### **II.3.1 D'un concept de gouvernance problématique à la problématique de la gouvernance des CM**

Le concept de gouvernance, centrale dans cette thèse et dans les critiques des CM qu'il nous reste à présenter, apparaît problématique dans ses acceptations académiques (plurielles et contradictoires). Son contenu sémantique, ses fondations épistémologiques comme ses usages font débat, et dépendent des acteurs et du champ dans lequel ils en usent. La notion de gouvernance est ancienne, dérivant « *du latin “gubernare”* » signifiant gouverner, piloter un navire (Baron, 2003, p. 330). En France, l'usage longtemps équivalent de « gouvernement » (Paye, 2005, p. 13) voit son sens se modifier à la faveur du tournant libéral des années 1980-1990 : émanant du monde anglo-saxon, il puise dans la science économique, mais relève d'abord de pratiques politiques (Baron 2003; Paye 2005; Coutrot et Rebérioux 2005). D'où une polysémie et des allures d'un « *concept fourre-tout* » (Paye, 2005, p.29), fait d'entrelacements d'usages scientifiques et d'usages idéologiques rendant ardu l'établissement d'une définition unique, rigoureuse et stabilisée, et qui continue de susciter confusions, ambiguïtés et controverse à la fois dans le champ académique (Rhode 1996; Baron 2003) et dans celui des CM. Au niveau académique, si son acception large « *renvoie aux modalités d'organisation et d'exercice du pouvoir lorsque est en jeu une action collective* » (*Ibid.*, p. 2), ce concept est mobilisé au sein de cadres épistémologique et théorique parfois contradictoires dont on peut

départir deux grandes familles d'usages<sup>285</sup> : la première, originelle, est normative et prescriptive ; l'autre, que nous emprunterons, est plus positive et empirique (Boyer et Dehove 2001, Baron, 2003 ; Paye, 2005).

## Du concept de gouvernance et de sa polysémie : un concept normatif premier

La première famille d'usages fut portée par des acteurs politiques et non scientifiques, le concept de gouvernance servant de matrice à la réforme des fins et moyens de l'action publique des dernières décennies : c'est la Banque mondiale qui impose ce concept comme véhicule d'une idéologie « néo-libérale » (Rodrik 2002, Baron 2003, Paye 2005). Le premier usage particularisant du concept de gouvernance date d'un rapport de la Banque mondiale sur le développement de 1989, et vient étayer « *le concept en vue de rationaliser, déployer et relégitimer [...] ses pratiques vis-à-vis des États demandeurs d'aides financières pour leur développement* » par une série d'autres rapports (en 1992, 1994 et 2000, Paye 2005, p. 23). Cet usage stratégique permet de contourner un mandat lui interdisant d'interférer dans les décisions politiques des États quand, à l'époque, l'aide au développement et ses prescripteurs sont contestés. Les principes du « *consensus de Washington* »<sup>286</sup>, doctrine qui formule des prescriptions prenant la « *forme proverbiale d'une "liste de blanchisserie"* » (Rodrik 2002, p. 8), présideront aux politiques de développement international et aux plans d'ajustement structuraux mis en œuvre par la Banque mondiale et le Fonds Monétaire International au début des années 1980, et seront critiqués (*Ibid.*, p. 1; Baron 2003). Ce premier usage, très politique, donne des variations sous forme d'« État minimal », de « gouvernance d'entreprise »<sup>287</sup>, ou de Nouveau Management Public, qui partagent un fond idéologique et programmatique. Ces usages prennent appui et s'étayent sur les axiomes et méthodes de l'économie orthodoxe déjà abordés. La diffusion de la notion de gouvernance émane de la science économique. En science politique, c'est le livre de J. Campbell, R. Hollingsworth et L. Linberg (dir.), « *Governance of the American Economy, Cambridge, Cambridge University Press, 1991* », « à cheval sur la science économique et la science politique », qui témoigne « *de ce transfert* » (Paye 2005,

---

<sup>285</sup> Rhodes (1996) recense six usages du concept de gouvernance, en termes de : bonne gouvernance ; d'État minimal ; de gouvernance d'entreprise ; de Nouveau Management Public ; de Systèmes socio-cybernétiques ; et de réseaux auto-organisés. Les quatre premiers participent des démarches normatives, les deux restantes de celles positives.

<sup>286</sup> Formulée par l'économiste J. Williamson, issue des corpus néo-classique et monétariste, cette doctrine faisait des prêts conditionnés l'outil principal du développement et de la lutte contre les déficits budgétaires et l'endettement public (Baron 2003). Rodrik (2002) la résume en dix principes : la discipline fiscale ; la réorientation des dépenses publiques ; la réforme fiscale ; la libéralisation financière ; un taux de change unifié et compétitif ; une libéralisation du commerce ; une ouverture aux investissements directs étrangers ; la privatisation ; la dérégulation ; la sécurisation des droits de propriété (*Ibid.* p. 10). Considérant que l'*« échec »* de cette doctrine était dû à une « application inadéquate de principes solides », ces prescriptions ont été complétées par des réformes de la gouvernance et de la propriété des pays concernés, formant le « Nouveau Consensus de Washington augmenté ». Celui-ci inclut dix éléments complémentaires : gouvernance d'entreprise ; lutte contre la corruption ; flexibilisation du marché du travail ; respect des accords de l'OMC ; codes et normes financières ; ouverture prudente du compte de capital ; régimes de change non intermédiaires ; banques centrales indépendantes avec ciblage de l'inflation ; filets de sécurité sociale ; et politiques de réduction ciblée de la pauvreté (*Ibid.* Table 1, p. 10).

<sup>287</sup> Le terme de gouvernance d'entreprise « *recouvre un thème ancien, celui de la finalité des entreprises* » et peut être retracé jusqu'à « *la publication de l'ouvrage de Berle et Means, The modern corporation and private property, en 1932* » (Coutrot et Rebérioux 2005, p. 2). Indifféremment par gouvernance ou gouvernement d'entreprise en français, il tend à rendre compte de la structure et de l'exercice du pouvoir dans les firmes suivant les nouvelles relations qui s'y nouent (actionnaires, dirigeants, salariés, etc.). Prescripteur, ce concept établit les principes par lesquels les organisations (publiques ou privées) se doivent d'être dirigées par un ensemble de règles et procédures de contrôle et d'incitation des dirigeants en vue de protéger les actionnaires, dont l'intérêt devient la finalité primordiale des firmes ((Rhodes 1996; Baron 2003; Reberiou 2003; Coutrot et Rebérioux 2005)

p. 22). Dans le champ économique, l'époque voit un « *regain d'intérêt porté [...] à la fois à la gouvernance et à l'économie institutionnaliste [et] l'accent est mis sur le rôle des institutions comme mode de coordination des activités [alternatives] au marché.* » (Baron 2003, p. 341). Cette « *idée selon laquelle le marché comme mécanisme n'est pas l'unique mode de coordination* » n'est pas nouvelle et se trouve au centre de *The Nature of the Firm* de R. H. Coase, dès 1937 (Favereau 2010). En présence d'imperfections de marché (coûts de transaction\*, contrats incomplets, aléa moral, anti-sélection), le mode de coordination marchand connaît des « défaillances » que d'autres pallient, comme la coordination hiérarchique dans le cadre des firmes. Dans les années 1970, Williamson met ces problématiques au cœur de son « *New Institutional Economics* », proche du programme de recherche de la « Théorie Standard Étendue » (TSE) consistant à « *modéliser les institutions comme des règles dans un jeu formel* », analysé stratégiquement (Favereau 1997, citant Binmore 1988) et dérivant lui-même de la théorie économique « Standard ».

Au sein de cette famille d'usages, le concept de gouvernance permet moins de relativiser la place du marché que de l'absolutiser, puisqu'il « *renvoie à des mécanismes de coordination essentiellement économiques afin de réduire les coûts de coordination. L'analyse des institutions reste enfermée dans le cadre économique de l'efficience, le contrat étant l'objet unificateur des modalités de coordination.* » (Baron 2003, rejoint par Favereau 2010) Les catégories analytiques centrales sont proches, le contrat pour la TSE et les transactions\* chez Williamson. Et c'est l'opportunisme et l'intérêt individuel qui expliquent les comportements et endogénèse le marché. Le nouvel institutionnalisme coasien engendrera une théorie des « *droits de propriété comme fondement de l'ordre économique où la propriété privée est vue comme la base nécessaire de l'ordre marchand.* » (Weinstein 2013, p. 3) Hardin (1968) et sa « *tragédie des communs* », ainsi que les « *travaux plus sophistiqués [...] d'Alchian et Demsetz (1973)* », s'érigent en « *doxa économique [postulant] que les organisations sociales ne reposant pas sur l'appropriation privative des ressources mettaient en œuvre des formes non efficientes d'exploitation des ressources.* » (Coriat et Broca 2015, p. 269) Doxa qui conduit aux réformes de la propriété intellectuelle et, par ricochet, aux revendications de liberté logiciels présentée dans le Chapitre I. La gouvernance se traduit par moins de gouvernement et prescrit d'importer au cœur des secteurs publics des méthodes du management privé (normes et mesures de performance explicites, contrainte de résultats, optimisation des ressources). La gouvernance se fait relégation du politique, du pouvoir et du conflit, et si l'État et ses administrations ont leur place, c'est comme suppléants au marché pour des situations de « *défaillance* » bien circonstanciées : elle enjoint à penser *des politiques (policy)* en dehors *du politique (politics)* (Baron, 2003).

### **Retournement positif du concept : réintégrer le pouvoir et la politique**

Cette famille d'usages n'épuise pas le concept de gouvernance et une myriade d'approches en ont fait un outil heuristique au cœur de démarches plus positives et scientifiques (en science politique, sociologie, urbanisme, économie spatiale, Rhodes 1996, Baron 2003, Paye 2005). Constatant une porosité croissante entre public et privé *via* de nouveaux modes d'action publique, ces démarches interrogent les modalités de coordination à l'œuvre, faites d'une multiplicité d'acteurs et de niveaux d'intervention, en se décentrant des seuls schémas marchand ou hiérarchique opposant État et marché (Baron 2003).

Il s'en dégage des dénominateurs communs et un « *cœur sémantique* » comme des « *ambitions heuristiques* » (Paye, 2005, p. 15) : dans le cadre d'actions collectives, le concept de gouvernance sert à analyser (au-delà de leurs seuls aspects institutionnels formels) les *processus de gouvernement*, leur partie prenante, les arrangements et dispositifs mis en œuvre,

comme leurs visées et justifications. Ces approches conçoivent les processus de gouvernance comme des constructions sociales singulières qu'il faut documenter et analyser, relevant des situations locales particulières comme des interactions qui s'y nouent. Les logiques d'acteurs ne sont pas données, encloses en axiomes, mais analysées à travers les objectifs poursuivis, comme les processus décisionnels et cognitifs mis en œuvre pour y arriver<sup>288</sup>. Au sein de cette famille, la gouvernance continue de désigner l' « *art de gouverner* », mais son sens et sa portée s'enrichissent dans des directions permettant de toucher à des thématiques cruciales entourant notre objet : il n'est pas vecteur d'effacement du politique au profit de la seule coordination marchande et permet de revitaliser la question du politique et le débat entre État, marché et société civile. La gouvernance est ici au centre d'un cadre conceptuel qui vise à comprendre l'évolution des processus de coordination au cours du temps, en recouvrant un « *nouveau mode de gestion des affaires publiques fondé sur la participation de la société civile à tous les niveaux* » (Baron 2003). Ce cadre permet d'inscrire et d'analyser en son sein des modes de gestion historiquement originaux, dans des environnements marqués par une pluralité d'acteurs qui disposent, à des degrés divers, de pouvoir de décision (*Ibid.*, p. 330 rejoint par Paye 2005). Il permet de marquer une distinction franche d'avec *le gouvernement*, renvoyant à ses institutions formelles, ses représentants et ses modes de coordination et de coercition (Boyer et Dehove, 2001 ; Baron, 2003; Paye 2005). L'État, pour important qu'il reste, n'est plus de son propre fait qu'un « *acteur parmi d'autres* » (Le Galès, cité par Baron, 2003, p.334). Ses actions sont contenues dans un ensemble de processus de gouvernement plus large, résultant de la participation, multi-niveau, d'un ensemble composite d'acteurs hétérogènes d'où des collectifs peuvent « *gouverner sans gouvernement* » (titre de Rhodes 1996). La différenciation du système politique et l'entrelacement des activités privées et publiques ont donné naissance à une « *société sans centre* », « *un État polycentrique caractérisé par de multiples centres* », où « *le gouvernement central n'est plus suprême.* » (Rhodes 1996, p. 657) Si, à travers ce concept, s'affirme l'idée qu'il n'« *existe plus d'autorité souveraine unique* » (*Ibid.*), l'État et la société civile n'y sont pas pour autant conçus comme supplétifs du marché. Ce concept permet de dépasser la hiérarchisation, toujours présupposée dans le cadre des théories de la « bonne » gouvernance, entre État, marché et société civile : l'empirie interdit à ce que l'articulation entre ces trois pôles, faite d'arrangements variables en dynamique, soit « *pens[ée] a priori* » (Baron 2003, p. 338).

Notre intérêt pour les travaux d'E. Ostrom et de l'école de Bloomington s'explique justement par le fait qu'ils ont développé, au sein de l' « *Institutional Analysis and Development framework* (IAD, élargi en cadre SES - « *Social ecological system* » ; Chanteau et Labrousse 2013, p. 6) , un appareillage conceptuel dont l'avantage est de traiter explicitement de ces thématiques de gouvernance. Ce cadre d'analyse développé autour des ressources communes, « Common Pool Ressources » (CPR) - physiques ou immatérielles –, est ainsi tourné tout entier vers l'analyse de la diversité des modes de gouvernance, par des communautés « autogérées » et « polycentriques » (Ostrom 1990; Hess et Ostrom 2003; Hess et Ostrom 2007; Hess 2008; Chanteau et Labrousse 2013). Conçu pour déchiffrer – décrire et analyser - tant la diversité institutionnelle que ses modalités d'évolutions, ce cadre semble indiqué. Fait d'une collection d'analyses empiriques disparates, couvrant des arrangements institutionnels divers, il ne présuppose pas de hiérarchie entre des types (réifiés) de coordination

---

<sup>288</sup> Les rationalités limitée ou procédurale se substituent à celles paramétriques et instrumentales pour rendre compte du fait que les relations d'interdépendance entre les acteurs impliquent des comportements évolutifs et non prédictibles (suivant H. Simon ; Baron 2003, p. 434). Si les acteurs conservent un degré de liberté vis-à-vis du contexte institutionnel auquel ils sont confrontés, cela nécessite pour eux « *d'assimiler et/ou de créer (par des mécanismes d'apprentissage)*, mais aussi *d'accepter comme légitimes (par des mécanismes de pouvoir)* ces repères et comportements » (*Ibid.*) .

ou des régimes de propriété. Il se fait cadre anormatif et agnostique, en ce que la gouvernance s'y conçoit, sans pour autant que soit présupposées les formes et fonctions qu'elle devrait revêtir. La gouvernance renvoie à une configuration toujours située d'un ensemble de règles et d'interactions – et de « faisceaux de droits » afférents, permettant « *d'échapper au dilemme simple et manichéen* » entre propriété publique et privée (Coriat et Broca 2015, p. 270). À la malléabilité de cette boîte à outils (composantes structurelles d'un système de règles, régime de propriété et faisceau de droit) répond sa systématicité : qu'importe le degré de décentralisation du système de gouvernance de la communauté étudiée, il est possible d'analyser le cadre des interactions, de définir qui a quels droits et en quels termes. Il s'agit d'un cadre rigoureux, systématique et ouvert à l'empirie et aux données qualitatives (Chanteau et Labrousse 2013 ; Allaire 2013), dont on peut affirmer qu'il s'inscrit de plain-pied dans l'institutionnalisme historique (Chanteau et Labrousse 2013). Cadre construit en opposition aux approches de types normatives précédentes, qu'il permet de critiquer, il s'inscrit dans la lutte contre la montée *irrésistible* de la propriété intellectuelle des années 1990, que critiquaient les juristes participant à la contre-offensive du logiciel libre comme Lessig (cf. Chap. I. ; Coriat et Broca 2015, p. 272).

La gouvernance permet alors de réintroduire les problématiques du politique, du pouvoir et du conflit dans l'analyse économique, sans se limiter à la coercition publique. Elle se distingue d'*« avec l'idée de gouvernement qui suppose un acteur central, dominant »* en répartissant autorité, pouvoir, responsabilités et obligations de rendre des comptes entre une myriade d'acteurs de statuts différents (*Ibid.*, p. 334). L'élaboration de consensus collectifs nécessite de prendre en compte la capacité des acteurs à créer, modifier et interpréter les règles de coordination dans un environnement donné. Avec le remplacement d'un pouvoir en surplomb par des formes plus horizontales d'autorité, les problématiques de légitimité deviennent centrales. Que ce soit celles entourant les décisions collectives et leurs résultats, ou celles créditées aux dispositifs et processus y ayant conduit (formes de démocratie participative, par exemple). Partant des transformations importantes de nos sociétés avec un désengagement de l'État au niveau national et un processus de mondialisation au niveau international, ce concept met l'accent sur les problématiques entourant les interactions entre dimension locale et globale, et les jeux d'acteurs qui en constituent la trame. L'espace se trouve endogénisé comme facteur explicatif de certains processus économiques et sociaux (Baron 2003), comme celui de l'effritement de la pleine souveraineté des États. Aux conflits d'intérêts est opposée l'élaboration de compromis collectifs, dont les fondements ne sont plus seulement juridiques, puisque l'environnement dans lequel opèrent les différentes parties prenantes à l'élaboration de consensus peut être local et infranational ou, au contraire, supranational, ou à cheval sur différents espaces juridictionnels, induisant que ces parties prenantes conservent, à des degrés divers, une capacité de définition et d'interprétation du cadre de leur coordination (*Ibid.*).

Retourné positivement, le concept de gouvernance permet de faire resurgir analytiquement autorité, pouvoir, conflit, en un mot : le politique. Appliqué aux CM, il invite par l'empirie à aller au-delà des postulats partagés par les *coiners*\* et leurs détracteurs, ceux d'une absence de gouvernance autre que celle offerte par les codes protocolaires. Postulats au cœur de la controverse (relevant de la famille des usages normatifs) qui les opposent sur la qualification des CM de « bonne » ou de « mauvaise » monnaie.

### II.3.2 Quand les CM réactivent un débat monétaire ancien : conflit symbolique et matériel autour de la « bonne » gouvernance des CM

Le contexte entourant le renouveau du concept de gouvernance est important. Il aide à comprendre comment, aux explications déjà avancées fondant les critiques formulées par les experts monétaires à l'égard des CM, s'en ajoute une autre : Bitcoin et les CM trouveraient sens

et justification au sein de cadres épistémologiques et symboliques hétérodoxes situés. Cette situation contribue à la relation compliquée qu’entretiennent entre eux les experts monétaires et les « *coiners*\* », marquée par des conflits idéologiques et des risques matériels. Les critiques de Nakamoto à l’endroit de la monnaie traditionnelle et sa centralisation renvoient, nous l’avons vu, à différentes filiations. Si les pensées cypherpunk et crypto-anarchiste du premier chapitre nous étaient étrangères, il n’en était pas de même des références au système métalliste, empruntant à la théorie autrichienne, aux partisans du *free banking* et aux « *gold bugs* » qui promeuvent le retour à l’étaillon or. N’en déplaise aux *coiners*\*, ces autres filiations des CM font que nombre d’entre eux partagent pour partie les visions monétaires de leur critiques. Avec leur libéralisme techniciste, une partie des *coiners*\* épouse le cadre marchand et concurrentiel qui sert de terreau commun aux critiques académiques : les forces de marché et la concurrence conduisent « naturellement » à sélectionner *la monnaie la plus efficace* comme intermédiaire d’échange (celle qui réduit le plus les coûts de transaction\*), d’où le fait que les propriétés d’homogénéité, d’unicité et d’exclusivité qui y sont associées sont conçues abstraitemment et universellement comme « bonnes » en soi. N’en déplaise aux académiques, ils partagent avec les *coiners*\* des vues similaires en questionnant les CM à l’aune d’une *concurrence* entre « bonne » et « mauvaise » monnaies. D’où le fait qu’ils prennent aux mots certains *coiners*\* et leur « *hyper-cryptomonétisation* » (ou l’« *hyper-bitcoinisation* » qu’appellent de leurs vœux des *bitcoincers*\*, cf. épigraphe d’Ammous) sans plus de distance critique. Dans ce sens, *coiners*\* et critiques des CM partagent la question de savoir s’il est possible et même désirable que les CM se substituent aux « *fiat monnaies* » et au système monétaire traditionnel, postulant que les CM n’ont aucune gouvernance socio-politique. C’est cette absence de gouvernance, cachant les qualités qu’ils attendent chacun d’une « bonne » monnaie, qui est au fond l’objet de leur désaccord : pour les critiques, cette massification de leurs usages n’est ni possible, ni souhaitable, en opposition aux seconds.

Cette question d’une « bonne » monnaie et, corrélativement, celle de la gouvernance qui la rend possible, renvoient à une controverse structurante du champ monétaire. Le renouveau du concept de gouvernance en a alimenté les débats récents.

### **De la bonne monnaie à la bonne gouvernance : une approche normative partagée par les *coiners* et leurs détracteurs**

L’apparition des CM, en tant qu’épreuve d’explication, a conduit à réactiver un débat ancien et structurant de l’histoire monétaire, de « la règle contre la discréption »<sup>289</sup>, histoire qui « peut-être reconstruite à partir de l’émergence progressive du concept de “monnaie neutre”, dont la réalisation pratique a toujours été l’objectif exclusif des politiques monétaires orthodoxes » (Tutin 2009, p. 10). Neutralité « intrinsèquement bonne pour l’économie » (Davies [2002], p. 171 cité par Théret 2008, p. 12), qui amène à réfléchir sur l’opportunité de règles contraignantes intangibles permettant de protéger la monnaie des interférences politiques qui essaient de l’en détourner. L’innovation des monnaies de crédit (à support papier non

<sup>289</sup> L’appellation « *Rules versus Discretion* » renvoie à la forme contemporaine de ce débat et à un article devenu classique de F.W. Kydland et E.C. Prescott, publié en 1977 intitulé : « Rules rather than discretion: the inconsistency of optimal plans », *Journal of Political Economy*, Vol. 85, No. 3. (June), p. 473-91. Cet article, référence de la Nouvelle Économie Classique (avec celui de Barro et Gordon, 1983), permet aux tenants de la règle de dépasser les critiques du camp opposé, alors dominant (théoriquement et pratiquement). Alors que la littérature plus ancienne se concentrait sur les intentions et les capacités du décideur politique à les mettre en œuvre, favorisant la discréption et la flexibilité, Kydland et Prescott renversent cette perspective. Ils conçoivent la règle comme un contrat d’engagement responsabilisant l’autorité monétaire, imposant théoriquement l’idée, au-delà de leur seul courant, que les régimes de politiques monétaires discrétionnaires sont toujours sous-optimaux relativement à ceux fondés sur la règle (Barro 1986; Salle 2013; Carré 2014).

convertible) détachées de leurs liaisons aux métaux précieux avait en son temps été l'occasion d'ouvrir vigoureusement le débat de la « bonne gestion » de la monnaie par les banques et les banques centrales (de Boyer des Roches et Rosales 2003; Kindelberger 2004 ; Tutin, 2009) et de poser les bases des activités de *Central Banking* contemporaine (Feiertag et Margairaz 2012).

### *De la « règle contre la discréption » à la « discréption-contrainte »*

Les partisans de la neutralité de la monnaie – ou de sa neutralisation – s'inscrivent dans les approches instrumentales et substantialistes déjà vues. La monnaie, comme tout bien marchand, doit sa quantité d'« équilibre » à un prix de marché. Pour qu'une monnaie soit considérée comme saine (« Sound money »), seule la stabilité de l'unité de compte doit être assurée, car la fonction de réserve de valeur est la plus importante à leurs yeux. Pour eux, les fiat monnaies ne sont pas des monnaies. La liaison au métal n'aurait pas dû être remise en cause, car elle protégeait la stabilité en érigent des contraintes exogènes à la politique monétaire, particulièrement à la création monétaire. De leur point de vue, la « bonne gestion » de la monnaie par les banques et les banques centrales renvoie alors à l'instauration de règles et de contraintes strictes pesant sur la politique monétaire et les autorités qui en sont responsables (de Boyer des Roches et Rosales 2003; Kindelberger 2004; Tutin 2009). Pour le camp d'en face (auquel nous appartenons), pas de bonne monnaie en soi : ses qualités s'apprécient suivant une logique différente et même opposée, celle de la reproduction du système monétaire lui-même, dans le respect des principes fondateurs reconnus par les citoyens. De ce point de vue, il s'agit aussi d'assurer la viabilité des échanges et du système de paiement de la communauté, en le garantissant contre le risque d'illiquidité (version classique du prêt en dernier ressort), voire aujourd'hui d'insolvabilité (le « too big to fail » contemporain, De Boyer des Roches et Rosales, 2003). La politique monétaire est une affaire d'arbitrages relatifs, et la bonne gouvernance renvoie ici à la capacité des autorités monétaires à réaliser des actions discrétionnaires légitimes dans le but d'éviter un effondrement systémique : la fonction du prêteur en dernier ressort popularisée par Bagehot en 1873 vient couronner les débats d'un XIX<sup>e</sup> siècle qui n'a jamais tant réfléchi aux rôles et fonctions des banques centrales naissantes (Kindelberger 2004; de Boyer des Roches et Rosales 2003).

Les lignes de fracture précédentes sont récurrentes dans l'histoire de la pensée monétaire : alors qu'elles étaient déjà présentes dans les débats préclassiques, on les retrouve dans les controverses entre école monétaire (*Currency School*) et école bancaire (*Banking school*), entre monétaristes et keynésiens (Kindelberger, 2004 ; Tutin, 2009). La période de 1970 à aujourd'hui marquerait la victoire des tenants de la règle et de la « *vision quantitativiste* » (Galbraith, 2008). Fini le gouvernement politique de la monnaie, place à sa « bonne gouvernance ». La théorie monétaire contemporaine et ses praticiens de s'entendre sur l'inefficacité à long terme des politiques discrétionnaires et de leur impact sur la stabilité des prix<sup>290</sup>. Ces approches *aprioristes*, *ahistoriques* et *asociales*, en préjugeant des qualités de « bonne » ou « mauvaise » monnaie, conduisent à l'établissement d'un ensemble de prescriptions normatives, qui évoluent d'ailleurs au gré des raffinements théoriques. Car si une attention particulière est accordée à « la bonne » quantité de monnaie, celle-ci, réputée exogène, doit encore sa création à la seule

---

<sup>290</sup> Voir Feiertag & Margairaz sur la construction historique de l'International central banking (Feiertag et Margairaz 2012). Le texte de Larosière, gouverneur de la Banque de France de 1987 à 1993, est également éclairant sur ce point (chap. 11). L'auteur y détaille la grande entente entre les gouverneurs de banques centrales européennes sur les questions de politique monétaire durant le Comité Delors. Feiertag qualifie ce consensus émergeant et ses acteurs de « communauté épistémique transnationale » [Feiertag et al., 2012, chap. 10]. L'absence d'effets des politiques monétaires, à plus ou moins long terme, continue cependant de faire débat (J.K. Galbraith 2008; B. Friedman 2008).

banque centrale. Puisque le bouclage monétaire et financier impose un émetteur ultime, à la fois régulateur et superviseur, cela redouble la question des règles le contraignant, précises, intangibles et publicisées. C'est à la faveur de la victoire de cette conception qu'ont émergé, théoriquement et pratiquement, les politiques de libéralisation financière<sup>291</sup> portées par les organisations nationales et internationales et le *Nouveau Consensus Monétaire*, succédané du monétarisme<sup>292</sup>, et qu'il est prescrit indépendance, transparence et crédibilité aux politiques monétaires et aux institutions qui les portent. Pratiquement, les banques centrales, leurs membres, leurs objectifs et moyens se sont vu légalement « autonomisés » du département du Trésor et des pressions politiques afférentes (B.Friedman 2008; King 1999; Feiertag et Margairaz (dir) 2012). Suivant « *Kydland et Prescott [1977] [et] Barro et Gordon [1983a,b]* », la littérature monétaire « *s'inscrit principalement [dans] la nouvelle économie classique* », dont les hypothèses centrales d'anticipation rationnelle et de taux naturel conduisent à s'attarder essentiellement sur les « *questions d'incohérence temporelle et de crédibilité des annonces des responsables de la politique économique, et de la politique monétaire en particulier* » (Salle 2013, p. 703). Dans le champ académique et politique, cette orthodoxie monétaire qualifiée de néolibérale (Rodrik 2002) s'accompagne de raffinement conceptuel qui démontre que la seule règle est insuffisante. En effet, le régime monétaire « *discrétionnaire* », selon lequel la banque centrale peut réviser sa politique monétaire quand elle le souhaite, n'est pas *a priori* satisfaisant. Mais un régime associé à un mécanisme d'engagement sur une règle ne l'est pas plus : en effet, la règle ne suffirait pas à pallier le risque d'incohérence temporelle, dans la mesure où la banque centrale conserve la possibilité de dévier d'objectif ou de stratégie au fil du temps, au péril de sa crédibilité et de la confiance que les agents leur accordent. Pour rendre crédibles les déclarations des décideurs politiques et les politiques monétaires qu'ils mènent, les règles mises en place doivent produire des résultats cohérents dans le temps et sanctionnables, donc évaluables par les agents. C'est le ciblage de l'inflation qui apparaît dans ce contexte « *comme une solution au biais inflationniste* », ce ciblage d'inflation étant considéré « *comme une règle* », où la banque centrale s'engage « *à conduire la politique monétaire selon la règle optimale, et ce grâce à la transparence imposée par ce régime* ». Pour cela, il est essentiel que les informations privées qu'elle détient sur ses objectifs réels et monétaires soient transmises au public, la transparence permettant « *de révéler cette information aux agents et [...] d'évaluer les performances de la politique monétaire. Au regard de ces performances, les agents accordent de la crédibilité à la banque centrale, qui est ainsi responsabilisée par rapport à ses objectifs (accountability).* » (Salle, 2013, p. 705) Ce « ciblage d'inflation » correspond en fait à un troisième régime, qualifié de « *discréction contrainte* », qui revient « *à contraindre la banque centrale par la transparence à agir comme si elle pouvait s'engager sur la règle optimale* » (Bernanke et al. [1999] cité par *Ibid.*).

---

<sup>291</sup> Le phénomène de libéralisation financière, débuté en 1970, renvoie à des modifications profondes des systèmes monétaires et financiers, incluant des modifications légales et réglementaires sur deux points clés : la suppression des plafonds de taux d'intérêt (Demirgüt-Kuntasli et Detragiache 1998) et la réduction ou la suppression des contrôles internationaux de capitaux (*Ibid.*; Miotti et Plihon 2001; Rodrik 2002; Mah-hui Lim 2008). Jusqu'alors prévalait pour les fiat monnaies un monnayage construit autour de régulations strictes des autorités (taux de change fixes, taux d'intérêt, etc.), une période qualifiée de « *répression financière* » par McKinnon et Shaw (1973). Cette libéralisation ouvrirait sur une période qualifiée de « *répression monétaire* » (Théret 2012, p. 20).

<sup>292</sup> Appellation de M. Goodfriend qui qualifie la refonte des politiques monétaristes, notamment la substitution d'un contrôle direct de la masse monétaire à un contrôle indirect, sous forme de ciblage d'inflation (Galbraith 2008, p. 3). L'obsession pour la lutte contre l'inflation et pour l'indépendance des banques centrales vis-à-vis du politique persiste. Cette doctrine négligeant la lutte contre le chômage et les crises financières, accordant un rôle léonin aux politiques monétaires, ces promoteurs estiment que la politique monétaire pourrait à elle seule contrôler et maintenir efficacement la stabilité monétaire et financière (*Ibid.*).

## *Les CM : une radicalisation théorique et pratique de la règle ?*

Peu de partisans de la discréption politique et citoyenne de la monnaie (qui peuvent justifier des évolutions brutales des règles) ne se réclament de ce régime de « discréption contrainte », aujourd’hui dominant au sein des banques centrales. Les *coiners*\* aussi rejettent ce régime : se réclamant d’une règle radicalisée, ils prouvent que cette « *bataille constante* » opposant « *sous un nom ou sous un autre, depuis le XVII<sup>e</sup> siècle et probablement avant* » ces deux factions monétaires « *n'est pas près de s'éteindre* » (Kindelberger, p. 62) : les CM réactivent ce conflit singulièrement, en s’annonçant comme un dépassement radical des ambitions monétaires les plus rigoristes, comme celles du monétariste M. Friedman, celles du retour à l’étalon-or<sup>293</sup> ou encore celles du *Free Banking* d’un Hayek et de ses suiveurs. Friedman avait accepté comme un mal nécessaire le fait qu’une banque centrale strictement encadrée ait la charge exclusive de l’émission et de la régulation monétaires. Mais sa « bonne » monnaie véritable manque encore. Optimiste, il la voit être « *bientôt développée, une monnaie électronique fiable - une méthode par laquelle, sur Internet, vous pouvez transférer des fonds de A à B sans que A ne connaisse B ou que B ne connaisse A. La façon dont je peux prendre un billet de 20 dollars et vous le remettre sans qu'il n'y ait de trace d'où il provient. Et vous pouvez l'obtenir sans savoir qui je suis* ». Un « *ecash* » qui, bien que facilitant les activités illégales, réduira la capacité des gouvernements à prélever les impôts, ce qui pour lui est très positif (Friedman 1999). Cet effacement souhaité des banques centrales et des gouvernements que les CM représentent fait aussi écho au courant libéral autrichien et la théorie du *Free Banking*, dont se réclament d’ailleurs des promoteurs vocaux de Bitcoin et auquel fait référence Nakamoto lui-même.

Cette convergence intellectuelle, souvent soulignée (De Filippi 2013; Dréan 2013; De Filippi et Loveluck 2016; Desmedt et Lakomski-Laguerre 2015; Rolland et Slim 2017; Dodd 2017) dépasse la simple référence indirecte. Elle s’est construite pratiquement. En 1994, N. Szabo, « *après s'être impliqué dans le mouvement cypherpunk, [va] créer sa propre liste de diffusion privée appelée libtech-l* » (Lars 2020). La liste est un lieu d’échange entre des figures cypherpunks et des économistes réputés pour leurs positions monétaires libérales, dont le dénominateur commun est d’être intéressés par l’idée de « *dénationaliser* » la monnaie. Ce qui, d’après Szabo, « *était certainement une idée marginale à l'époque où [il] travaillait et qu'il n'y avait qu'une poignée de personnes dans le monde à qui [il pouvait] en parler et qui avaient même une idée [...]. Nous étions sur une liste de diffusion, la liste de diffusion des cypherpunks et ensuite moi, Wei Dai, Hal Finney, Larry White, George Selgin et quelques autres [étions] sur une liste de diffusion que j'ai créée et qui s'appelle libtech et c'est là que j'ai eu l'idée de Bitgold et Wei Dai a eu l'idée de B-money et nous avons eu de grandes discussions là-dessus.* » (McCormack et Szabo 2019). Ainsi, la défiance vis-à-vis des autorités centrales, la recherche d’une monnaie émancipée des cadres juridiques étatiques comme, plus généralement, la

---

<sup>293</sup> La thèse en faveur de l’étalon-or, largement mobilisée par les *coiners*\* et dont les théories du Free Banking dérivent historiquement, recommande que toute émission de monnaie soit la contrepartie d’un stock d’or. L’étalon monétaire est défini par un poids et une qualité fixes d’or, et chaque unité monétaire doit pouvoir à tout moment être escomptée en ce métal, dont une valeur de marché existe. Une monnaie à contrepartie en or ne peut pas être émise arbitrairement par un État. En conséquence, ses partisans affirment que prix et taux d’intérêt ne seraient pas manipulés et que les agents économiques valideraient des plans d’action correspondant aux besoins réels de la société. Cette liaison de la monnaie au métal et à son marché ne devrait pas être remise en cause. Cette liaison érigerait des contraintes exogènes à la politique monétaire, notamment à la création monétaire. Pour Hayek, l’abandon de l’étalon-or conduirait à une crise généralisée : « la perspective qui est devant nous est celle d’une inflation indéfiniment accélérée, aggravée par le contrôle des prix, suivie d’un effondrement rapide du marché, des institutions démocratiques, et finalement de la civilisation telle que nous la connaissons » (Hayek, 1977). Ce constat conduit cet auteur à préconiser la concurrence entre monnaies privées, dont les quelques expériences historiques (cas du Free Banking intégral aux États-Unis de 1837 à 1863 ou celui de l’Écosse) acquièrent un caractère exemplaire, pourtant peu significatif (Aglietta 1992).

croyance dans la primauté de rapports interindividuels médiatisés naturellement par le marché permettent de faire se rencontrer les vues monétaires cypherpunks / crypto-anarchistes et celles du courant libéral autrichien, dont Selgin et White sont les héritiers. Depuis un point d'origine proche de l'orthodoxie, par sa conception de monnaie marchandise, cette école se fait hétérodoxe par sa position radicale ayant trait à la question de la gouvernance : suivant Hayek, l'État disposerait d'un droit « illégitime » en matière de monnayage de par la monopolisation de l'émission de monnaie (et de la définition de taux et règles d'usage) qu'il faudrait faire disparaître au profit d'une mise en concurrence d'émetteurs privés. Le marché sans entrave apparaît comme le mécanisme par lequel les mauvais acteurs sont sanctionnés et les acteurs vertueux récompensés. L'autorégulation de l'offre de monnaie est ainsi assurée et ce, sans intervention d'un gouvernement ou d'une banque centrale (Hayek, 1976).

La relation privilégiée qu'a permis de tisser la liste de diffusion de Szabo, entre des acteurs aussi différents que des cryptographes et des économistes académiques, va perdurer et se reproduire, puisque nombre de *coiners*\* et quelques économistes continuent de l'entretenir. Si la référence au système métalliste, à l'étalon-or et aux affres des monnaies de crédit prédomine dans ces discussions, c'est parce que Bitcoin et les CM développent un « *métallisme digital* » (Maurer et al, 2014 ; Mallard et al, 2018) qui mime à différents degrés les monnaies métalliques : le terme « minage » et sa contrepartie de récompense qui permet l'émission d'UCN\* filent l'analogie. Les « *coiners*\* », à la manière de leurs « *vieux cousins les gold bugs* » (J.P Koning 2019b), se présentent comme les défenseurs contre les tenants des « fiat » monnaies, nombreux, puissants et coalisés<sup>294</sup>, d'un « or numérique », d'une « monnaie saine » (« *sound money* »), supérieurs à toute autre forme du fait d'une absence de gouvernance... qui, pour les académiques, est au contraire un inconvénient rédhibitoire.

### Une opposition quant à la « bonne » gouvernance des CM

Les *coiners*\* et leurs critiques s'opposent du haut d'une épistémologie parente. Au centre de leurs disputes sur les CM trônent des questions normatives entourant les caractéristiques que doit revêtir absolument une gouvernance monétaire de qualité. Les *coiners*\*, « *plus royalistes que le roi* », reprochent aux seconds ce qu'ils conçoivent comme des compromissions et des échecs ; les autorités monétaires auraient démontré une encore trop grande dépendance à des intérêts politiques dont elles étaient censées s'être autonomisées. Si la victoire de la règle fut totale dans les esprits<sup>295</sup>, il n'en fut pas de même matériellement. Les faits des dernières décennies désavouent la doctrine de « *discretion contrainte* » : d'une part, sa poursuite s'est traduite par une recrudescence de l'instabilité économique et des crises monétaires et financières ; d'autre part, elle a conduit à un recours accru aux politiques monétaires « non conventionnelles » pourtant condamnées par ce corpus théorique. C'est à l'aune de ce conflit ancien et du contexte consécutif à la crise de 2007-2008, qui « *a eu le mérite de relancer les discussions autour de la construction d'un nouvel ordre monétaire et financier comme en son temps la conférence de Bretton Woods* » (Dupré, Ponsot et Servet 2015, p. 16), qu'il faut comprendre l'opposition entre thuriféraires et contempteurs des CM.

---

<sup>294</sup> Voir S. Livera <https://twitter.com/stephanlivera/status/1280783169503916033?s=20> [consultation au 01/06/2020] ou encore P. Rochard [https://twitter.com/pierre\\_rochard/status/1241548273938300930?s=20](https://twitter.com/pierre_rochard/status/1241548273938300930?s=20) [consultation au 01/06/2020].

<sup>295</sup> Cette vision monétaire et les pratiques qu'elle justifie font aujourd'hui consensus parmi les praticiens et les banquiers centraux, qui peuvent être conçus comme une communauté épistémique transnationale, partageant « *un ensemble de normes théoriques communes, d'analyses partagées et de choix politiques semblables : consensus sur la stabilité, la libéralisation financière et l'indépendance des BC* » (Feiertag et Margairaz 2012, p. 243).

C'est à travers un « *fiatsplaning* » virulent<sup>296</sup>, que nombre de *coiners\** critiquent le système monétaire traditionnel, contestant aux experts monétaires la pertinence de leurs analyses sur Bitcoin, ainsi que leur expertise monétaire et financière. Les *coiners\** affirment la supériorité des CM, qui seraient les seules à même de garantir transparence, crédibilité et donc cohérence temporelle puisqu'elles substituent à la gouvernance humaine du code informatique « immutable » et neutre. À l'inverse, cette absence de gouvernance conçue comme absolument désirable par certains *coiners\** est, pour les académiques, la marque rédhibitoire qu'elles ne seraient que de mauvais succédanés de monnaie.

*Pour les coiners : une absence de gouvernance, marque d'une monnaie absolument « bonne »*

Saifedean Ammous, économiste se revendiquant de l'école autrichienne<sup>297</sup> et *bitcoiner* maximaliste\* reconnu, incarne parfaitement la figure du libéral-techniciste radical univoquement mobilisée pour représenter l'ensemble des *coiners\**. Dans son livre *The Bitcoin Standard* (2018), il explique comment Bitcoin serait une meilleure monnaie que les monnaies nationales, et en quoi il pourrait servir à refonder le système monétaire international (Ammous, 2018, p. 15). Selon lui, Bitcoin n'automatiserait pas moins « *les fonctions d'une banque centrale moderne* » en les rendant « *prévisibles et pratiquement immuables* » du fait de leur décentralisation, érigant Bitcoin en « *premier exemple opérationnel et fiable d'argent numérique et de monnaie forte numérique* » (« *digital cash and digital hard money* », *Ibid.* p. 15). À la manière des monnaies parfaitement convertibles, Bitcoin est pensé comme une critique du système monétaire fractionnaire et non convertible contemporain. Les CM permettraient d'avoir à disposition une monnaie sous le plein contrôle de son utilisateur et susceptible de maintenir sa valeur à long terme (on retrouve l'idée de neutralité monétaire dans son acception de conservation de pouvoir d'achat dans le temps, et non celle d'une certitude quant aux grandeurs nominales des instruments monétaires). D'après l'auteur, Bitcoin permettrait de remédier à des problèmes aussi anciens que la société humaine elle-même et ce, plus efficacement encore qu'avec l'étalon-or d'autan.

Monnaies natives d'Internet, dépassant les frontières nationales et échappant aux contrôles gouvernementaux, les CM seraient vues comme des solutions efficaces et supérieures aux problèmes de manipulation monétaire et d'inflation, tout en permettant des transferts de valeur sécurisés sans avoir à faire confiance à des tiers. L'or est considéré historiquement comme « *le grand vainqueur de cette course* » vers une monnaie « *saine* », d'où les références récurrentes que les *coiners\** lui font. Cette référence sert pour Bitcoin et ses UCN\* à faire ressortir par contraste les avantages inédits qui seraient les leurs (Ammous, 2018, p.34). Les CM « *combine[nt] les meilleurs éléments des supports monétaires physiques, sans aucun des inconvénients physiques liés à leur déplacement et à leur transport* [leur permettant de] prétendre [à] être la meilleure technologie d'épargne jamais inventée » : elles offrent « *efficacement la liquidité de l'or dans le temps et la liquidité de la monnaie fiduciaire dans l'espace, dans un ensemble apolitique, immuable et à code source ouvert* »<sup>298</sup> (Ammous 2018,

---

<sup>296</sup> Ce terme péjoratif, à la manière du terme « *Mansplaining* », renvoie au fait qu'un *coiner\** explique à un expert monétaire la nature et le fonctionnement des « *fiat monnaies* » de manière condescendante, assurée et inexacte ou simpliste. Koning (2018f) le construit en opposition au terme indigène « *Bitcoinsplaining* » ou « *coinsplaining* », correspondant, lui, à la situation inverse. On doit à Elaine Ou (2017) son apparition, au détour d'un billet de blog critiquant une analyse de P. Krugman considérée comme fallacieuse. Si Koning reconnaît que des figures de la communauté (A. Antonopoulos) sont de bons « *coinsplainers* », il est critique de certains qui, au contraire, démontrent « *généralement une compréhension incertaine du système financier réel et de la banque centrale en particulier* » (Koning 2018f).

<sup>297</sup> Voir la biographie sur le site internet de l'intéressé <https://saifedean.com/> [consultation au 20/07/2023].

<sup>298</sup> Voir <https://saifedean.com/the-fiat-standard-chapter-1> [consultation au 05/07/2023].

p. 198-199). Et contrairement à la « *version historique de la monnaie saine, l'or* », elles offriraient « à l'individu moderne la possibilité de se soustraire aux États totalitaires, managériaux, keynésiens et socialistes » (Ammous p.202).

Pour les *coiners\** qui partagent de telles vues, nos problèmes n'ont pas d'autre source que les « fiat monnaies » et leur gestion unilatérale par les gouvernements. Ces monnaies et leur gouvernance sont présentées comme sources de tous maux : les « fiat monnaies », en plus d'être fragiles (une « fausse information » largement diffusée prétend qu'elles auraient « une durée de vie moyenne de 27 ans »<sup>299</sup>), expliqueraient le fait que l'art et de la musique contemporaine soient devenus des « déchets sans goût » par la substitution des mécènes esthètes d'antan par des gouvernements à courte vue<sup>300</sup> ; elles causeraient aussi les guerres, les violences policières et étatiques<sup>301</sup>, et même l' « effondrement des valeurs familiales » (faute à l' « hedonisme » et à la « pédophilie » de Keynes, conçu comme unique démiurge<sup>302</sup> (Ammous 2018, p. 103-109; pour une recension critique de l'ouvrage, voir Coppola 2018, d'après qui la qualité des explications sur Bitcoin n'a d'égal que le caractère « délivrant » de ses analyses). Ce type de position en appelle à un phénomène d'« hyper-cryptomonétisation » - une adoption massive des CM - qu'ils conçoivent comme salutaire. Ce à quoi s'opposent bien entendu les critiques des CM.

*Pour les professionnels de l'argent : une absence de gouvernance, marque d'une monnaie absolument « mauvaise »*

Les filiations et le « *fiatsplaining* » précédent, dont ressort souvent un portait fallacieux et caricatural des économistes et du système monétaire et financier, concourent à ce que de grands noms de l'économie (prix Nobel en tête) se soient positionnés en défensive dans les médias généralistes, avant même qu'une littérature académique n'existe sur le sujet. La dimension revendiquée comme positive de ces prises de position, fondée sur la mobilisation de travaux faits par d'autres (rarement cités), sert à appuyer des raisonnements principalement

---

<sup>299</sup> Koning (2019) retrace la généalogie de cette « fausse information »: développée à l'origine par des tenants du retour à l'étalon-or, elle sera reprise par des *bitcoiners\** de premier plan comme Jimmy Song (2017), Dan Held (2018), Barry Silbert (2019), Tuur Demeester (2015), Francis Pouliot (2018) et Adam Back (2019) sans qu'aucun ne dispose ni ne vérifie les données auxquelles il s'adosse. Pour Koning, qui les a eu trouvées et analysées, elles sont « truffées d'erreurs ».

<sup>300</sup> « As government money has replaced sound money, patrons with low time preference and refined tastes have been replaced by government bureaucrats with political agendas as crude as their artistic taste. Naturally, then, neither beauty nor longevity matters anymore, replaced with political prattling and the ability to impress bureaucrats who control the major funding sources to the large galleries and museums, which have become a government-protected monopoly on artistic taste and standards for artistic education. Free competition between artists and donors is now replaced with central planning by unaccountable bureaucrats, with predictably disastrous results ». « It is no coincidence that Florentine and Venetian artists were the leaders of the Renaissance, as these were the two cities which led Europe in the adoption of sound money. The Baroque, Neoclassical, Romantic, Realistic, and post-Impressionistic schools were all financed by wealthy patrons holding sound money, with a very low time preference and the patience to wait for years, or even decades, for the completion of masterpieces meant to survive for centuries » (Ammous 2018, p. 106-108).

<sup>301</sup> Voir respectivement [https://twitter.com/pierre\\_rochard/status/1214759099159711744](https://twitter.com/pierre_rochard/status/1214759099159711744) et <https://twitter.com/realmaxkeiser/status/1269761503613407234> [consultation au 06/07/2023].

<sup>302</sup> « It is no coincidence that the breakdown of the family has come about through the implementation of the economic teachings of a man who never had any interest in the long term. A son of a rich family that had accumulated significant capital over generations, Keynes was a libertine hedonist who wasted most his adult life engaging in sexual relationships with children, including traveling around the Mediterranean to visit children's brothels. » (Ammous 2018, p. 103)

normatifs<sup>303</sup>. Ces pontes jettent dans l'arène leur expertise et réputation afin de contrecarrer ce qui pour eux n'est rien d'autre qu'un « *techno-mysticisme à l'intérieur d'un cocon d'idéologie libertarien* » (Krugman 2018b), une nouvelle forme d'« *extrémisme de droite* », « *utilisés par des ploutocrates populistes, comme Trump, pour détruire la démocratie et créer un État autoritaire* » (Roubini<sup>304</sup>). Pour ces économistes et praticiens (banquiers ou financiers), une CM comme le Bitcoin « *soulève deux questions distinctes. Est-il durable ? Et en supposant qu'il le soit, contribue-t-il au bien commun ?* ». Ils répondent de concert « *probablement pas (le jury n'a pas encore rendu son verdict) et certainement pas* » : concernant « *la question de la soutenabilité, le bitcoin est une pure bulle, un actif sans valeur intrinsèque - son prix tombera à zéro si la confiance disparaît* ». Aussi, quand bien même « *il pourrait devenir le nouvel or, [Tirole ne] parierai[t] pas [s]es économies dessus, et [il] ne voudrai[t] pas que des banques réglementées jouent sur sa valeur.* » (Tirole 2017). Par ailleurs, « *la valeur sociale du bitcoin [...] échappe à ces critiques (Ibid.)*. Ces sommités en concluent donc que le phénomène CM ne peut et ne doit pas durer, car il serait au mieux économiquement imparfait et techniquement limité ; au pire, ce ne serait qu'une pure escroquerie, une pyramide de Ponzi vouée à s'effondrer. Ils rejoignent certains des chercheurs de science informatique qui n'y voient que « *des systèmes de paiement totalement dysfonctionnels, [voire] une fraude technologique* » (J. Stolfi , cité par Colomé 2022, cf. Chap. I, section I.1.1).

Au cœur de leur argumentaire et quelle que soit leur obédience, toutes les critiques s'accordent sur une hypothèse qu'elles empruntent aux *coiners\** sans recul critique : les CM sont conçues comme n'ayant pas de gouvernance (ou celle-ci se réduit aux seules règles protocolaires canoniques). Bien que ces professionnels de l'argent, en tant que communauté épistémique (Feiertag et Margairaz 2012, chap. 10), partagent avec les *coiners\** l'idée qu'il faille cadrer strictement les objectifs et moyens de la politique monétaire, leurs conclusions pratiques s'opposent. C'est le cas en particulier sur la question de l'immutabilité tant vantée des codes protocolaires et du monnayage des CM. Mervyn King illustre parfaitement cette opposition en affirmant « *qu'il est à la fois indésirable et impossible pour un gouvernement d'engager ses successeurs dans un régime monétaire immuable* », car les « *décisions collectives d'aujourd'hui ne peuvent pas lier les décisions collectives futures... les arrangements monétaires peuvent toujours être modifiés [suivant qu'un] très mauvais gouvernement se redonnera simplement le pouvoir discrétionnaire (Ibid., pp. 3-4)* » (King (2004), cité par Selgin 2014b, p. 24). De ce péché originel d'absence de gouvernance, qui en ferait des monnaies « apolitiques » dangereuses et fantaisistes (titre du billet de blog de Varoufakis 2013), ils en déduisent toute une série de tares monétaires, conduisant à des conclusions inverses de celles des *coiners\**. Ces critiques, qui s'attaquent essentiellement à « *certaines aficionados du bitcoin [qui] ont vu en lui* » « *une alternative pour dépasser le désordre monétaire international et la guerre des monnaies* » (Dupré, Ponsot et Servet 2015, p. 16), sont moins adressées aux CM elles-mêmes qu'aux ambitions que certains des *coiners\** les plus radicaux leur font préemptoirement porter. Et sur ce point, la conclusion de leurs contemporains est simple : elles sont de mauvaises monnaies de leur monnayage absolument déconnecté de l'économie réelle, qui les érigent en système monétaire ontologiquement inefficace et déflationniste (Varoufakis 2013; Krugman 2018a), « *incapable de stabiliser et d'équilibrer le système monétaire international ou les échanges entre systèmes nationaux* » et dont l'utilité individuelle et

---

<sup>303</sup> Krugman (2013) distingue explicitement ces dimensions, assurant que sa relégation des CM hors du champ de la monnaie est fondée positivement ; il affirme que nombre de ses critiques sont, elles, normatives. Idem pour Tirole (2017), pour qui les CM, au-delà de la question de leur soutenabilité (et à supposer qu'elles le soient), interrogent leurs contributions « au bien commun ? », de même chez Stiglitz (2017) ou Shiller (Ellyatt et Shiller 2018).

<sup>304</sup> Voir <https://twitter.com/Nouriel/status/1051079089652666368?s=20> [consultation au 08/07/2023].

collective est discutable (Tirole, 2017). Aucun d'eux (nous non plus, d'ailleurs) n'est « *impressionné par le bitcoin en tant qu'alternative à la monnaie fiduciaire* », hypothèse qui n'est ni « *probable [ni] souhaitable, dans notre situation capitaliste actuelle* » et ce, pour deux raisons selon Varoufakis (2020) : une CM « *ne disposeraient pas du mécanisme nécessaire pour empêcher les crises capitalistes de déboucher sur des dépressions qui ne profiteraient qu'à l'ultra-droite ; et [...] ses protocoles démocratiques basés sur la communauté ne contribueraien guère à la démocratisation de la vie économique* » (*Ibid.*). Tirole (2017), partant de « *l'exemple du seigneurage* », considère que, si « *une augmentation de la masse monétaire fournit traditionnellement des ressources supplémentaires au gouvernement [puisque logiquement] le produit de l'émission doit être reversé à la collectivité* », les CM les font à contrario *disparaître* puisque « *les premières pièces frappées sont allées dans des mains privées [et celles] nouvellement frappées créent l'équivalent d'une course au gaspillage* » (Tirole 2017). Or, nous l'avons vu, le seigneurage n'a pas disparu. Le monnayage des CM est moins connecté à l'économie réelle des économistes qu'aux contraintes et ressources de leur infrastructure et des acteurs qui y participent (cf. Chap. I, section I.1.2). Nous l'avons vu aussi, le statut et les qualités des monnaies nationales ne se sont pas faits en un jour : leur haut degré d'intégration à nos vies est le résultat d'un long processus.

Or, les CM ne peuvent prétendre à ce haut degré d'intégration, ni offrir les mêmes leviers d'interventions collectives aux différentes instances de régulation. Si elles ne sont pas conçues pour cela, les CM ne peuvent pas non plus « *forcer les nations à [y] renoncer* » (Golumbia 2015, p. 121) alors que « *les promoteurs du bitcoin visent à détruire l'État, socle minimal de reconnaissance des règles communautaires contre la force* » (Dupré, Ponsot et Servet 2015, p. 18). Le développement de leur usage charriera des risques, notamment pour les autorités monétaires.

### **Les autorités monétaires et leurs capacités de régulation en péril ?**

Bitcoin et les CM sont accusés d'un « *cyber libertarianisme* » fondé sur une rhétorique « *anti-gouvernementale* » et « *anti-banque centrale et/ou banque commerciale* » (Golumbia 2015, p. 119-120). À partir de cette charge idéologique, Bitcoin et les CM sont critiquées par la grande majorité des commentateurs, car elles apparaissent aussi comme un « *véritable casse-tête pour tous ceux qui considèrent les politiques publiques comme un complément nécessaire aux économies de marché* » : « *trop souvent utilisé[es] pour l'évasion fiscale ou le blanchiment d'argent [elles interrogeraient la capacité des] banques centrales [à] mener des politiques contracycliques dans un monde de cryptomonnaies\* privées* » (Tirole 2017). Le problème ici n'est plus qu'elles sont considérées comme inutiles, mais surtout comme dangereuses et toxiques. Elles sont déjà perçues comme des « *désastres écologiques* » (Dupré, Ponsot et Servet 2015; Bank of International Settlements 2018; Servet et Dufrêne 2021, entre autres) du fait de leur utilisation de la PoW\*. Mais sur le plan politique, elles sont aussi vues « *comme une arme destinée à nuire aux banques centrales et aux banques d'émission de monnaie [et par là même] à la capacité des États à percevoir des impôts et à surveiller les transactions\* financières de leurs citoyens* » (Krugman 2013). Elles se trouvent réduites par ces commentateurs à de simples outils de contournement des règlementations, favorisant des activités illégales : financement du terrorisme, contournement des contrôles de capitaux, blanchiment d'argent et fraude fiscale, échange de biens et services illégaux (*Ibid.*; Stiglitz 2017; Tirole 2017; Krugman 2018b; Krugman 2018a; Roubini 2018; Green 2021). Pourtant, les activités illégales n'ont pas attendu l'apparition des CM pour exister. Les CM sont même plus facilement traçables du fait de la nature publique des registres\* (propriétés intéressantes des dires mêmes du capitaine Edouard Klein, docteur en Intelligence Artificielle et gendarme spécialisé dans le cyber, Observation participante n°12), relativement aux « *fiat monnaies* » et au cash qui lui, est réellement

anonyme. Que dire de la cohérence des critiques qui, dans un paragraphe, ramènent les CM à de purs actifs spéculatifs et expliquent leur dangerosité sociale dans le paragraphe suivant, car des groupes terroristes se financent avec ces mêmes actifs financiers ?

En outre, parce que les CM ont un monnayage automatique permettant d'émettre leur UCN\* hors du giron étatique, elles seraient incapables de s'adapter aux conditions macroéconomiques (Varoufakis 2020) et participeraient à priver les États et autorités monétaires de leurs capacités d'intervention (Tirole 2017). Ces risques pratiques avaient déjà été soulevés avant les CM. Dès les années 2000, les nouvelles technologies d'information et de communication, en particulier l'émergence des « monnaies électroniques », avaient conduit à des débats similaires. Inspirants pour notre objet, ils concernaient tant le statut de ces innovations monétaires que les bouleversements potentiels à en attendre (Bounie 2001; Aglietta et Scialom 2002; Bounie et Lavoisier 2003). La monnaie électronique n'est pas une innovation récente, ne serait-ce que parce que les impulsions électriques sont le support des monnaies scripturales. Précédant l'apparition des CM d'une petite dizaine d'années, ces débats ont établi que, en fonction de leur architecture, les monnaies électroniques n'ont pas toutes le même impact sur les systèmes monétaires préexistants à leur création. Partant de la distinction entre système de paiement et système de règlement, établie par Shackle en 1971, Bounie (2001) distingue trois types de systèmes de paiement électronique : le premier s'articule encore autour d'un compte bancaire ; le deuxième s'ancre autour d'un compte non bancaire ; tandis que le troisième correspond à une nouvelle forme de monnaie, la « monnaie électronique » pure. Il importe de différencier les types en fonction de la profondeur des modifications qu'ils entraînent sur la structure hiérarchisée préexistante. Car des différences qualitatives importantes existent, et seuls les systèmes relevant du troisième type sont considérés comme potentiellement problématiques (Bounie, 2001). Aglietta et Scialom (2002) précisent que seul le circuit de règlement mobilisé est déterminant pour juger de l'aptitude d'une monnaie à s'autonomiser du système monétaire dont elle est issue. Ainsi, le développement des deux premiers types, qualifiés de « monnaies électroniques » de première génération, n'est pas conçu comme problématique, ce qui n'est pas le cas du troisième, recouvrant, lui, les monnaies électroniques dites de deuxième génération (Bounie 2001; Aglietta et Scialom 2002; Sitruk 2008). L'innocuité du premier groupe tiendrait au fait que ces systèmes opèrent encore dans l'espace contrôlé par la banque centrale : les paiements circulent dans un circuit fermé contrôlé par les banques qui restent un passage obligé. Leurs monnaies restent libellées en unité de compte nationale et utilisent pour les règlements le stock de monnaie traditionnelle. Mais ce n'est pas le cas des monnaies électroniques de deuxième génération : construites autour de système de compensation *ad hoc* (Cohen 2002), elles s'articulent à différents systèmes de règlement et unités de compte, elles-mêmes potentiellement *ad hoc*. Ces monnaies électroniques, opérant au sein de circuits ouverts, contribuent ainsi à trois risques qui érodent la capacité de contrôle des autorités monétaires : la réduction de la demande de monnaie bancaire, la prolifération de crédit non bancaire et l'émergence de chambres de clearing privées. Les banques perdent le contrôle des règles de sécurité des paiements et deviennent dépendantes d'une multiplicité de nouveaux intervenants, non assujettis aux mêmes contraintes réglementaires et prudentielles. Si elles devaient se pérenniser et se généraliser, ces nouvelles monnaies ne seraient pas sans conséquence sur les banques (perte de compétitivité, perte de contrôle sur la chaîne de valeur, perte de clientèle) et sur les autorités monétaires (moindre capacité à contrôler la masse de monnaie en circulation, inadaptation des instruments de la politique monétaire).

Les risques perçus dépendent des représentations que l'on a sur la monnaie et sur les canaux de transmission utilisés par la Banque Centrale pour influer sur les prix et la production. Deux camps s'affrontent quant à l'effectivité de ces risques. Pour le premier, l'autonomisation d'une partie de la base monétaire que les monnaies électroniques de deuxième génération

engendrent conduira à remettre en cause la capacité effective des autorités centrales à infléchir l'économie réelle, en affaiblissant la portée de la fourniture de monnaie centrale, sur laquelle elles ont monopole et dont la demande dépend du respect de normes contrôlées (Mervyn (Bank of England - Deputy Governor) King 1999; Benjamin M. Friedman 1999; Cohen 2002). C'est alors le cœur de la politique monétaire qui s'en trouverait affecté puisqu'il ne subsisterait, pour les autorités monétaires, qu'un simple pouvoir d'influence *via* les annonces de leurs taux préférentiels<sup>305</sup> (B. Friedman 1999). C'est alors une course perdue d'avance pour les autorités publiques, les velléités de réglementation n'y changeront rien (Cohen, 2002) : il faudrait voir dans l'avènement de ces nouvelles monnaies privées la fermeture de la parenthèse monétaire, ouverte au XX<sup>e</sup> siècle, de monnaies contrôlées par les banques centrales (King, 1999, p. 14). Pour l'autre camp en revanche, les monnaies nationales et leur système hiérarchisé ne sont pas près de disparaître. Les autorités monétaires devraient tout d'abord conserver des pouvoirs d'influence sur les taux, du fait de leurs prérogatives *d'open market* ou de réescompte (Woodford 2000; Goodhart 2000). En second lieu, les monnaies nationales conserveront, du fait de leurs propriétés spécifiques (anonymat, garantie légale, routine d'usage longue), des avantages compétitifs, à commencer par celui d'être porteuses de la confiance en l'État et en ses capacités à tenir ses engagements. En définitive, la dimension symbolique de l'unité de compte sera toujours matérialisée et exprimée au passif d'une banque centrale en raison de la confiance que l'on a dans la totalité sociale qu'elle incarne légitimement. Aucun risque dès lors de voir ce type de monnaies se substituer totalement aux monnaies traditionnelles.

Les CM soulèvent donc des questions de régulation similaire aux monnaies électroniques de deuxième génération. Elles ajoutent aux caractéristiques de bidirectionnalité, d'usage de chambre de compensation et d'unité de compte *ad hoc* (Aglietta, Ponsot et Ould-Ahmed 2014) des questions et incertitudes quant à l'identité des acteurs en présence. Les risques induits par le développement à grande échelle des CM dépendront de leur capacité d'attraction de nouveaux utilisateurs, mais aussi de la capacité de rétention des monnaies nationales. Il n'est donc pas étonnant que celles-ci pensent à faire évoluer les formes monétaires qu'elles émettent. C'est à l'aune de ces débats qu'il faut appréhender les annonces actuelles de Monnaie Digitale\* de Banque Centrale (CBDC). Si les autorités monétaires considèrent le risque engendré par les CM encore marginal, du fait des volumes relativement faibles rapportés aux monnaies de réserve et autres actifs (ECB, 2015 ; Pfister 2017), elles prennent acte de l'intérêt que leur porte le grand public<sup>306</sup>. Pour parer à toute éventualité, les autorités monétaires ont développé des scénarii et des stratégies de contention, au cœur desquels l'émission de CBDC : le choix de leur architecture et de leurs caractéristiques dépendra, dans une logique défensive, des velléités monétaires privées auxquelles les autorités publiques auront à faire face et auxquelles elles

---

<sup>305</sup> Pour Friedman, c'est l'indépendance même des politiques monétaires qui est touchée : les autorités centrales continueront d'avoir un pouvoir sur la base monétaire, mais celle-ci sera rendue de moins en moins indispensable (Friedman 1999).

<sup>306</sup> Trois raisons principales à la détention des monnaies digitales sont soulignées (Pfister 2017) : le pseudonymat des transactions qui préserve la vie privée ; leur coût relativement faible pour certains types de paiement (les paiements internationaux) ; et des motifs de spéulation, voire pour s'affranchir de certaines contraintes légales (contrôles de capitaux, éviction fiscale).

s'adapteront afin de garder une influence sur la monnaie et l'économie (Broadbent 2016; Pfister 2017)<sup>307</sup>.

CM et *coiners\** participent donc, du fait de leur altérité, à réactiver un conflit ancien et structurant d'un champ monétaire opposant des courants dont l'apprehension de la monnaie est diamétriquement différente. Pire, les *coiners\** « viennent à marcher sur [les] plates-bandes » (J.P Koning 2012) d'experts réputés qu'ils critiquent en *outsiders*. Ces derniers questionnent tant les théories orthodoxes concevant la monnaie comme une marchandise (« *commodity money* ») que celles prévalant dans l'hétérodoxie, qui la conçoivent de manière « *chartale* » comme une créance sur l'État (« *claim money* ») (*Ibid.*; Selgin 2013; Beat Weber 2014b; Selgin 2014b). En ce qui nous concerne, du fait du positionnement singulier que nous avons adopté, nous n'adhérons à aucune de ces positions. La question posée en termes de substitution / concurrence entre les monnaies nationales et les CM n'est pas selon nous la bonne. Tout d'abord, il est faux de croire que les CM sont immutables, qu'elles ne s'adaptent pas à leur environnement et donc qu'elles ne disposent d'aucune gouvernance, comme l'a déjà pointé notre chapitre premier. En second lieu, caractériser cette gouvernance devient un critère de distinction déterminant dans le champ de la monnaie et des crypto-actifs\*. Par conséquent, il est impératif de l'analyser positivement, cette monnaie et sa gouvernance n'étant « bonnes » que du point de vue des acteurs et de la reproduction de la communauté de paiement, et non depuis une position normative de surplomb.

### II.3.3 Caractériser la gouvernance des CM hors normativité en surplomb : enjeu théorique et pratique d'un éclaircissement catégoriel primordial

*Coiners\** et professionnels de l'argent s'opposent quant au statut et aux qualités monétaires qu'ils prêtent aux CM, tout en partageant certains aspects d'une même épistémologie monétaire. Ils se demandent si Bitcoin, Ethereum et les CM pourraient / devraient remplacer les monnaies nationales par un processus de concurrence. Notre analyse diverge en des points importants. Si les paroles d'acteurs nous importent, nous ne les prenons pas pour argent comptant. Par ailleurs, les paroles jusqu'à présent restituées, conformément à nos problématisation et choix narratifs, ne rendent pas compte de l'hétérogénéité des vues que les communautés de *coiners\** portent en leur sein. Les critiques des CM reprennent de fait, sans plus de distance analytique, des affirmations de certains *coiners\** seulement. Mais d'autres vues, plus nuancées, existent et soulignent par là même que Bitcoin et toute CM renvoient à des communautés diversifiées, et sont donc des objets de débat. Pourquoi alors redoubler l'idéologie qui les enserre en participant à ne visibiliser que certains idéologues vocaux ? Trace d'une nature monétaire partagée avec toute monnaie, les CM relèvent de communautés de paiement « *multifacette[s], politiquement contestée[s] et sociologiquement riche[s] en fonction*

---

<sup>307</sup> La Banque d'Angleterre fut pionnière, publiant sur ces questions dès 2013 (Ali et al. 2013). Rejointe par beaucoup d'autres, elle a tôt mené des recherches sur Monnaie Digitale\* de Banque Centrale (CBDC) permettant à la banque centrale de conserver un rôle dans les politiques monétaires (Danezis et Meiklejohn 2015). Le choix des architectures et des périmètres choisis - compétition avec les monnaies fiduciaires et/ou avec les dépôts de banques commerciales – dépend des velléités privées d'autonomie. En fonction de ces choix, de nouvelles politiques monétaires pourraient être mises en place, comme le paiement d'intérêts sur le dépôt à vue et le cash numérique (positif, voire négatif), la compartimentation des marchés financiers, ou l'avènement d'un système de « banque étroite ». Dans ce scénario extrême, les banques centrales ouvriraient leurs bilans à tous les acteurs économiques en concurrence des banques, dont les parts de marché s'effondreraient du fait de la meilleure qualité du passif de la banque centrale comparativement à tout acteur privé (Raskin et Yermack 2016; Broadbent 2016; Pfister 2017).

*et sens. Il n'y a pas un Bitcoin, [un Ethereum] mais plusieurs* » (Dodd, 2017 p. 4 et 8), comme l'a esquissé notre premier chapitre.

Occulter cette diversité, c'est se priver de voir de la gouvernance là où pourtant elle apparaît, dans les conflits qu'elle implique par définition. Postuler l'absence de gouvernance, c'est abdiquer sa capacité à discerner les ensembles relationnels en jeu, leurs supports et les espaces pertinents de leur intrication. C'est perdre au même moment sa pleine capacité à réguler effectivement. Nos travaux revendentquent l'inverse. Cette gouvernance, pour énigmatique et singulière qu'elle apparaisse encore, existe et se structure autour de problématiques particulières liées aux contraintes inhérentes à l'usage des CM. Cette gouvernance met aux prises une pluralité d'acteurs, d'activités et de secteurs économiques en développement, à travers des arrangements sociaux techniques mêlant des logiques *hors-protocole*\* et *au sein du protocole*\*. C'est par leur analyse fine qu'on pourra discerner les pouvoirs relatifs des uns vis-à-vis des autres, donc les risques, responsabilités et devoirs qui pourraient s'attacher légalement à chacun. Si, comme le disait Camus, « *mal nommer un objet c'est ajouter au malheur du monde* »<sup>308</sup>, pour nous, la relégation des CM au statut d'actif financier spéculatif est un problème en soi, qui ouvre plus de questions qu'il n'en clôt. Loin de refermer la question de leur gouvernance, cela l'ouvre en grand. Car ni la logique contractuelle de signature, ni celle du sceau, permettant logiquement de différencier facilement monnaie publique et titres/monnaies privées, selon le statut de l'entité centralisée émettrice, ne semblent s'appliquer aux CM. D'où notre hypothèse d'une singularité monétaire gisant au sein d'une gouvernance d'un nouveau type, dont la caractérisation relève d'un enjeu primordial tant pratique que théorique. L'enjeu pratique est de permettre un éclaircissement catégoriel entre CM, crypto-actifs\* et autres monnaies digitales\*, sans lequel il est impossible d'établir et de rendre exécutoires les régulations tant demandées. L'enjeu théorique renvoie à la nécessité de ne pas s'appuyer sur des critères normatifs et exogènes pour préjuger, au-delà même de l'attribution d'un statut monétaire, ce qui fait ou non « bonne » monnaie et/ou « bonne » gouvernance. De telles « qualités » doivent se juger selon nous à l'aune de leur capacité respective à assurer leur reproduction dans le respect des normes et valeurs qu'elles et leur communauté de paiement portent. Le chapitre III visera justement à comprendre comment les CM et leur communauté se construisent et se maintiennent en dynamique, suivant l'implication (plus ou moins coordonnée) d'une pluralité d'acteurs participant à leur production, à leur usage et à leurs évolutions.

## Communautés hétérogènes, controverses, gouvernance duale et polycentrique

En tant que communautés de paiement, Bitcoin et Ethereum sont moins homogènes que ce que prétendent les professionnels de l'argent. Elles sont constituées de groupes monétaires différenciés en pratique et en valeur, reflétant l'existence d'une pluralité d'univers symboliques en concurrence. Nakamoto a initialement cherché à éviter l'intermédiation en utilisant un réseau\* de noeuds\* avec une coordination minimale, voire inexisteante (2008, p.8). Il n'a pas abordé le concept de gouvernance dans ses écrits, mais ses critiques des systèmes de paiement hiérarchisé et des gouvernements renseignent sur ses ambitions implicites. Les écrits de Nakamoto, ayant un statut presque sacré, (cf. Chap. I) sont souvent cités, bien que leur exégèse donne lieu à des gnoses parfois opposées. L'initiateur de Bitcoin conçoit l'immutabilité de règles protocolaires comme essentielle à la production d'un consensus décentralisé, gage d'un monnayage « sain » et d'une résistance à la censure\*. Le protocole est censé se suffire à lui-

---

<sup>308</sup> Dans *Œuvres complètes*, Vol I, p. 901-910, « Sur une philosophie de l'expression », Poésie 44, janvier-février 1944, voir [http://www.ttoarendt.com/2020/10/mal-nommer-un-objet-c-est-ajouter-au-malheur-de-ce-monde.html#\\_ftn1](http://www.ttoarendt.com/2020/10/mal-nommer-un-objet-c-est-ajouter-au-malheur-de-ce-monde.html#_ftn1) [consultation au 02/09/2024].

même du fait du consensus par PoW\* : « *toutes les règles et incitations nécessaires peuvent être appliquées grâce à ce mécanisme de consensus* » (Nakamoto 2008, p.8). Suffisance et autonomie revendiquées par le slogan « *Code is Law* », selon l’interprétation rigoriste que lui donnent de nombreux *coiners*\* (cf. Chap. III). V. Zamfir, de la communauté Ethereum, appelle cette conception la « *loi de Szabo* », en référence au cypherpunk libertarien Szabo, qui a popularisé cette interprétation. La « *loi de Szabo* », stipulant que le code informatique est souverain dans les systèmes décentralisés, a influencé « *un grand nombre de discussions [...] sur le fait que la blockchain est immuable et doit le rester* », justifiant le refus des développeurs\* « *d’apporter des modifications au protocole [...] lorsqu’ils sont engagés dans des conflits de gouvernance* [comme lors du] *débat sur la taille des blocs de Bitcoin* [dit « *Scaling Debate* »] (voir Encadré n°4 suivant), ou durant] *le hard Fork\* de The DAO* [qui donna lieu à] *une violation évidente de la loi de Szabo* » (Zamfir 2019, cf. Chap. III.3). Zamfir critique la « *loi de Szabo* » qu’il considère « *profondément et radicalement anti-juridique et anti-politique* » (*Ibid.*). Szabo favorise une gouvernance *on chain* et par le code impliquant uniquement les acteurs non humains (et leur opérateurs). Zamfir propose de fonder une « *loi crypto* » ou « *crypto law* »), intégrant l’ensemble des composantes communautaires humaines, même si leur accès au réseau\* est intermédiaire. Cette conception privilégie les dispositifs de gouvernance *off chain\**, et propose de réfléchir aux institutions décentralisées permettant de reconstruire un système politique plus démocratique et participatif.

#### Encadré n°4: Le « Scaling Debate » de Bitcoin

Le « Scaling Debate » traite des conflits sur la montée en charge de Bitcoin (cf. Chap. I). Tous les critères d'une « *controverse technologique* » sont présents (Callon 2006, p.5) : des enjeux socio-techniques, des solutions multiples reflétant des intérêts hétérogènes, en opposition... jusqu'à scission. Présent dès l'origine, le problème de la « scalabilité » devient un problème public par étapes. Dès le WP\*, certains soulignent que Bitcoin ne pourrait « *s'adapter à la taille requise* » pour concurrencer des prestataires comme « *Paypal* » (Champagne 2014, p. 35-37 et 206-207). La vulnérabilité de Bitcoin aux attaques DOS a conduit à des régulations pour assurer *efficacité et soutenabilité du réseau\** (cf. taille limite des blocs à 1 Mo, frais relais ou de poussière ; cf. Chap. I). Le trilemme des Blockchains\* (cf. Chap I) montre que la limite de 1 Mo sécurise mais contraint la capacité de traitement. À l'époque de Nakamoto, ces questions sont secondaires. Le relèvement de ce seuil devient l'objet d'une dispute que Nakamoto n'anticipait pas, pensant que « *la limite pourrait être relevée* » (Theymos 2015) « *plus tard si nous en avons besoin* » (Nakamoto 2010c). Les priorités changent avec l'explosion des frais de transaction\* et des délais de confirmation\* (orchestrées par des attaques de spam) qui donnent forme à un problème public.

Si le problème est reconnu, les diagnostics divisent. Deux camps antagonistes se forment autour de deux familles de solutions et de justification. Le camp des « *Big Blockers* » soutient que la « bonne » monnaie circule (la fonction d'échange est prioritaire). Pour être massif, l'usage de Bitcoin doit rester abordable, d'où leur soutien à l'augmentation de la taille de bloc. Le camp des « *Small Blockers* » voit Bitcoin comme un « or numérique » non censurable, car décentralisé, priorisant la fonction de réserve de valeur. Il juge cette augmentation inefficace et non viable, menaçant la décentralisation de Bitcoin. Selon eux, maintenir les transactions\* bon marché augmentera leur nombre. Imposant des blocs plus lourds, cela nécessitera des noeuds\* plus puissants et donc plus coûteux, induisant une centralisation. Maintenir les blocs petits permet à plus de personnes de maintenir un noeud. Cela incite les acteurs à optimiser l'usage qu'ils font de Bitcoin et à élaborer des solutions pérennes, comme « *SegWit* » et le « *Lightning Network* » (cf. Chap. I). Les débats sont houleux, car modifier ce seuil équivaut à « *une mise à niveau de tout un réseau\** », c'est « *un changement incompatible* » nécessitant de « *convaincre la grande majorité* » des opérateurs de noeuds\* (Garzik 2010, cf. Chap III). Chaque solution induit des coûts et bénéfices différents, selon les représentations, les intérêts et les positions des acteurs dans l'écosystème. La première augmentation de la limite est proposée en 2013, mais les débats s'intensifient en 2015 (Wirdum 2017). Les divisions parmi les développeurs\* "Core" de Bitcoin ont conduit à plusieurs tentatives d'implémentations, dont Bitcoin XT, Bitcoin Unlimited et Bitcoin Classic, toutes ayant échoué pour manque de soutien.

Certains acteurs économiques soutiennent l'augmentation immédiate, organisant des conférences pour la promouvoir. Mineurs, bourses d'échange, opérateurs de portefeuille et certains développeurs\* (M. Hearn, G. Andresen, J. Garzik) y voient un intérêt pour gérer plus de transactions\* sans augmenter les délais et coûts. Les deux camps sont représentés à la conférence dédiée de Montréal en septembre 2015, avec G. Andresen pour les « *Big Blockers* » et G. Maxwell pour les « *Small Blockers* » (Bier 2021a). D'autres suivront : Hong Kong pour toucher la communauté chinoise (Bier 2021d, Bier 2021b) ; puis Milan. Le « *New York Agreement* » de 2017, initié par B. Silbert (CEO de « *Digital Currency Group* ») et dernière tentative de conciliation, propose « *SEGWIT2X* ». Comme compromis, les signataires acceptent SegWit à la condition d'une augmentation de la taille des blocs à 2 Mo. Les signataires se vantent de représenter « *une masse critique de l'écosystème Bitcoin* » : « *58 entreprises [...] dans 22 pays, 83,28% de la puissance de hachage* », « *5,1 milliards USD de volume mensuel* » et « *20,5 millions de portefeuilles\* bitcoins* » (Bier 2021f). Vanté comme bénéfique pour entreprises, mineurs et usagers, les signataires oublient qu'ils n'ont pas mandat de représentation. Le consensus se forme autour des arguments des « *Small Blockers* », une majorité de *bitcoiners\** soutenant « *SegWit* » (« *Segregated Witness* »). Proposée dès 2015 par P. Wuille, cette modification protocolaire change le format des données transactionnelles, permettant d'en intégrer plus dans un bloc de taille inchangée (Lars 2019b). Un autre avantage est qu'il permet « *de faciliter les modifications futures du protocole* » telles que « *Lightning Networks* » (*Ibid.*, cf. Chap. I.). Minoritaire chez les *bitcoiners\**, les acteurs dominants du minage sont « *Big Blockers* ». Les noeuds\* mineurs produisant le consensus, ils pensent que le choix de changer le protocole leur revient. Shaoling Fry, développeur extérieur (« *Core dev* » Litecoin), propose l'« *User Activated Soft Fork\** » (UASF) pour activer SegWit sans l'approbation des mineurs, redistribuant ainsi le pouvoir de gouvernance aux utilisateurs et contrecarrant l'influence exclusive des mineurs. Sa méthode repose sur les noeuds\* complets menaçant de bloquer les blocs des mineurs refusant SegWit : cela mène à son adoption le 1er août 2017 sans l'augmentation de taille des blocs de SEGWIT2X. En réponse, les « *Big Blockers* », à l'initiative de l'entreprise de minage Bitmain, lancent Bitcoin Cash avec des blocs augmentés, mais sans soutien, Bitcoin Cash, une nouvelle CM est créée

Le débat portait sur les valeurs partagées entre *coiners\**, les qualités monétaires attendues (décentralisation, faible coût, etc.), les coûts et bénéfices des modifications, et les « *visions de Bitcoin* » (Carter et Hasuflly 2018). Song (2018a; 2018b) décrit ce conflit comme opposant les tenants de la règle, incarnés par les « *Small Blockers* », aux « *crypto-keynésiens* » qu'il voient en les « *Big Blockers* ». Le schisme devenu « *Indépendance Day* » de Bitcoin, où les *bitcoiners\** ont défini leur « *consensus communautaire* » (Harper 2019).

Dans le champ des CM, Szabo et Zamfir représentent les deux pôles idéal-typiques de l'éventail des conceptions de « bonne » CM, bien gouvernée, selon les *coiners*\*. Lustig et Nardi (2015, p. 1) ont analysé qualitativement cette diversité des vues, à travers le concept d'« autorité algorithmique », conçue comme la confiance placée dans les algorithmes pour diriger les actions humaines et valider les informations : ils ont montré que tous les *bitcoiners*\* ne croient pas en l'incorruptibilité de Bitcoin et qu'ils reconnaissent la nécessité des jugements et médiations sociales et humaines, même pour ce qui a trait aux CM. Des recherches similaires de DuPont (2018) sur la communauté Ethereum et à la crise de « The DAO » (cas d'étude du chapitre III), révèlent le même type d'idéaux et d'imaginaires hétérogènes, surtout sur les questions de gouvernance. Musiani, Mallard et Méadel (2018) partent d'*« événements controversés dans l'histoire récente de Bitcoin »*<sup>309</sup> pour mettre au jour « *des tensions, des conflits ou des divergences entre les acteurs concernés [que cela concerne] la modification d'une caractéristique technique, [...] l'organisation et [...] la hiérarchie entre les développeurs\* principaux, ou [...] l'introduction ou de la disparition d'un intermédiaire* » (p.134). Dans ce sens, la crise du « Scaling Debate » a révélé au grand public l'hétérogénéité de Bitcoin et sa communauté de paiement. Cette controverse autour de changements protocolaires a mis en lumière l'*« invisible politique »* de ses codes et des disputes communautaires entourant leur évolution, et une gouvernance duale (Rolland & Slim 2015 ; De Filippi & Loveluck 2016). À la gouvernance *par l'infrastructure* (codes protocolaires, selon la « loi de Szabo ») se superpose une gouvernance *sur l'infrastructure* plus large, concernant la CM, ses propriétés et les modifications éventuelles. Cette gouvernance *sur* met en conflit des composantes communautaires aux intérêts divergents. Conflits qui proviennent de « *visions de Bitcoin* » (en terme de « ecash », de « *réseau\* de paiement P2P peu coûteux* », « *d'or numérique résistant à la censure* », etc.) mutuellement exclusives (Carter et Hasufly 2018), que cette gouvernance est censée permettre de réconcilier. Cela interroge la définition du « consensus communautaire » (Harper 2019) qui prévaut : les groupes d'acteurs légitimes à participer aux décisions (opérateur mineurs dans la conception de Szabo, ou le plus grand nombre d'usagers dans la conception de Zamfir) et les types de dispositifs assurant l'expression des désaccords sont en question. L'absence de résolution du « Scaling Debate » à l'époque de l'analyse de De Filippi et Loveluck (2016) les conduit à conclure que la gouvernance de Bitcoin est en « crise » : bien que projet open source impliquant divers groupes, elle reposera sur « *un petit noyau de développeurs\* hautement qualifiés* » (p. 1 ; les développeurs\* protocolaires ou « Core dev », cf. Chap. I), menant à une « *domination basée sur l'autorité charismatique* ». Cela révélerait les « *limites de la formation de consensus entre des individus mus par des intérêts politiques et commerciaux* » différents et pointe l'existence de « *divergences entre les objectifs globaux du projet [...] et les élites trop centralisées et technocratiques* » qui en ont la charge (*Ibid.*).

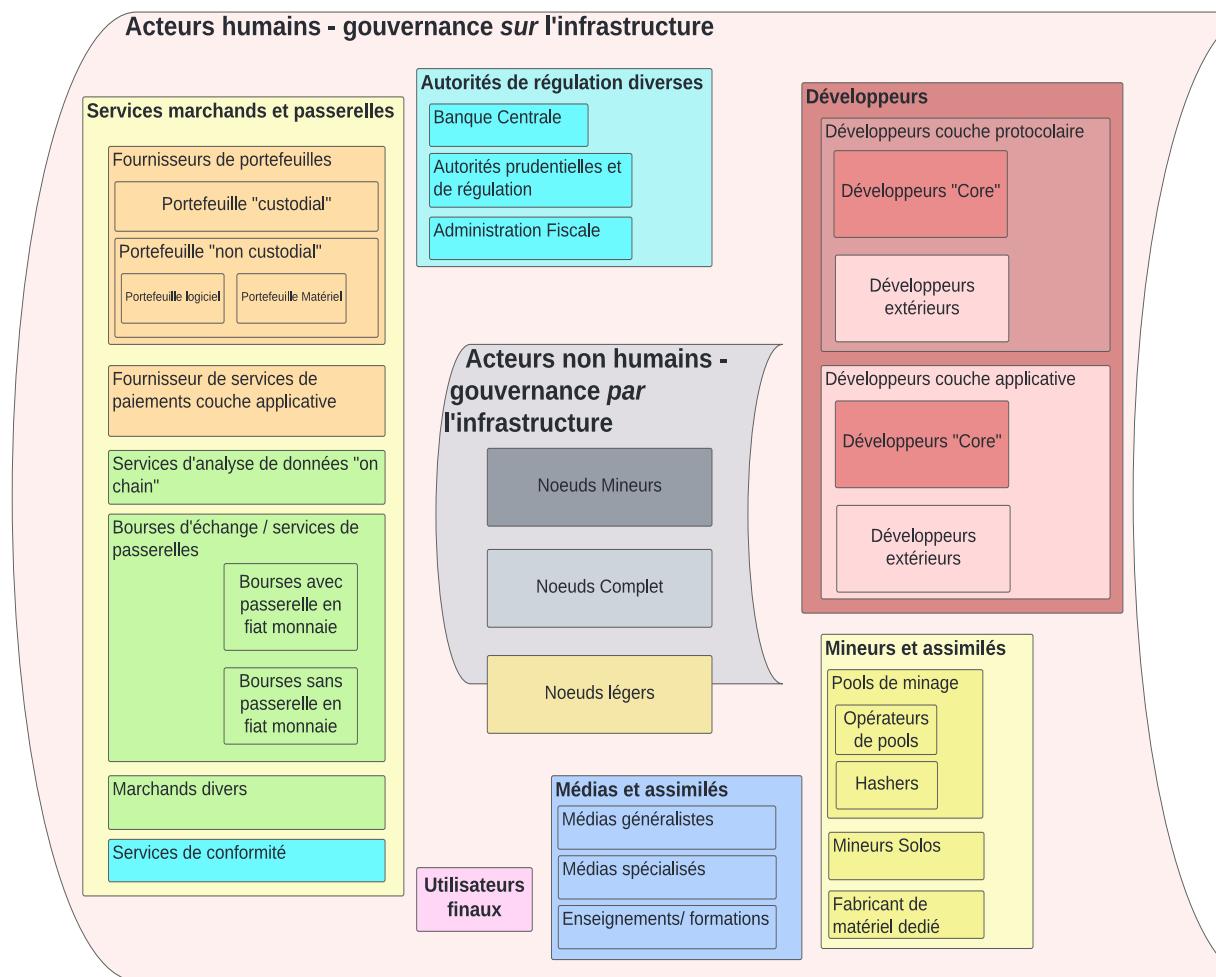
Les analyses qui, à la manière de celle de Columbia (2015), considèrent Bitcoin comme « *une manifestation de “l'extrémisme de droite distribué”* » [reflètent seulement] *la politique de certains de ses défenseurs* » et sont unilatérales (Dodd 2017, p. 6-7). L'hétérogénéité des représentations d'une « bonne » CM et de la « bonne » gouvernance qui la garantit, ainsi que les conflits qu'elle engendre, présente des caractéristiques singulières. Elle nécessite des interactions multi-niveaux et multi-acteurs complexes avec une multiplicité de centres de décision : la gouvernance duale des CM apparaît polycentrique. Avec le « Scaling Debate », Bitcoin apparaît moins comme une monnaie « acéphale » (titre de Favier et Takkal Bataille 2017) que « polycéphale ». Cette crise éclairerait une structure de gouvernance pas aussi fragile,

---

<sup>309</sup> L'une est une crise protocolaire (le Bogues CVE-2013-3220, cf. crise n°19 Chronologie 4 Chap. III), les deux autres sont plus infrastructurelles, avec les hacks et la fermeture de la bourse MtGox (Sedgwick 2019g; Sedgwick 2019h), ainsi que l'affaire de Silk Road, cf. Chap I.

ni centralisé qu'annoncé dans les mains des « Core Dev », mais distribuées autours d'eux *via* la présence d'un ensemble de canaux et d'arènes de discussion, ainsi que d'arrangement, dispositifs et mécanisme de décision. Les développeurs\* sont un centre qui doit composer avec d'autres, comme les acteurs du secteur marchand et des passerelles\*, les mineurs, renvoyant comme chez Ostrom à différentes échelles territoriales/communautaires et à différents secteurs et acteurs. La gouvernance *sur l'infrastructure* devait produire un consensus entre toutes les franges de la communauté : en tant que « *bataille pour le contrôle des règles protocolaires Bitcoin* » (Bier 2014a), le scaling debate « *a été une discussion très intéressante [,] un groupe de personnes [les acteurs économiques en faveur des big blocks poussant SegWit 2X] se sont réunies littéralement dans les coulisses et ils ont décidé que leur définition de Bitcoin est maintenant cela, et ils ont hard Fork\*é et c'est pourquoi vous avez vu un tel débat contentieux autour [.] Une sorte de large communauté a dit « allez-vous faire foutre », ce n'est pas notre définition de Bitcoin, notre définition de Bitcoin inclut les noeuds\* complets qui font partie de la décision et la communauté étant active dans ce processus de prise de décision [,] la résolution [...] a été très saine en ce sens qu'elle a établi un précédent clair sur la manière dont les changements doivent être effectués : « Non, vous ne pouvez pas décider cela dans les coulisses, oui, tout le monde doit être d'accord avec la direction que prennent les choses ».* [M. Corallo Entretien n°15]. Ce polycentrisme apparaissait dans le Chapitre I à travers la monétisation des CM et les différents domaines de développement infrastructurel qui y ont contribué, et qui sont autant de systèmes de ressources différenciés (à unité de ressources propres) servant d'appui au système de ressources qu'est le protocole de la CM. Ce polycentrisme renvoie au travail, plus ou moins coordonné, d'une multiplicité d'acteurs, groupes et composantes communautaires ayant contribué à tracer le sentier de développement infrastructurel de Bitcoin et d'Ethereum. À ce point de la thèse, il est possible de tracer le périmètre des grands groupes d'acteurs apparaissant participer à la gouvernance *sur l'infrastructure* des CM (représentés dans la Figure 7 suivante).

**Figure 7 : Cartographie préliminaire des parties prenantes à la gouvernance des CM**



Source : Rolland Maël

Du travail déjà réalisé, nous pouvons dessiner deux groupes de parties prenantes de la gouvernance des CM : les acteurs non humains de la gouvernance *par* l'infrastructure (en gris) et les acteurs humains de la gouvernance *sur* l'infrastructure, recouvrant nos huit domaines de développement (cf. Chap. I, avec le même code couleur). Contrairement à ce qu'en disent Dupré, Ponsot et Servet (2015), une CM comme Bitcoin définit tant formellement qu'informellement des groupes d'acteurs à statuts et rôles différents et qui sont partie prenante

de cette gouvernance<sup>310</sup>. Les acteurs non humains sont les clients protocolaires. Selon la loi de Szabo, il existe une hiérarchie entre des nœuds\* considérés comme passifs (les nœuds\* légers des usagers non mineurs) et les nœuds\* actifs (les nœuds\* mineurs), qui participent à la totalité des processus de consensus (vérification, production et validation\* des enregistrements). Les nœuds\* complets, bien qu'absents de l'analyse de De Filippi et Loveluck (2016), sont actifs dans la gouvernance *par* l'infrastructure<sup>311</sup> (cf. leur rôle crucial lors du « Scaling Debate » *via* la proposition d'UASF). De ce fait, nous incluons les nœuds\* complets, car même d'un rang inférieur aux nœuds\* mineurs, ne faisant que vérifier la validité d'informations qu'ils ne participent pas à produire, ils sont bien actifs dans la gouvernance *par* l'infrastructure, comme l'a prouvé le rôle important qu'ils prendront *via* la menace de l'UASF, lors du « Scaling Debate » (Lopp 2014; Rolland et Slim 2017; Janssens 2017). Nous incluons les nœuds\* légers, en contradiction à la loi de Szabo, pour montrer que tout utilisateur « inactif » peut « activement » changer de fournisseur de services, pour sanctionner des choix de gouvernance qu'il désapprouverait (comportement visible lors du « Scaling Debate »). Le statut particulier des nœuds\* légers est indiqué par leur position entre les deux logiques de gouvernance et leur couleur orange. Les acteurs humains de la gouvernance *sur* l'infrastructure incluent : les autorités de régulation (domaine de conformité aux règlementations nationales) ; les développeurs\* (domaine du protocole Bitcoin (couches 1 et 2) ; les mineurs & assimilés (domaine de l'activité de traitement des transactions\*) ; les médias & assimilés (domaine de l'information et de la connaissance) ; les utilisateurs finaux. Les services marchands et passerelles\* regroupent les domaines de la sphère d'usage (financière et réelle), des services de portefeuille et de paiement et des services de conformité.

---

<sup>310</sup> Dupré, Ponsot et Servet (2015), considèrent Bitcoin comme un « anti-commun » et nient toute dimension socio-politique en son sein, comme l'existence de toute relation sociale autre que concurrentielle, donc l'idée même de communauté. Ces conclusions, souvent reprises, reposent sur des imprécisions et erreurs, que notre Chap. III visera à amender. Déjà, les matériaux et références indigènes ne sont pas présentés et seul un corpus théorique ultra-libéral sert d'assise aux raisonnements. Pour eux, les CM ne reposent sur aucune communauté définie, les relations ne sont qu'*« on chain\**, concurrentielles et anonymes, entre des utilisateurs « prédateurs », qui s'*« enrichissent* sur le système » en ne « dépens[ant] rien pour l'améliorer » (p. 3). Ensuite, ce texte écorne le cadre et la portée théorique du cadre ostromien sur les « Communs » en ne mobilisant que les recherches sur les communs physiques, sans tenir compte de l'extension contemporaine aux communs immatériels. Ce papier entretient la « troïka de confusions » sur les droits de propriété que ces autrices combattent : confusion entre la nature du bien et le régime de propriété, entre « Système de ressources » et « Unité de ressources », entre « Propriété Commune » et « Régime d'accès libre » (Hess et Ostrom 2007, p. 119). Déclarer que « *l'idée de "commun" se différencie [...] de celle de "bien privé" et de celle de "bien public"* » (Dupré, Ponsot et Servet 2015, p. 3) entretient la première confusion, alors que ces autrices affirment qu'il « *n'y a pas de correspondance entre catégories de biens et régimes de propriété* » et que « *les common-pool ressources peuvent être détenues par des gouvernements [,] des groupes communaux, [ou] des individus privés ou des entreprises* » (Hess et Ostrom 2007, p. 119). La seconde confusion soutient qu'*« avec le bitcoin le but n'est pas de répartir le plus équitablement possible sa distribution. Il est au contraire de développer une rivalité concurrentielle de façon à ce que sa rareté s'accroisse, au profit de ceux qui le détiennent déjà »*. La distinction entre « système de ressources » et « unité de ressources » est ignorée, pourtant l'empirie démontre que, si un système de ressources est souvent collectivement détenu, les unités de ressources, elles, peuvent être appropriées individuellement (Hess et Ostrom 2007, p. 119). En outre, sont invisibilisées les réflexions communautaires originales autour de la PoW\* comme modalité d'émission monétaire équitable, même si cela est en pratique discutable.

<sup>311</sup> Ces auteurs partent des seuls nœuds\* mineurs et nœuds\* légers, sans tenir compte de la diversité d'autres types de nœuds\* que nous regroupons par simplification sous l'appellation nœuds\* complets (« *nœuds\* archive* », « *nœud\* de minage* », « *nœuds\* d'élagage* » ou « *pruned node* », Zhao 2020). Cela explique qu'ils ne considèrent actifs que les nœuds\* mineurs. Ainsi, ceux des utilisateurs finaux, des bourses d'échange et autres services qui dépendent dans leurs accès au réseau du nœud\* d'un autre acteur sont considérés comme inactifs en ce sens qu'ils dérogent la définition de la validité des blocs. Ces nœuds\* sont en réalité des nœuds\* complets, comme expliqué pour les portefeuilles\* légers dans le Chapitre I.

Posons d'emblée la distinction entre le protocole Bitcoin, en tant que système de ressources (en stock) et les unités de ressources (en flux) : les UCN\* et la capacité de traitement des données transactionnelles que ledit système permet d'administrer. Rappelons qu'un système de ressources est souvent collectivement détenu là où les unités de ressources sont appropriées individuellement et qu'il peut être constitué de sous-systèmes de ressources (plus ou moins autonomes) articulés entre eux (Hess et Ostrom 2003). Grâce aux sept faisceaux de droits majeurs des communs numériques (Hess et Ostrom 2007, p. 52-53), il est dès lors possible d'interroger les droits conférés aux groupes d'acteurs, notamment la hiérarchie singulière entre nœuds\* de la gouvernance *par* l'infrastructure, qui se traduit par rôles/pouvoirs différenciés, dont certains dépendent de la gouvernance *sur* l'infrastructure : (i) le droit d'accès à Bitcoin est effectif pour les nœuds\* mineurs et les nœuds\* complets, car les nœuds\* légers sont dépendants ici du nœud\* complet de leur prestataire de service, induisant un pouvoir et des risques (cf. Chap. I) ; (ii) le droit d'extraction, ou la capacité à obtenir une unité de ressources de Bitcoin est plus complexe (les UCN\* émises sont réservées aux nœuds\* mineurs suivant des modalités déjà explicitées, et les acteurs souhaitant utiliser les capacités de traitement transactionnel du système devront acquérir des UCN\* pour s'acquitter des frais d'usages, devant créer un bouclage offre et demande) ; (iii) le droit de management et ceux dérivés de contribution et de suppression, pour les nouveaux communs numériques, sont intéressants dans le cas des CM (le fait de pouvoir réguler l'utilisation du système et de transformer les unités de ressources en réalisant des modifications apparaît moins comme un droit individuel que collectif, relevant de la gouvernance *sur* l'infrastructure, seule capable de modifier les codes protocolaires et de voir une majorité de nœuds\* se mettre à jour pour changer les règles faisant consensus) ; (iv) le droit d'exclusion, qui permet de déterminer qui a le droit d'accès comme ceux qui ont le droit de refuser l'accès, est du même ordre. Bien qu'un nœud\* mineur ou une pool puisse censurer des adresses et des transactions\* à leur guise, la compétition entre mineurs rend ce type d'action peu effectif au niveau global. Pour modifier la mécanique protocolaire du marché des frais de transaction\* (condition d'accès/exclusion) et/ou exclure effectivement des adresses ou transactions\*, il faudrait une modification protocolaire, dépendant là encore de la gouvernance *sur* l'infrastructure. Idem pour (v) le droit d'aliénation, la capacité de vendre ou de céder le droit de management et d'exclusion de Bitcoin n'a pas de réalité au niveau du système dans sa globalité, et ne recouvre empiriquement que des droits d'acteurs au niveau des sous-systèmes de ressources participant de l'infrastructure : client de portefeuilles\*, services plus ou moins centralisés, etc.

Questionner la gouvernance de Bitcoin et d'Ethereum nécessite une cartographie de ces acteurs et de leurs relations, même sommaire. Cette étape permet d'établir les contours de la gouvernance des CM, des rôles, statuts et faisceaux de droits différenciés en présence et de cerner les modalités selon lesquelles les acteurs participent à, usent *de* et gouvernent ces monnaies parallèles communautaires d'un nouveau genre.

## **Une anarchie catégorielle problématique**

Les CM et la grande diversité des objets monétaires et financiers qui s'y apparentent nourrissent des inquiétudes chez les régulateurs (banque centrale, BRI, FMI, etc.)<sup>312</sup> et les gouvernements<sup>313</sup>, ce qui les pousse à réfléchir à l'opportunité pour les banques centrales de mettre en place de nouvelles formes monétaires, les CBDC, lâchement inspirées de l'architecture des CM. Mais avant d'identifier les risques et les opportunités de ces objets,

---

<sup>312</sup> Voir Mme Lagarde, directrice du FMI (Lagarde 2017; Lagarde 2018) ou Mark Carney (2019) de la Bank of England.

<sup>313</sup> Voir la tribune du ministre français de l'Économie, Bruno Le Maire (2019), par exemple.

comme d'adapter leur fonction de réaction aux évolutions portées par l'écosystème, encore faut-il avoir des éléments définitionnels et un cadre conceptuel précis, apte à cerner de tels objets. Et force est de constater que, au sein du champ émergeant des CM, l'indistinction règne. Les appellations, concepts et catégories clefs du champ des CM sont « *inconsistantes* », « *anarchiques* » et floues (Vergne et Swain 2017, p. 190). Tant dans les médias (*Ibid.*) qu'au sein de la littérature indigène, voire grise (Walch 2017), à l'image des cadres administratifs et légaux qui peinent à les qualifier (cf. section II.1.2). On parle indistinctement de « Blockchain », de « cryptomonnaies\* », de « crypto-actifs\* », de « monnaies digitales\* », de « cyber-monnaie » et même de « cryptomonnaies\* d'État »<sup>314</sup> ! Certains vantent une technologie miracle qui, à elle seule, permettrait d'établir une traçabilité parfaite des marchandises, une gestion de l'identité et des cadastres, des voies de gouvernance, de vote démocratique, une meilleure gestion des chaînes d'approvisionnement, etc. (Iansiti et Lakhani 2017 ; Lehr et Lamb 2018). Difficile de s'y retrouver face à des appellations non encore stabilisées, auxquelles s'attachent des concepts et des visions différents, voire antinomiques, suivant les situations, les technologies et les acteurs en présence (la présentation des Altcoins\* du chapitre I a ébauché cette diversité).

Le manque relatif de littérature académique explique l'absence d'un cadre conceptuel conventionnel bien défini (soulignée par Bano et al, 2017 ; Bonneau et al, 2015 ; Walch, 2017 ; Rauchs et al, 2018). Cette indétermination est problématique tant pour les chercheurs que pour les organismes de régulation qui sont confrontés au langage *indigène* forgé par les praticiens. Ce langage *emic* et ses catégories (« décentralisation », « désintermédiation », etc.), qui évoluent au gré des changements de stratégie économique et discursive des acteurs, peut malheureusement se trouver repris sans discussion par certains académiques (Iansiti et Lakhani 2017, par exemple), voire - et cela est plus dangereux - par des autorités de régulation (voir (*Ibid.*; Walch 2017b; Walch 2019)). De ce fait, forger un langage *etic*<sup>1</sup>, comme cadre conceptuel rigoureux, est nécessaire afin de pouvoir repérer et analyser les CM, les crypto-actifs\* et autres monnaies digitales\*, suivant leurs enjeux respectifs.

Derrière la même appellation générique de *protocoles à registre\* distribué*, on trouve des objets socio-techniques relevant de principes différents et dont les implications seront fonction de choix technologiques et des acteurs qui les établissent. Pour le/les créateur(s) et promoteurs de Bitcoin, de telles technologies portent une contestation de l'ordre économique et monétaire, capable de le remettre en cause. Mais pour d'autres, la seule « *blockchain* » (qualification abusive selon nous<sup>3151</sup>) – libérée de son *unité de compte native* inutile et de ses voies de consensus ouvert intensives en ressources – serait vectrice d'innovation et d'optimisation des secteurs qu'elle était supposée renverser. Comme on l'a suggéré, le développement de l'écosystème des CM, que nous avons qualifié de carnavalesque, autorise une diversité d'acteurs aux vues différentes, se traduisant par des arrangements socio-techniques relevant d'arbitrages parfois opposés, en ce qu'ils réintègrent de l'intermédiation. Un protocole de registre\* distribué renvoie à un système multipartite fonctionnant sans opérateur ou autorité

<sup>314</sup> Voir <https://www.lefigaro.fr/secteur/high-tech/2018/08/20/32001-20180820ARTFIG00170-le-venezuela-veut-sauver-son-economie-grace-a-sa-cryptomonnaie-petro.php>, par exemple [consultation au 30/06/2019].

<sup>315</sup> L'usage du terme « *Blockchain\** » est une synecdoque particularisante popularisée par des slogans comme « *Forget Bitcoin, embrace Blockchain\** » émanant d'acteurs de la finance traditionnelle (en l'espèce, Blythe Master dans *Bloomberg*). Cette notion est discutable, car elle renvoie à la structure de données du registre\* en escamotant les éléments cruciaux : (i) le protocole qui le soutient et (ii) le rôle incitatif fondamental du monnayage et de l'unité de compte émise dans la production d'un consensus entre des acteurs et des nœuds\* distribués du réseau. Ce concept ne doit être réservé qu'à qualifier la structure de données pour les systèmes de protocoles de registre\* distribué fonctionnant sur cette architecture, car d'autres protocoles voient la couche de base de données prendre une forme différente que des « blocs ».

centrale, même en présence de parties peu fiables ou malveillantes (Rauchs et al, 2018). Les protocoles de registre\* distribué se définissent formellement comme « machines à consensus » qui garantissent à chaque participant de s'accorder sur un ensemble de données partagées et sur leur validité. Cela implique cinq propriétés simultanées, qui ont trait à la gouvernance du protocole considéré : (i) la production partagée du registre\* ; (ii) un consensus multipartite, ouvert ou fermé<sup>316</sup> ; (iii) une *validation indépendante\** de l'état de ses transactions\* et l'intégrité du système ; (iv) des preuves de falsification et (v) une résistance à l'altération / censure unilatérale des enregistrements présents et passés (c'est-à-dire l'historique des transactions\*, voir *Ibid.*, p. 77). Ces caractéristiques permettent une première caractérisation d'objets socio-techniques pourtant très différents dans leurs formes et leurs fonctionnements. Au niveau protocolaire, d'abord. Rauchs et al. (2018, p. 77) ont montré que, si Bitcoin et Ethereum « *satisfont [à ces] cinq propriétés* » essentielles, ce n'est pas le cas d'autres protocoles, comme Ripples présenté dans le premier chapitre : pour le protocole de consortium fermé de Ripple, « *l'influence de Ripple Labs sur les nœuds\* de validation\* rend litigieuses les propriétés de consensus multipartite et de résistance à la falsification* » (*Ibid.*). Cette influence problématique sur l'établissement *ad hoc* du collège de pairs autorisé à produire les enregistrements n'est pas sans rappeler les protocoles de consensus classique et centralisé, que pourfendait Nakamoto. À cette diversité des protocoles de registre\* distribué s'en ajoute une autre : au sein de chacun des protocoles de registre\* considérés existent des protocoles applicatifs ou Dapp reposant eux-mêmes sur des UCN\* propres (*token* ou jetons), porteurs d'usages monétaires ou non (cf. les ICO que le chapitre I illustre). Ces protocoles applicatifs et leurs UCN\* posent là encore la question de leur degré de décentralisation et de l'influence potentielle d'un centre. Leurs design et paramètres socio-techniques peuvent octroyer plus ou moins de pouvoir à l'équipe de développement : influence et pouvoir sur les codes sources, sur la participation au réseau\* ou sur le prix des UCN\*, du fait de la part relative de la masse totale en circulation qu'ils détiennent, comme l'illustre parfaitement *Ripple Labs*. Au sein de cette diversité, Bitcoin et Ethereum sont pris comme référents de la catégorie de CM, car ils apparaissent comme des constructions monétaires inédites. Mais il n'en est pas de même pour de nombreux objets qui, comme de nombreuses innovations financières, ne représentent que du « *vieux vin, mis dans de nouvelles bouteilles* » (titre de l'article de Mah-hui Lim 2008, concernant les crédits hypothécaires) : malgré leurs atours innovants, pléthore de monnaies ou d'actifs numériques circulant au sein de protocoles de registre\* distribué voient les conditions d'émission et de circulation des UCN\* et celles entourant les codes sources protocolaires relever de logiques centralisées connues de longue date.

### **Caractériser la gouvernance des CM : une voie de remise en ordre ?**

Les propriétés distinctives précédentes permettent d'y voir clair dans le champ des protocoles de registre\* distribué. Complémentés par les outils conceptuels de l'institutionnalisme monétaire, ils permettent selon nous de remettre de l'ordre au sein de l'anarchie catégorielle dans le champ de la monnaie. La distinction conceptuelle entre la logique contractuelle de la signature propre à la finance et celle fiduciaire du sceau, au cœur de la monnaie (Orléan 1998, repris par Scialom 2003), permet d'aborder des problématiques de gouvernance en questionnant le statut juridique de l'émetteur, la qualité de la signature qu'il appose sur sa monnaie ou son titre et la confiance/défiance qui peut s'y développer.

---

<sup>316</sup> Les conditions de participation à la production du consensus protocolaire (degré d'ouverture / fermeture de transaction) permettent de distinguer deux types de protocoles de registre\* distribué : (i) les systèmes « ouvert[s] et sans autorisation » (« permissionless »), comme Bitcoin et Ethereum et des « protocoles fermés avec autorisation » (« permissionned »). Rauchs et al. (2018, p. 24).

Nous l'avons vu, si les CM font porter des risques similaires aux monnaies électroniques de deuxième génération, elles s'en distinguent en n'ayant ni dimension strictement nationale, ni émetteurs centraux reconnus, ce qui est au cœur de la définition légale des monnaies électroniques. Leur espace territorial premier est l'Internet, elles s'inscrivent dans un localisme monétaire communautaire (quoique des localismes étatiques ou infra-étatiques puissent s'y étayer *via* des expériences et arrangements socio-techniques *ad hoc*, cf. l'acceptation en paiement d'impôts locaux, octroi à leur UCN\* d'un statut de monnaie légale et forcée). Malgré les efforts de conception réalisés afin que leur monnayage s'approche de celui des monnaies métalliques, les CM ne s'adossent nullement à une marchandise ou à un passif de personnalité tierce, contrairement au Ripples ou au *stable coin* USDT, suivant l'influence respectivement des entreprises *Ripples Labs* et *Tether Limited*, par exemple. Ces Tokens sont des crypto-actifs\* puisqu'ils relèvent d'émetteurs privés reconnus juridiquement et voient la confiance prêtée par les usagers, donc leur liquidité, reposer sur une logique contractuelle de signature. De même pour de nombreux autres crypto-actifs\* qui, sans être garantis par des dollars conservés par l'entreprise Tether (dont est évaluée régulièrement la crédibilité des annonces en termes de réserves), voient leurs protocoles ou la valeur de l'UCN\* dépendre de l'action discrétionnaire d'acteurs reconnus, disposant de pouvoirs discrétionnaires plus ou moins formels (Ripples en est un bon exemple). La confiance dans ce type de monnaie / titres privés est fragile, car elle repose en dernier ressort sur la signature d'émetteurs de qualités différentes, dont s'éprouvent pratiquement la crédibilité et la solvabilité, d'où l'existence de risques ouvrant à la survenue de défauts de paiement.

À l'inverse, les CM n'apparaissent pas fondées sur cette logique contractuelle et privée, mais bien plus sur une logique fiduciaire qui, si elle n'est pas de « sceau », au sens d'une puissance publique incarnée formellement, suppose la confiance en une puissance publique incarnée dans une communauté informelle. L'émetteur d'une CM n'est pas tant un mineur isolé victorieux dans la course à la découverte d'une PoW\* valide, que le protocole qui délègue ses fonctions à un ensemble d'acteurs qui en assure le fonctionnement. De ces considérations provient notre rejet d'un statut d'actif financier premier (qui se réduit à la présence de la logique de signature). Nous contestons aux *coiners*\* la prétention que les CM seraient des objets techniques autonomes et souverains, gouvernés par leurs seuls codes sources, hors interventions humaines. Pour autant, les CM comme Bitcoin et Ethereum n'apparaissent pas relever formellement d'une ou plusieurs entité(s) formelle(s), qui disposerai(en)t sur celles-ci d'un pouvoir exorbitant. Reconnaître une logique fiduciaire au cœur des CM explique qu'elles se fondent si facilement dans la définition d'une « fiat monnaie » au sens que leur donne une épistémologie nominaliste (Maurer et al 2014; Kindelberger 2017) non étatiste. Nous soutenons que les CM bitcoin et ether, en tant que créances au porteur sur le protocole d'émission qui les accepte en paiement des services offerts, sont des monnaies parallèles de type communautaire. A la manière des monnaies nationales, leur monétisation au sein de leur communauté de paiement repose sur une confiance distribuée (Mallard et al., 2014), leur valeur et leur pouvoir d'achat sont auto-référentielles et trouvent à être garantis, par un ensemble d'institutions, d'acteurs, de relations sociale, à la différence près du statut de ces garants. Néanmoins, derrière cette logique fiduciaire commune aux monnaies nationales et aux CM, se cache une différence importante. C'est en effet sur le statut des institutions et des acteurs garantissant ce pouvoir d'achat que les CM se distinguent des monnaies nationales. Non émises par un organisme de droit public (d'où leur relégation à être des monnaies privées, même en l'absence d'émetteur individuel), elles questionnent sur leur capacité à assurer une pérennité et une stabilité similaire aux monnaies nationales. À l'encontre de la « fausse information » des *coiners*\* concernant la faible durée de vie moyenne des « fiat monnaies », présentée précédemment (cf. Chap II., section II.3.2), les « fiat monnaies » sont plus pérennes que les monnaies privées. Par-delà l'identité qui incarne le collectif (le sceau renvoyant au collectif plus qu'à la personne qui le porte), leur continuité

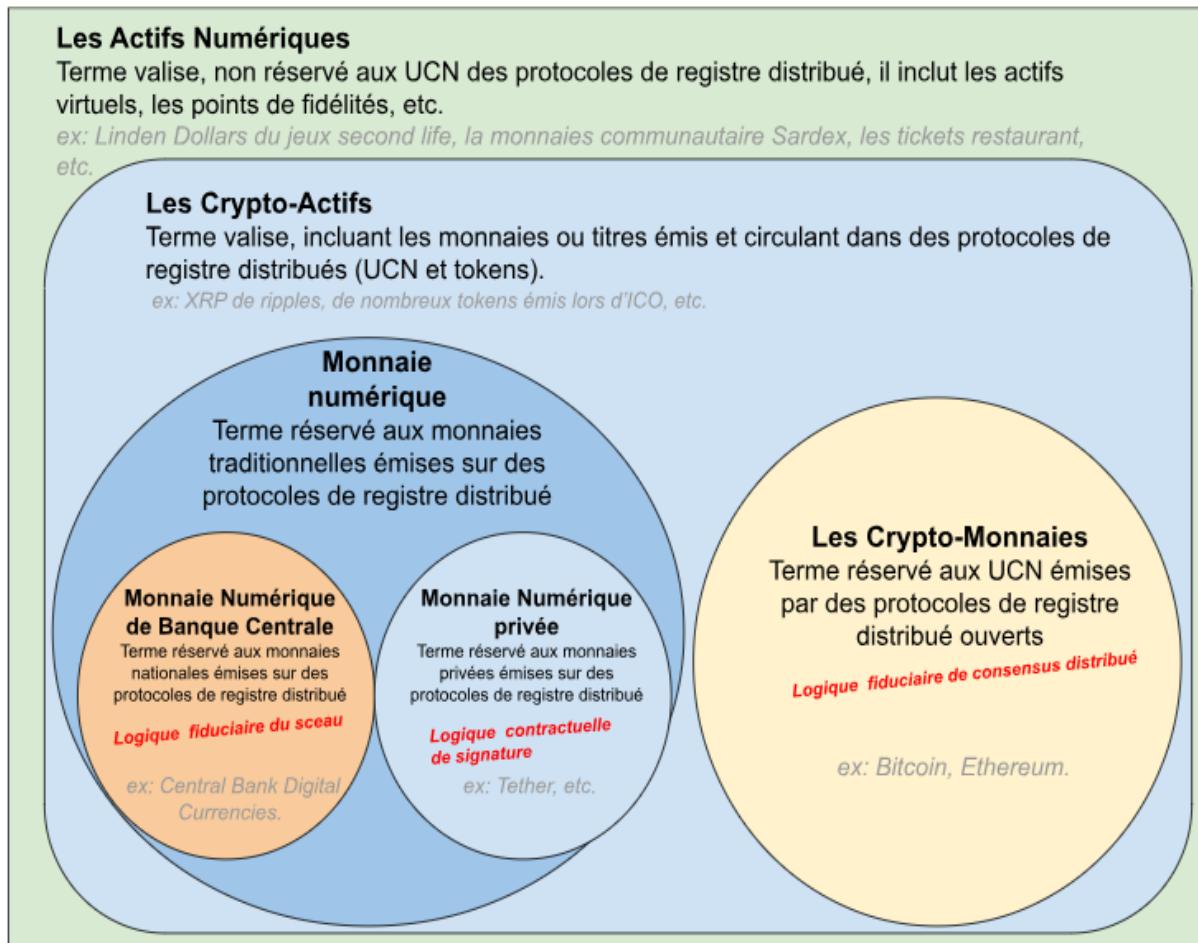
est saisie par la formule « *Le roi est mort, vive le roi* » : si un individu peut faillir et disparaître, il n’en est pas de même pour une Nation, incarnation d’un collectif politique qui ne disparaît jamais d’un coup, et tout au mieux se recompose. Une telle pérennité temporelle dérive de ce à quoi les CM ne peuvent prétendre de prime abord : une gouvernance monétaire qui s’articule plus largement à la structure formelle des États, à leur centralisation et à leur capacité de coercition. L’histoire de l’écosystème des CM et leur *turn-over* important<sup>317</sup> démontrent que les CM et leur communauté peuvent péricliter du jour au lendemain, en l’absence d’acteurs engagés dans leur développement et leur maintien. Cette fragilité rapproche les CM des monnaies privées et titres sous logique de signature. Cette altérité que les CM entretiennent vis-à-vis de la logique fiduciaire du sceau et celle contractuelle de signature conduit à proposer une hypothèse conclusive permettant une remise en ordre de l’anarchie catégorielle entourant les CM : elles sont des formes monétaires inédites, fondées sur une logique que nous qualifions (faute de mieux) « *de logique de consensus distribué* ». Ce terme permettant de retrouver l’idée de consensus, essentielle à toute monnaie, tout indiquant un polycéphalisme inédit pointant un travail communautaire et collectif de co-monnayage.

Nous proposons d’analyser la singularité monétaire de CM à partir de cette distinction entre *logique de signature*, *logique de sceau* et *logique de consensus distribué*. Se distinguent les catégories de CM, celle de monnaies digitales\* (qu’elles soient de banque centrale (CBDC) ou non) et celle de crypto-actifs\*. Nous proposons d’ordonnancer ces formes monétaires comme présenté dans la Figure 8 suivante.

---

<sup>317</sup> Voir le panorama « exhaustif » de l’évolution de l’écosystème des CM, entre avril 2013 et juin 2017 (ElBahrawy et al. 2017).

**Figure 8 : Distinguer actifs numériques, crypto-actifs, monnaie numérique et cryptomonnaie**



Source : Rolland Maël

De manière générale, l'appellation « actif numérique » est le terme le plus englobant, ne renvoyant pas seulement aux technologies de registre\* distribué, contenant aussi toute forme de monnaie ou titre virtuel (pensons aussi aux monnaies de jeux, aux points de fidélité, qui sont des actifs de ce type). Les « crypto-actifs\* » correspondent à des objets dont le point commun est d'être émis et de circuler au sein d'un protocole de registre\* distribué, pouvant indistinctement renvoyer à des monnaies ou des titres. En leur sein, on distingue les monnaies numériques correspondant à une catégorie générique<sup>318</sup>, dont la gouvernance est fondée sur un/des centre(s) établi(s), reconnu(s) et disposant de droits exorbitants. S'y distinguent les monnaies numériques privées, qui relèvent d'une logique contractuelle de signature, par exemple les UCN\* Tether dont l'émetteur a un statut juridique privé. Les monnaies digitales\* de banque centrale (CBDC) correspondent à des monnaies nationales sur une logique de sceau, dont la confiance repose en dernier ressort sur une autorité émettrice publique. Enfin, la catégorie monétaire inédite constituée selon nous autour des CM, dont les UCN\* sont émises et circulent au sein de leur protocole natif suivant une *logique de consensus distribué*, où la

<sup>318</sup> La « monnaie numérique », comme définie par Dodgson et al. ( 2015, p. 325) « désigne tout moyen de paiement qui a une équivalence en espèces, mais qui est stocké sous une forme purement numérique ».

confiance monétaire repose sur l'imbrication d'institutions, de conventions, d'acteurs et de représentations participant d'une gouvernance duale et polycentrique, qu'il reste à étudier.

Finalement, beaucoup d'objets émis et circulant sur les protocoles de registre\* distribué des CM n'en sont pas eux-mêmes et relèvent bien de logique et catégorie connues chères aux régulateurs, comme celles de crypto-actifs\* et de monnaies numériques. Selon nous, les CM s'en distinguent singulièrement et démontrent du même coup l'inanité des catégories valises actuellement mobilisées qui, trop englobantes et floues, rendent difficiles les velléités de régulation. Dans tous les cas, ces distinctions sont suspendues à la reconnaissance du type de gouvernance, donc de logiques de confiance à l'œuvre. Cela nécessite d'étudier au cas par cas la multiplicité des objets et des arrangements socio-techniques en présence et d'évaluer leur propriété de « sécurité » et de « décentralisation », suivant les choix architecturaux qui ont présidé à leur conception (cf. positionnement au sein du trilemme des Blockchains\*, cf. Chap. I, section 3.3 ), comme à leur développement infrastructurel (présence ou non d'organisation formelle en charge du développement et de la maintenance, trésorerie, etc. ; cf. Chap. I). Caractériser la présence d'une logique de consensus distribué ou d'une logique de signature renvoie à l'analyse d'éléments aussi différents que le nombre et la diversité des opérateurs de nœuds\* structurant le réseau\* (pool de minage et parts relatives dans le traitement des enregistrements, nombre de Hasheur, etc.), le nombre de développeurs\* en présence, leurs conditions de participation et les modalités d'administration des répertoires des codes sources sur les forges logicielles, puisque chacun dénote des degrés de centralisation dans la prise de décision (donc des droits et devoirs afférents aux catégories d'acteurs impliqués). De ce point de vue, Bitcoin et Ethereum apparaissent de parfaits cas d'études, en ce que leur développement jusqu'alors pérenne et leur valeur non nulle à l'échange interrogent, au-delà de la fragilité de leur « logique de co-monnayages à consensus distribué », les conditions pérennes de leur reproduction. Nous soutenons donc que si les CM sont des innovations radicales dans le champ monétaire, c'est du fait de la nature de leur gouvernance. Et si de grands types de gouvernance ont déjà été proposés pour caractériser la gouvernance de certaines CM (anarchique, hiérarchique, plutocratique, etc. ;(Rauchs et al. 2018). Un travail empirique qui reste à réaliser.

## II.4 CONCLUSION DU CHAPITRE II

Ce chapitre a cherché à apporter une contribution critique à la controverse sur le statut monétaire des CM. À travers elle, nous avons interrogé les deux propositions du syllogisme « libéral-techniciste » des *coiners*\* que nous contestons : que les CM sont des monnaies et qu'elles en sont de « meilleures » que les monnaies nationales en raison d'un prétendu apolitisme découlant d'une absence de gouvernance humaine. Pour la première proposition, nous surprenons en donnant raison aux *coiners*\*, puisque nous affirmons, malgré l'avis contraire de la majorité des analystes, que les CM font monnaie. Mais notre affirmation de la nature monétaire de Bitcoin et d'Ethereum ne repose cependant pas sur la vision libérale techniciste des *coiners*\*. Le lecteur aura également peut-être été surpris de ne trouver aucune réponse franche à la deuxième proposition. Ce refus de statuer clairement sur la qualité des CM contourne-t-il une controverse essentielle ? Cette question n'apparaît-elle pas dans toute introduction aux questions de théorie monétaire, qui rappelle la loi de Gresham selon laquelle « la mauvaise monnaie chasse la bonne » ? Cette absence de positionnement résulte en fait de notre positionnement théorique. Selon celui-ci, la qualité et la viabilité d'une monnaie s'apprécient à leur capacité à se reproduire légitimement aux yeux des acteurs et non relativement aux autres monnaies. Que les CM soient « meilleures » ou plus « mauvaises » que les monnaies nationales ne trouve pas chez nous de réponse, car les monnaies sont « bonnes »

si leur gouvernance leur permet à minima de définir et réaliser les objectifs collectifs, de gérer les conflits, de contrôler les relations de pouvoir au sein de la communauté concernée, tout en restant légitimes aux yeux de tous.

La première section du chapitre (II.1) a exploré les controverses entourant le statut monétaire des CM dans le cadre des théories économiques et monétaires existantes. Nous avons examiné les arguments des détracteurs académiques et praticiens des CM, en éclairant les fondements théoriques et épistémologiques de leurs critiques. La plupart des arguments reléguant les CM hors de la catégorie monnaie se divisent en deux grandes familles : l'approche substantialiste, instrumentale et orthodoxe de la monnaie d'une part, et le corpus nominaliste concurrent, notamment dans sa version chartaliste étatiste, d'autre part. La deuxième section (II.2) se distingue de ces deux approches par l'adoption d'un positionnement nominaliste non étatiste, qui conduit à étudier les usages et la façon dont les utilisateurs accomplissent des actions relevant des fonctions canoniques de la monnaie. Nous reconnaissions certes la pertinence de certaines critiques : indéniablement, les CM servent peu à acheter des biens et services (même illégaux), elles ont une valeur de marché très volatile, qui explique la faible propension à les dépenser, et, pour ces mêmes raisons, la part importante des usages spéculatifs. Mais il serait partiel et partial de réduire les CM à des actifs financiers « sans valeurs », les assimilant aux bulles financières et à la Tulipomania. Nous considérons que la nature monétaire des CM réside moins dans leur capacité à porter pleinement les fonctions monétaires érigées comme canoniques que dans la manière dont elles sont perçues et adoptées par les utilisateurs. Des pratiques - les usages en compte et en paiement, centraux dans notre définition de la monnaie - sont irréfutables. Les usages illégaux, par exemple, ont existé et ont été structurants en termes de monétisation, les activités légales (dont la spéculation) qui les ont marginalisé depuis 2013 le sont tout autant (cf. Chap. I.2.1). Ces transactions\*, souvent mentionnées lors de nos entretiens, participent à l'« effet whaou » des CM, à l'instar des paiements transfrontaliers qui éprouvent leur valeur monétaire aux yeux des usagers [Super Anon, entretien]. La spéculation ne se limite pas à parier sur le cours des UCN\* BTC ou ETH via des plateformes centralisées à la Coinbase (même si c'est majoritairement le cas). Ethereum a vu se développer une infrastructure monétaire et financière complexe et différenciée, où, *on chain*\*, les BTC (sous forme de WBTC) et les ETH donnent accès à de nombreux services (bourse décentralisée, protocole de prêts, emprunt collatéralisé) permettant de les échanger, les prêter ou d'emprunter d'autres UCN\* ou « stable coins ». Nous avons observé et participé à ces usages et à d'autres pratiques de compte et de paiement (événementiel, cérémoniel, crypto « finance vivrière » à la Allard 2018). Réduire ces usages à des usages en compte dérivés, comme on le fait souvent, ignore pour finir l'usage essentiel pour lequel elles ne sont pas substituables : ces UCN\* servent un type d'usage primordial qui leur est exclusif et souverain au sein de leur protocole : elles seules permettent l'expression nominale et le paiement réel de la dette ouverte par la demande transactionnelle que les frais de transaction\* permettent à régler. Comme le postule le nominalisme, la monnaie est un rapport de dette inscrit dans les règles édictées d'une entité supérieure. Si l'émetteur n'est pas l'État ou la banque centrale, il n'est pas non plus le mineur individuel : ces UCN\* représentent des créances au porteur sur le protocole, qui les accepte en paiement de l'usage de sa capacité de traitement des transactions\* et de son espace d'enregistrement. L'acceptation des CM au sein de leur communauté de paiement relève d'une fiduciarité similaire au fiat monnaie nationale où leur valeur et leur pouvoir d'achat sont garanti par des institutions et des acteurs sociaux, à la distinction près du statut de ces garants.

Dans une troisième section, la question de l'absence de gouvernance des cryptomonnaies\*, au cœur de l'argument selon lequel elles seraient supérieures aux monnaies fiduciaires, a révélé que les cryptomonnaies\* reprenaient une ancienne discussion sur la "bonne" gouvernance monétaire, touchant à des enjeux idéologiques (rôle de l'État et des banques

centrales) et pratiques (risque de perte de régulation). Nous avons insisté sur le fait que ces usages, cette capacité de traitement et cet espace d'enregistrement, sont dynamiques et évolutifs, et non statiques comme le postule la thèse selon laquelle ils sont irrémédiablement fixés par les codes protocolaires. Le développement infrastructurel de Bitcoin, retracé dans le chapitre I, a montré que le protocole connaissait des bogues et des évolutions conduisant à des controverses communautaires. Le cas du « Scaling Debate » étudié dans ce chapitre a illustré succinctement comment la communauté des *bitcoiners*\* s'était divisée dans un conflit à la Gresham : les « bons » Bitcoins des « *Small Blockers* » sont les « mauvais » des « *Big Blockers* », les premiers privilégiant la fonction de réserve de valeur au détriment de la fonction d'échange comme le désiraient les seconds. La majorité des *bitcoiners*\* a considéré l'augmentation de la taille des enregistrements comme une remise en cause inacceptable de la sécurité et de la décentralisation de Bitcoin, et de ce qui fonde sa demande comme monnaie de réserve. La victoire des « *Small Blockers* » a poussé ceux qui souhaitaient voir les bitcoins circuler massivement et facilement à faire sécession. L'usage en compte et en paiement repose sur la reproduction du système monétaire, produit d'un processus de monnayage qui dénote « *une intentionnalité collective visant à la pérennité de la monnaie* » (Théret 2008, p. 8-9). Ce processus hautement politique doit susciter l'adhésion des membres de la communauté de paiement, sans quoi c'est la crise monétaire. Les conclusions acerbes sur la gouvernance en crise de Bitcoin, tirées par De Filippi et Loveluck (2016) questionnaient la place des « core devs » de Bitcoin dans « *la structure de pouvoir technocratique* » (p. 19) empêchant la résolution du conflit. Selon leurs mots, la crise du « Scaling Debate » « *a révélé la difficulté d'établir une structure de gouvernance qui interfacerait correctement* » « *deux types de communautés différentes* », la communauté des usagers (les « *nœuds\* actifs* » et « *passifs* ») et « *la communauté des développeurs\**, qui contribuent au code du projet Bitcoin » (p. 10). Pour autant, comme nous l'avons vu, il est difficile d'affirmer qu'il faut voir dans ce débat une « *crise de gouvernance* » et « *l'échec de la résolution des conflits* », alors qu'au moment de cette recherche le « Scaling Debate » prenait tout juste forme comme problème public (pour la communauté des usagers) et n'était pas encore entré dans sa phase de résolution. Faire du *statut quo* observé, et du refus de l'augmentation de la taille des blocs qui l'a supporté, un échec de la gouvernance de Bitcoin, relève d'un jugement extérieur à la communauté[ : dire « *Bitcoin a des problèmes de gouvernance* », c'est comme "Van Gogh n'est pas photoréaliste" [, c']est vrai, mais [...] ridicule. Les Cypherpunks détestent la gouvernance. Le but était de bloquer les changements. D'autres projets ont des expériences différentes, mais ne soumettez pas Bitcoin à des normes autoritaires [...]. L'idée que les systèmes de gouvernance servent l'utilisateur moyen est constamment réfutée par l'histoire : la résistance au changement est une résistance à la capture" » (James Prestwich<sup>319</sup>). Pour la majorité des acteurs, ce long *statu quo* est plutôt de la marque d'un succès.] Le schisme communautaire et protocolaire n'était pas un bogue mais une fonctionnalité. Ce dernier peut *a contrario* être vu comme l'« Indépendance Day » des *bitcoiners*\*, comme le moment où ils ont démontré que le « consensus communautaire » n'était aux mains ni des « Core Devs », ni des mineurs et autres acteurs économiques coalisés, mais relevait d'un ensemble plus large de parties prenantes participant à la communauté de paiement.

Pour autant, De Filippi et Loveluck (2016) ont ouvert la voie en mettant au jour l'hétérogénéité communautaire, les conflits qu'elle engendre et certains des arrangements et dispositifs de la gouvernance. Il est désormais impossible d'occulter la diversité des communautés de *coincers*\*. Paradoxalement les académiques et praticiens critiques qui veulent

---

<sup>319</sup>

[https://twitter.com/\\_prestwich/status/1114568012726583296](https://twitter.com/_prestwich/status/1114568012726583296) & [https://twitter.com/\\_prestwich/status/1114569752477753344](https://twitter.com/_prestwich/status/1114569752477753344) [consultation au 04/07/2019]

réguler (voire interdire) les CM, parce qu'ils postulent une absence de gouvernance humaine des CM, gage de leur « mauvaise » qualité monétaire, perdent du même coup leur capacité à réguler effectivement. Cette absence présupposée, en plus d'être factuellement fausse, les fait abdiquer leur capacité à discerner les ensembles relationnels en jeu (les types d'acteurs humains, non humains et leur dépendance ou non), leurs supports et les espaces pertinents de leur intrication (*on chain\**, *off chain\**). Nos travaux affirment l'inverse.

L'hypothèse conclusive de ce chapitre est que la singularité monétaire des CM réside dans une gouvernance duale et polycentrique, les plaçant dans une nouvelle catégorie de monnaie, distincte des monnaies privées ou publiques existantes, fondée non sur la logique fiduciaire du sceau ou celle contractuelle de signature, mais sur une logique de consensus distribués, qui s'établit comme critère de clarification catégoriel dans le champ monétaire et crypto-monétaire séparant clairement les CM des autres crypto-actifs\* et monnaies digitales\*. Cette gouvernance énigmatique et singulière doit être analysée. Les qualités de la gouvernance polycentrique des CM ne peuvent être interrogées qu'au travers de l'analyse empirique des usages des *coiners*\*. Et pour nous, s'intéresser à la gouvernance de crise des CM impose de regarder la crise dans son entier, c'est-à-dire de la mise en crise à la remise en ordre. Le troisième chapitre de la thèse est justement dédié à un tel travail d'enquête sur les crises. Il vise à approfondir les réflexions autour des statuts, rôles et droits de chacun des groupes de *coiners*\*, ainsi qu'autour des procédures et dispositifs de régulation et contrôle mis en place.

### CHAPITRE III - AU-DELÀ DES CODES : LA GOUVERNANCE DISCRÈTE DES CM, DÉVOILÉE PAR LEURS CRISES

« Il y a trois époques pour la monnaie : la monnaie basée sur les matières premières, la monnaie basée sur la politique et, aujourd'hui, la monnaie basée sur les mathématiques. »

Chris Dixon (Co-Founder of Hunch and SiteAdvisor)

« Donc voilà, "don't trust verify", ben oui, il ne faut pas truster, il faut vérifier. "Code is law", là par contre au fur et à mesure du temps, au début j'étais dans ce côté-là, en effet : ben si le code dit cela, il va se passer cela. J'étais encore dans ce côté-là pendant la "CVE2018 je ne sais plus quoi là"... je me suis dit, ben finalement si quelqu'un avait exploité cela, est-ce que il aurait fallu accepter ou pas les changements, je me suis dit bon... il a fait ça, ok... Pareil avec "The Dao", avec le temps,...] je me dis qu'il y a quand même un consensus social. "Code is law", as long as people don't mind" [Il rigole]. »

A. Le Calvez, Entretien n°20

En 2018, « le monde du Bitcoin a été surpris » d'apprendre qu'un bogue critique nommé « Bitcoin CVE 2018 #17144 », venait d'être corrigé en secret (Song 2018; Bitcoin CVE 2018 ci-après). La surprise qu'évoque Song (2018) tenait au fait que le réel mettait ainsi à l'épreuve les prétentions monétaires libérales technicistes des *coiners*\* qui font de Bitcoin une monnaie naturellement saine et incorruptible car « régulée par un algorithme au lieu d'être régulée par des bureaucraties gouvernementales » (Antonopoulos cité par Kanev 2022). Une telle nouvelle avait de quoi ébranler ceux convaincus d'avoir « placé leur [...] argent et [leur] confiance dans un cadre mathématique exempt de politique et d'erreur humaine » (Tyler Winklevoss, cité par Mullin 2013). Pourtant, force est de constater que l'antienne des *coiners*\* les plus radicaux se heurte à la réalité et que, de fait, les CM ont réussi à traverser « une litanie de problèmes de sécurité [qui] alimentent régulièrement les gros titres des journaux » (*Ibid*), ce qu'une simple requête en ligne associant les mots « Bitcoin » / « Ethereum » et « vulnérabilité » permet de vérifier en produisant de milliers de résultats<sup>320</sup>.

Notre étonnement à nous renvoie plutôt à l'invisibilité relative des crises, à la fois pour les *coiners*\* et pour la plupart des académiques. A se demander « que se passerait-il si des circonstances imprévues comme une faille dans le code, une cyberattaque ou une instabilité systémique apparaissaient ? », impossible de conclure que « la communauté bitcoin ne semble pas s'en préoccuper car elle a foi dans bitcoin » (Ponsot 2021, p. 2), alors même que la crise Bitcoin CVE 2018 s'inscrit dans l'histoire longue de celles déjà traversées par Bitcoin et que sa gravité potentielle avait de quoi faire parler. La faille décelée permettait ce que Bitcoin est censé empêcher : l'émission d'UCN\* en dehors des règles de monnayage canoniques via l'acceptation de transaction\* de double dépense par des nœuds\* du réseau\*. Pour certains, il s'agit du « bogue Bitcoin le plus catastrophique jamais advenu » (Awemany 2018) et « l'une

320

Voir  
<https://www.google.com/search?q=%C2%AB+Bitcoin+%C2%BB+et+%C2%AB+vulnerabilit%C3%A9+%C2%BB> et  
<https://www.google.com/search?q=%C2%AB+Ethereum+%C2%BB+et+%C2%AB+vulnerabilit%C3%A9+%C2%BB#ip=1> [consultation au 04/07/2022].

*des plus importantes failles de sécurité de [son] histoire* » qui aurait pu en changer le cours même (Qtum 2020). Et il s'avère que cette crise n'est ni la première, ni la dernière : de 2009 à 2020, nous en avons recensé 38 (cf. Chronologie 4 section III.1.2). Cependant, la grande majorité n'était pas d'une telle gravité, et la faille Bitcoin CVE 2018, restée inactive et latente, n'éprouvera pas le monnayage de Bitcoin. Mais ce monnayage ne fût pas toujours épargné : ainsi, la crise dénommée « *Bitcoin bug Value Overflow* » de 2010 fut accompagnée de l'émission surnuméraire de près de 184 Milliards d'UCN\* BTC, très loin du cap des 21 millions (Sedgwick 2019n). De même, peu de *bitcoiners\** savent que ce cap pourtant annoncé par Nakamoto était mal codé à l'origine et ne fût réellement implémenté qu'au détour d'une nouvelle crise, en 2014. En revanche, les *coiners\** savent par expérience que des controverses et conflits communautaires parfois houleux peuvent dégénérer en crise (cf. « *Scaling Debate* », Chap.I section I.3.3, Encadré 4 ; et la crise du hard Fork\* d'Ethereum consécutif à l'attaque de « *The DAO* », ce chapitre).

Au fur et à mesure de nos recherches nous avons fini par trouver, au sein des groupes de *coiners\** et chez les académiques, des personnes pour qui la survenue de crise n'avaient rien de surprenant.

Du côté des *coiners\**, l'histoire des crises touchant à leur CM est souvent mal connue. Mais cette méconnaissance traduit les enjeux de visibilité et d'invisibilisation au cœur de tout phénomène de crise, et la forme particulière qu'elle prend dans le champ des CM. Rapportée aux slogans *coiners\** « *Don't trust verify* », « *Be your own Bank* » ou « *trust no one* », cette méconnaissance des crises révèle qu'une partie d'entre eux se désintéresse des questions de sécurité et ce, en contradiction avec l'ethos annoncé revendiquant une souveraineté individuelle faite du refus de toute forme de confiance, de délégation et d'intermédiation. Les crises, loin de n'être que de simples accidents techniques renvoient à l'existence de risques réels ou perçus pour le protocole et ses participants, comme d'arrangements institutionnels et de stratégies développées pour s'y adapter. Elles mettent en lumière une division sociale du travail qui voit des membres formellement en charge d'administrer les codes et les crises qui y touchent : les « *Core développeurs\** » du protocole considéré. De leur côté, ni surprise, ni alarmisme. Comme cela a été mis en évidence pour l'accident nucléaire de Fukushima, le statut de « *catastrophe inimaginable* » est suspendu à un processus de normalisation, dont certaines personnes (ici les Core Devs) sont les acteurs quotidiens : ces dernières réintègrent ces « *accidents* » dans l'ordre d'une normalité organisée, dont les modalités relèvent d'une « *politique de la crise* » qu'il faut interroger (Aguilon, Cabane et Cornilleau 2019, p. 17). La surprise des *bitcoiners\** à l'annonce de la crise Bitcoin CVE 2018 se comprend à l'aune de cette politique de crise faite d'arrangements socio-technique négociés, liant normalisation et normalisateurs : si pour de nombreux *bitcoiners\**, il est « *difficile de croire qu'un bug aussi critique* [que le bogue CVE 2018] *puisse se produire* [et qu'il soit] *passé inaperçu... pendant presque deux ans* », c'est qu'ils s'attendent à ce que de nombreuses « *relectures du code* [soient] *faites* » et que, dans le même temps, ce code soit exécuté par des logiciels clients, sur des machines et par des acteurs diversifiés, tenant des fonctions identiques (*Bitcoin Q&A* 2018). La « bonne » CM, celle en laquelle on a confiance, apparaît de ce fait moins fondée dans ses caractéristiques techniques faillibles (et « *les mathématiques* », cf. C. Dixon en exergue), que dans la capacité de la communauté et ses membres à faire face aux crises, des caractéristiques sociales et infrastructurelles. L'un des principaux enseignements de la crise Bitcoin CVE 2018 est que « *même la plus scrutée des cryptomonnaie\* n'est pas exempte de bogue critique* » (Böhme et al. 2020, p.68). En conséquence, même la CM déclamée comme la plus *apolitique, neutre et immutable* des CM ne l'est pas, et suppose l'existence d'une gouvernance de crise.

Du côté des académiques, il existe quelques travaux qui, interrogeant la doxa qui prévaut d'une absence de gouvernance humaine des CM, en dévoilent *a contrario* l'« *invisible politique* » (De Filippi et Loveluck 2016). Citons par exemple (cf. Chap.II section I.3.3) Lustig et Nardi (2015, p. 1) qui, avec le concept d'« *autorité algorithmique* », démontrent que les *bitcoiners*\* reconnaissent la nécessité de la compléter par des jugements et médiations sociales, soulignant l'hétérogénéité des sphères axiologiques en présence, et donc potentiellement en conflit. Même type d'approche et de résultats pour DuPont (2018) qui s'intéresse à la communauté Ethereum durant la crise de « The DAO » (notre deuxième cas d'étude). Musiani, Mallard et Méadel (2018), quant à eux, étudient trois crises Bitcoin - l'une est protocolaire (le Bogues CVE-2013-3220, cf. crise n°19 Chronologie 4), les autres, infrastructurelles, concernent les affres de la bourse MtGox et de Silk Road (cf. Chap I). On doit à De Filippi et Loveluck (2016) d'avoir pointé que Bitcoin relevait d'une gouvernance duale, grâce à l'étude de la crise du « Scaling Debate » de Bitcoin : à la gouvernance *par l'infrastructure* (établissement par les règles protocolaires), se superpose une gouvernance *sur l'infrastructure*, socio-économique et politique qui régule les codes logiciels et les propriétés de la CM. La crise du Scaling Debate n'ayant pas trouvé de résolution à l'époque de leur analyse, ils concluaient face au *statu quo* apparent, que la gouvernance *sur l'infrastructure* de Bitcoin serait incapable de tenir son rôle, c'est -à-dire de permettre la « *formation de consensus entre des individus mis par des intérêts politiques et commerciaux parfois divergents* », du fait d'« *une structure de pouvoir hautement technocratique* » au sommet de laquelle les « *Core Devs* » jouiraient de pouvoir exorbitant (De Filippi et Loveluck 2016, p. 12-13; cf. Chap II section II.3.3). Nos premières réflexions sur la gouvernance de Bitcoin (Rolland et Slim, 2017) trouvent également leur origine dans la controverse du Scaling Debate et dans les travaux de De Filippi et Loveluck (2016). Bien que leur cadre d'analyse soit pertinent, nous estimons qu'il nécessite d'être actualisé et précisé, ne serait-ce que parce qu'à l'époque où ils écrivent le scaling debate n'a pas encore connu sa résolution finale (cf. Chapitre II).

Nous définissons les crises comme des « événements » fabriqués et gouvernés comme tels, par des diagnostics d'acteurs qui contribuent « à la « *mise en crise* » d'une situation donnée » à travers un travail de qualification et des dispositifs techniques (Aguiton, Cabane et Cornilleau 2019, p. 11-12 et p.15). Afin d'éviter de juger en surplomb les objectifs et moyens de la gouvernance des CM, nous devons nous efforcer d'être « *impartial relativement aux arguments avancés par les uns et les autres* » et de ne « *privilégier aucun point de vue* » (Callon 1986, p. 8). Cette exigence nécessite aussi d'analyser « *la politique de la crise* » et « *son gouvernement* » d'un bout à l'autre, de la mise en crise à la remise en ordre : il convient d'interroger les conditions de sa « *survenue* », de sa « *normalisation* », de son « *aggravation* », de sa « *contention* », jusqu'à sa « *résolution* ». Dénaturaliser le phénomène de crise implique d'abandonner la recherche des causes et de se défaire de la distinction entre l'état routinier du monde et le phénomène critique. Il importe dès lors d'interroger les catégories mêmes qui opposent la routine au dysfonctionnement, le bogue à l'attaque, et le normal à l'exceptionnel (*Ibid.*, p.4). L'enjeu d'une crise, c'est d'abord la fixation d'un normal opposé à un pathologique. Les crises démontrent que ce n'est pas n'importe quel code qui peut être considéré comme la loi, alors même que le slogan « *code is law* » prive de sens les concepts de failles, de vulnérabilités, de bogues voire d'attaques, puisque tout résultat d'un code est réputé normal, indiscutable et légitime. Les *coiners*\* du camp de la règle radicalisée qui mobilisent ce slogan s'empêchent de reconnaître un écart problématique entre le produit désiré d'un code (son « esprit ») et le résultat obtenu de sa « lettre ».

Ce troisième chapitre resserre le propos de la thèse autour de la fabrique et de la gouvernance des crises de CM. Son enjeu principal consiste à documenter et analyser la gouvernance polycentrique que nous avons identifiée et présentée comme la caractéristique les

singularisant comme monnaie (cf. chap. II) à travers deux cas de crises différentes de CM – la crise Bitcoin CVE 2018 et la crise du *Hard Fork*\* d’Ethereum suite à l’attaque de « *The DAO* ». La crise Bitcoin CVE 2018 a été choisie pour le type de crise et de gouvernance qui s’y construit, d’apparence hautement centralisée et technocratique : relevant d’une vulnérabilité affectant le monnayage de Bitcoin corrigée « *dans les coulisses*, [sans que cela nécessite a priori que] *tout le monde* [soit] *d'accord avec la direction que prennent les choses* » [M. Corallo Entretien n°15], elle apparaît en contradiction avec l’idée d’une gouvernance polycentrique. La seconde crise, en revanche, émerge en dehors des codes du protocole d’Ethereum. Mais l’utilisation de ces codes comme moyens de remédiation – permettant d’annuler l’attaque du fonds d’investissement décentralisé « *The DAO* » et de restituer les fonds aux investisseurs volés – va conduire à une controverse communautaire intense. Nous avons choisi cette crise car elle partage avec le « *Scaling Debate* » le fait de revêtir les caractéristiques d’une controverse technologique à la Callon (2006, p. 5, cf. encadré n°4 Chap. II.3.3) et de conduire à un dénouement sous forme de schisme (ou *Fork*\*) du fait de la sécession d’une minorité en désaccord sur ce que doit être l’objet monétaire et donc, sur les modifications protocolaires désirables. Par ailleurs, cette crise de « *The DAO* » sur Ethereum a précédé le « *Scaling Debate* » de Bitcoin (qui ne fut donc pas pionnier) et a de fait établi un précédent. On peut la considérer comme fondatrice tant pour Ethereum que, plus largement, pour l’écosystème des CM, l’épisode du « *Scaling Debate* » en étant fortement imprégné.

L’analyse de ces crises permet de mieux saisir l’environnement matériel et idéal de la gouvernance des CM et de répondre à une série de questions les concernant : que recouvre une crise pour les *coiners*\*, en termes de diagnostic et de pathologies (réflétant les propriétés désirées ou non de la CM) ? Quels sont les nomenclatures, les catégories et critères de définition des crises de CM ? Qui sont les acteurs non humains défaillants ? Qui sont les acteurs humains, en charge d’établir diagnostics et parcours de soin ? Quels processus concourent à la mise en crise et à la remise en ordre ? Quels sont les dispositifs impliqués, à qui s’adressent-ils et à quoi servent-ils ? Comment se définit le consensus communautaire relativement aux modifications des codes protocolaires ? La gouvernance prend-elle une même forme relativement à une *crise liée à une vulnérabilité* et à une *crise liée à une volonté d’évolution* ? Comment ces crises révèlent-elles l’hétérogénéité et les conflits axiologiques présents dans les communautés de *coiners*\* ? Quelles institutions d’expression des accords ou désaccords structurent ces débats et conflits ? Quelles relations et dynamiques de gouvernance entre les différentes composantes des communautés de *coiners*\* se donnent à voir ?

Étudier des crises, c’est aussi l’occasion de réfuter l’ensemble des propositions du syllogisme « libéral-techniciste » des ambitions monétaires des *coiners*\* : très directement, en contestant précisément la proposition (iii) qui voudraient que les CM soient immunisées de la gouvernance humaine et de ses intérêts socio-politiques, et plus indirectement, en prouvant que la technique n’est pas autonome et neutre vis-à-vis du monde social (proposition [i]), que les CM ne sont pas des monnaies purement techniques (proposition [ii]) et qu’en faire de « meilleures » monnaies que les monnaies nationales, n’a que peu de sens (proposition [iv]) quand leur qualités attendues sont renégociées suivant l’existence de débats et de controverses endogènes à leur communauté de paiement.

Ce chapitre comporte trois sections. Les deux premières sont consacrées à l’analyse approfondie de Bitcoin et à notre cas de crise. Là encore, parce que Bitcoin est pionnier, les procédures, arrangements et dispositifs concourant à la fabrique et la gouvernance de ses crises servent de matériau génétique à ce qui est mis en place par les autres CM, comme Ethereum (d’où une présentation d’Ethereum qui fera l’économie des éléments déjà posés).

**La première section** (III.1), part d'une présentation périodisée de la crise Bitcoin CVE 2018, cernant à chaque étape les acteurs et arrangements impliqués. Cette crise sera ensuite replacée dans l'histoire des crises Bitcoin ce qui, en plus d'éclairer ses enjeux singuliers, offrira l'occasion de proposer un panorama de la diversité des crises que Bitcoin a déjà rencontrées.

**La deuxième section** (III.2) entend cartographier les acteurs qui participent de cette gouvernance - les logiciels clients et codes pris en défaut mais aussi les acteurs humains en charge de leur maintenance et de leur évolutions - ainsi que les dispositifs de régulation et de contrôle entourant ces activités critiques qui permettent à la communauté de se prémunir contre toute centralisation technocratique effective. De ce fait, nous distinguerons deux grands types de crise – les crises *vulnérabilité* et les crises *d'évolution* – ainsi qu'une gouvernance de crise des CM à deux faces : une face routinière, avec une gouvernance de *huis clos* où le consensus est tacite et local, comme dans le cas de la crise Bitcoin CVE 2018 et une face exceptionnelle, avec une gouvernance *publique*, où la production du consensus est large et manifeste, comme souvent conflictuelle.

Notre **troisième section** (III.3) vise à étudier spécifiquement cette face publique et conflictuelle de la gouvernance de CM à partir du cas de « The DAO ». C'est dans ces situations que s'éprouve de façon manifeste la réalité d'une gouvernance polycentrique où chaque frange de la communauté doit pouvoir décider du devenir de sa monnaie. Comme pour la crise Bitcoin CVE 2018, une présentation périodisée de la crise de « The DAO », permettra de réaliser une cartographie des acteurs et des dispositifs clefs à chaque étape des événements, d'expliciter ses enjeux conflictuels, tout en insistant sur les caractéristiques distinctives de cette forme de gouvernance publique en terme de production de consensus et de gestion des dissensus.

### III.1 CRISE BITCOIN CVE 2018 #17144 : D'UNE CRISE À DE NOMBREUSES AUTRES...

La crise ouverte par la faille « Bitcoin Core CVE 2018 #17144 » (Bitcoin CVE 2018, ci-après) est singulière. Tout d'abord, parce que la vulnérabilité touche aux sacro-saintes règles de monnayage de Bitcoin. Ensuite, parce que cette vulnérabilité ne sera pas « activée », ni par exploitation volontaire, ni par occurrence fortuite (Bitcoin Core 2018a ; Böhme et al. 2020). Enfin, parce que le processus de découverte et de divulgation a permis une résolution silencieuse et confidentielle, grâce à un travail « *off chain*\* » coordonné par une poignée d'acteurs de confiance. Cette faille Bitcoin CVE 2018 doit sa découverte, le 17 septembre 2018, à « Awemany », un développeur « extérieur » à Bitcoin (Awemany 2018 ; Bitcoin Core 2018a). Ce dernier travaille sur la CM « Bitcoin Cash » (ticker BCH), née d'un schisme communautaire et protocolaire retentissant (un *hard Fork*\* contentieux, cf. section III.3.3 ce chapitre) marquant le dénouement du « Scaling Debate » en 2017 (cf. Chap. II section II.3.3). Bitcoin Cash, en reprenant une partie du code source de Bitcoin lors de son *Fork*\*, hérite également de ses vulnérabilités potentielles, comme le démontre cette faille découverte sur l'implémentation « Bitcoin ABC », au développement de laquelle participe Awemany et qui affecte aussi Bitcoin. Sa découverte n'est révélée qu'à un groupe restreint de personne de confiance, dans le cadre

d'une procédure de « divulgation responsable »<sup>321</sup>: d'abord à des membres de son équipe, ensuite à ceux d'équipes travaillant sur des implémentations de CM exposées à la même vulnérabilité (Awemany 2018). Dans ce cadre, le même jour, l'équipe « *Bitcoin Core* » reçoit confidentiellement un rapport de vulnérabilité anonyme concernant une faille par *Deni de Service* (DoS, Bitcoin Core 2018). M. Corallo, qui analyse ce rapport, découvre qu'il est partiel. La faille rapportée induit deux itérations de bogue, suivant les versions du client logiciel concernées : à celle ouvrant à des d'attaques par DOS identifiées par Awemany s'en ajoute une plus grave, permettant ce que Bitcoin est censé empêcher, à savoir la création monétaire *ex nihilo* d'UCN\* en dehors du monnayage canonique, par acceptation de double dépense (Awemany 2018; Song 2018c).

Cette vulnérabilité et ses itérations différencieront sont complexes. Elles touchent aux processus de vérifications protocolaires entourant la double dépense. Leur introduction dans les codes est ancienne et ne s'est pas faite d'un seul coup : elle est le résultat de modifications et d'optimisations successives du code « *Bitcoin Core* » depuis son origine, et renseigne sur la dimension processuelle inhérente à la production et à la maintenance des codes logiciels Bitcoin. Il faut souligner le temps long pendant lequel la faille fut présente à l'état latent. Les versions vulnérables, toutes publiées en 2017, n'ont vu personne y prêter attention, de manière malicieuse<sup>322</sup> ou non (Bitcoin Core 2018a ; Song 2018) et il faut plus d'un an et demi à la communauté pour repérer et réparer le bogue. Oui, « *même la plus scrutée des cryptomonnaies\* n'est pas exempte de bogue critique* » (Böhme et al. 2020, p.68). Catastrophique pour les uns (Awemany 2018 ; Qtum 2020) et à relativiser pour d'autres (Song, 2018), cette crise et sa gravité questionnent. Que « *ce bogue ait été introduit puis autorisé à exister de la 0.14.0 à la 0.16.2 a indéniablement été un échec majeur [et] si toutes les pratiques de Bitcoin Core restent les mêmes [...] nous pourrions ne pas avoir autant de chance [puisque] un échec similaire* » se reproduira nécessairement (theymos 2018). L'auteur reconnu de cette alarme enjoint justement à documenter ces « pratiques » entourant l'évolution des codes et les acteurs, ainsi que les procédures et dispositifs en place qui les encadrent.

Ces pratiques et l'ensemble de ce qui s'y rapporte, nous proposons de les faire ressortir à travers la périodisation des évènements entourant la crise CVE Bitcoin 2018.

### III.1.1 Présentation périodisée de la crise Bitcoin CVE 2018

Comme nous le verrons, la faille étiquetée CVE 2018 #17144 n'est, pour Bitcoin et sa communauté, ni la première, ni sans doute la dernière (Cvllr 2018 ; Sedgwick 2019n ; Sedgwick 2020 ; Dashjr 2019)... ni même peut-être la plus intéressante en termes de sociologie des controverses technologiques au sens de Callon (2006, cf. section X). Mais pour s'en rendre

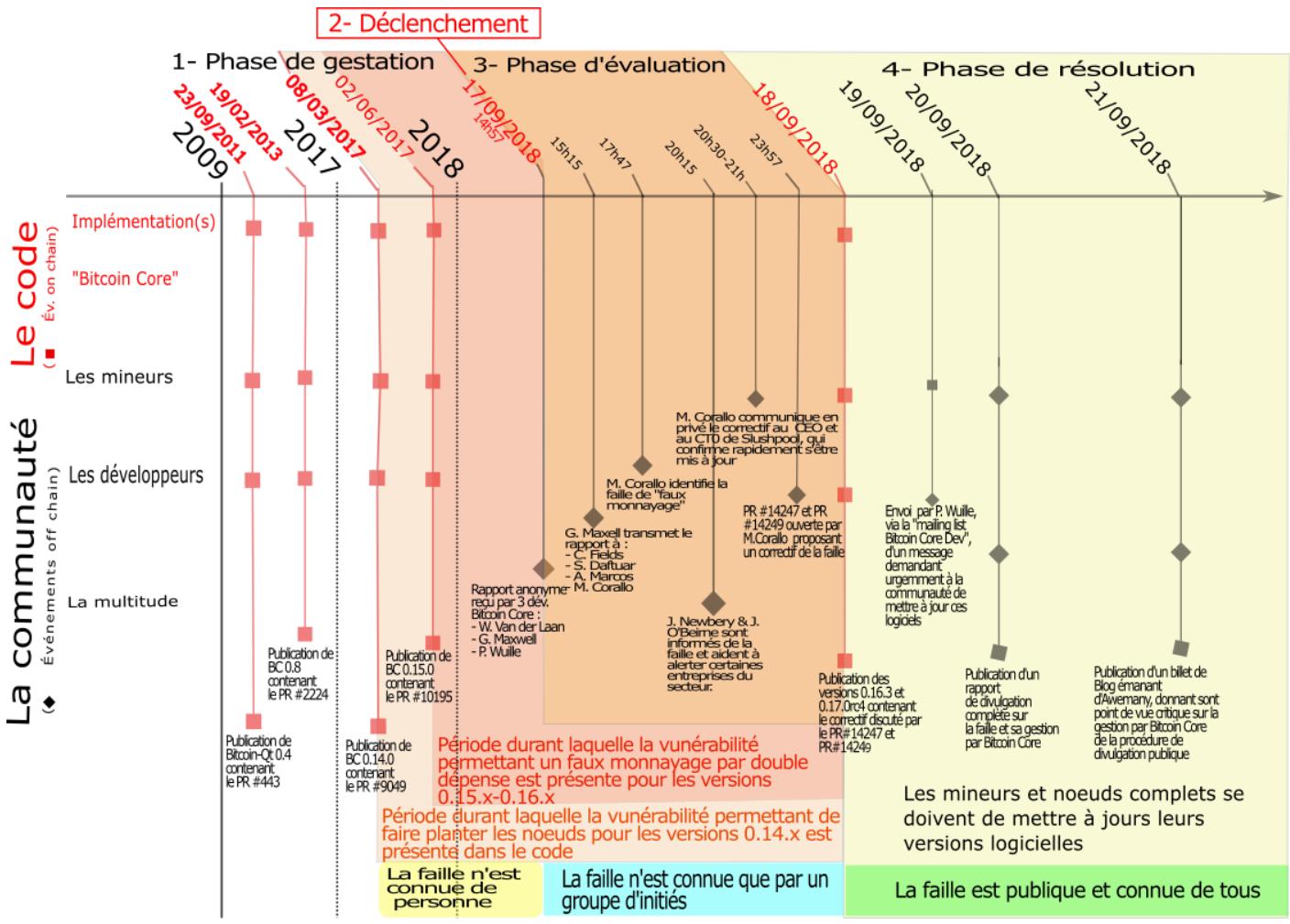
---

<sup>321</sup> Une procédure de « divulgation responsable » renvoie, dans le champ de la sécurité informatique, à un ensemble de conventions et de normes encadrant les pratiques de divulgation d'une vulnérabilité informatique : de sa découverte à sa divulgation publique, en passant par sa résolution. Ces procédures visent à préciser comment doivent être protégés les utilisateurs, qui doit être contacté, suivant quelle modalité et temporalité, et enfin, comment doit être récompensé le découvreur qui s'y est engagé. Ce type de procédure, normé au sein de l'industrie logicielle, reste largement informel, flou et problématique pour les CM et crypto-actifs\* (Böhme et al. 2020).

<sup>322</sup> Lors de la divulgation complète du 21 septembre 2018, l'équipe « *Bitcoin Core* » reconnaît, sans plus de certitude, n'avoir « *pas connaissance de tentatives d'exploitation de cette vulnérabilité* » (Bitcoin Core 2018a) et il s'avère qu'*« une analyse rétrospective a prouvé qu'il n'a jamais été exploité ! »* (Straw Hat 2019).

compte, il importe d'abord de présenter cette crise et son contexte, à travers la réalisation d'une périodisation. Analyser un événement oblige à le borner temporellement, ce qui n'est jamais chose aisée – le réel étant continu et non discret. Le travail de périodisation est en soi un acte nominaliste, toujours relatif aux vues de son auteur, et notre périodisation ne fait pas exception. Puisque le « *statut de la crise est délicat à saisir et sa temporalité difficile à fixer* », nous adoptons « *une définition a priori [qui part du] diagnostic porté par* » des acteurs contribuant « *à la "mise en crise" d'une situation donnée [par un] travail de qualification* » suivant différentes opérations et dispositifs techniques (Aguiton, Cabane et Cornilleau 2019, p. 15). Cela nous permet de découper les événements en deux périodes et quatre phases (cf. Chronologie 3 suivante). Précisons que, pour la crise Bitcoin CVE 2018, ce bornage fut facilité par ces caractéristiques. La période de la mise en crise d'abord, constituée d'une phase d'insémination et de gestation au cours de laquelle la vulnérabilité est introduite dans le code, sans qu'elle ne soit ni activée, ni connue. Ensuite, une phase de déclenchement de crise, qui voit le statut de ce code changer, la faille passant de latente à manifeste. Pratiquement, cette mise en crise, conçue comme apparition consciente de l'existence d'une vulnérabilité, correspond à la première borne posée. Elle renvoie explicitement à la date de mise en œuvre de la procédure de divulgation responsable. C'est la fixation de cette borne qui permet, à rebours, de retracer les événements ayant pris part à l'émergence de la vulnérabilité, à sa découverte, à son évaluation et, enfin, à la production et à la publication du correctif. Nous faisons en amont débuter la phase de gestation en janvier 2009, car la faille, nous le verrons, s'articule aux premières règles protocolaires permettant de réguler les transactions\* et le phénomène de *double dépense*\*. Le déclenchement, sous forme d'un rapport de divulgation anonyme et confidentiel, ouvre une période de remise en ordre décomposée, elle, en une phase d'évaluation (permettant aux acteurs informés d'évaluer la gravité du bogue et de discuter des voies de remédiation) et une phase de résolution au cours de laquelle une solution corrective est acceptée, implémentée dans une nouvelle version logicielle et publicisée (laissant aux acteurs du réseau\* le choix de l'accepter en mettant ou non à jour leur machine). Là encore, la phase de résolution se trouvait bornée par la date de publication des versions correctives. La frise chronologique suivante saisit, pour chacune de ces phases, les principaux événements et acteurs.

## Chronologie 3 : Périodisation des événements entourant la crise ouverte par le bogue CVE 2018



Source : Rolland Maël

### Une mise en crise longue et silencieuse

Retraçons l'origine de la faille en réalisant une généalogie partielle des codes sources Bitcoin.

*Insémination/gestation : une « étrange confluence d'événements » potentiellement catastrophiques*

La faille Bitcoin CVE 2018 est le résultat de modifications et d'optimisations successives du code source de l'implémentation « Bitcoin Core » depuis son origine. La comprendre impose de retracer les évolutions par sédimentation lente d'optimisations successives du code logiciel originel. L'ensemble de ces modifications – au nombre de 6 (cf. Figure 10 suivante) – prit la forme de « *Pull Requests* » (PR) acceptées et fusionnées, donnant lieu à la publication des versions vulnérables (le traitement de ces termes et des dispositifs auxquels ils renvoient est renvoyé à une section prochaine). Pour comprendre l'*« étrange confluence d'événements »* (Song 2018) qui conduira à l'introduction d'une faille d'une telle ampleur dans les codes protocolaires Bitcoin, il faut expliciter les objectifs et justifications qui ont présidé à ces PR et à leurs implémentations.

Le point de départ n'est autre que la première version du logiciel Bitcoin-QT (version 0.1, Nakamoto 2009c<sup>323</sup>), publiée par S. Nakamoto en février 2009 (Song 2018) et qui ne permet pas de se protéger de tous les cas de *double dépense* possibles. Dans le cadre normal de Bitcoin, il est par définition possible de produire et diffuser une transaction\* contenant une double dépense. C'est la faire accepter par les nœuds\* qui est logiquement impossible. Au sein de Bitcoin, les transactions\* valides sont définies négativement : les transactions\* produites et diffusées se voient appliquer des critères d'invalidité afin d'évaluer qu'elles sont « pathologiques » et, de ce fait, doivent être rejetées (un avertissement est même diffusé, cf. Chap. I, section I.1.3.). Mais l'encadrement pratique de la double dépense est complexe. Produire et diffuser une transaction\* Bitcoin renvoie à quatre situations possibles, dessinant quatre cas « *pathologiques* » de double dépense (les cas A, B, C, D ; voir Tableau 2 suivant, Song, 2018).

**Tableau 2 : Les quatre types de double dépense\* idéal-typiques sur Bitcoin**

|                         |                       | Origine des transactions*   |   |
|-------------------------|-----------------------|---|---|
|                         |                       | Transaction* publique de portefeuille   | Transaction* privée d'enregistrement  |
| Nombre de transactions* | Transaction* Multiple | (A)<br>Plusieurs transactions* au sein desquelles la/les même(s) UTXO* est/sont dépensée(s).              | (B)<br>Plusieurs blocs au sein desquels plusieurs transactions* dépensent la/les même(s) UTXO*. |
|                         | Transaction* Unique   | (C)<br>Une même transaction* au sein de laquelle la/les même(s) UTXO* est/sont dépensée(s) plusieurs fois | (D)<br>Un seul bloc au sein duquel la/les même(s) UTXO* est/sont dépensée(s) plusieurs fois     |

Source : Rolland Maël

Deux types de transactions\* de double dépense peuvent être produits. Tous d'abord, on peut créer plusieurs transactions\* différentes dépensant la même UTXO\*, c'est le plus connu (cas A). Il est aussi possible de créer une seule transaction\* dépensant en entrée plusieurs fois la même UTXO\* (cas B). Une fois produite, la transaction\* doit être proposée à l'intégration au registre. Bitcoin dispose de deux procédures de publication : soit avec des *transactions publiques issues de portefeuilles*\* (« *mempool transaction*\* », cas C), soit il s'agit d'une *transaction privée intégrée directement dans un bloc* (« *block transaction*\* », cas D, Song 2018). Les premières servent souvent à illustrer le fonctionnement de Bitcoin (comme nous l'avons fait dans le Chapitre I) : partant du client portefeuille des usagers. Ces transactions\* sont publiques de bout en bout, de leur consignation comme transaction\* en attente dans les journaux locaux des « mineurs » (la « *mempool*\* »), jusqu'à leur traitement et leur intégration dans un enregistrement candidat\*. Le second cas (les *transactions privées issues d'enregistrement*) est plus rarement explicité. Ce type de transaction\* ne peut être produit que

<sup>323</sup> Les codes sources sont accessible ici : <http://btc.yt/lxr/satoshi/source/src/main.cpp?v=0.10.0> [consultation au 12/09/2021].

par les opérateurs du traitement des transactions\*, ce qui souligne leur différence structurelle d'avec les autres acteurs. En effet, l'attention donnée aux « *transactions\* publiques, issues de portefeuille* » occulte le fait qu'une transaction\* Bitcoin n'a pas à être diffusée publiquement *via* la « *mempool* » pour être traitée et intégrée dans un « *bloc* » : tout producteur d'enregistrement peut créer un service de diffusion privée « *off chain* »\* afin d'intégrer les transactions\* de ses clients souhaitant éviter la *mempool* : ces transactions\*, n'étant publiques qu'une fois validées au sein d'un enregistrement candidat\*, sont protégées des abus de type MEV (cf. Chap. I., section I.3.3). Bitcoin permet de réguler ces quatre cas suivant des règles strictes, renvoyant à des procédures de vérifications de non-conformité (des « *checks* ») encadrant chacun d'eux (Song 2018). Les doubles de dépenses de type A suivent la règle stipulant que la première transaction\* intégrée dans un enregistrement canonique\* invalide toute transaction\* impliquant le/les UTXO\* déjà dépensée(s). Idem pour les types B : le premier enregistrement candidat\* à devenir canonique invalide tout enregistrement impliquant des transactions\* avec la/les même(s) UTXO\* déjà dépensée(s) qu'il contient. Les types C renvoient à un check établissant qu'une transaction\* contenant plusieurs fois les mêmes UTXO\* devra être considérée comme invalide. Le cas D, enfin, considère qu'un enregistrement candidat\* contenant plusieurs fois la/les même(s) UTXO\* sera considéré invalide, l'horodatage\* faisant foi. Le caractère multiforme pris par la vulnérabilité Bitcoin CVE 2018 repose, nous le verrons, sur le traitement différencié des régulations du cas D, suivant les versions logicielles concernées (d'où la cellule grisée, Tableau 2, Bitcoin Core 2018 ; Song 2018).

Dans le logiciel originel de Nakamoto, la régulation des types de double dépense\* n'est que partielle, poussant à des évolutions successives de son code (cf. Figure 9 suivante). En juillet 2011, expliquant que toute double dépense, qu'importe son origine, doit être invalide, le « Core Développeur » (« Core Dev » par la suite) M. Corallo propose la PR 443<sup>324</sup>. L'objectif est d'encadrer les cas de doubles dépenses issues de transaction\* publique de portefeuille (le cas C), en introduisant une nouvelle vérification<sup>325</sup> empêchant que ce type de transaction\* « *soi[t] relay[é]* » (*Ibid.*). Avec cette PR - acceptée de tous les participants et implantée dans la version Bitcoin Core 0.4 -, chacun des cas de double dépense possibles (A, B, C et D) est maintenant régulé, mais au prix d'une redondance pour les cas B et D, vérifiés deux fois<sup>326</sup> (*Ibid.*). En janvier 2013, P. Wuille (aka « *Sipa* »), un autre « Core Dev », propose *via* la PR 2224 de transformer la vérification inutile en une vérification de corruption de système afin d'améliorer « *la façon dont les erreurs lors de la validation\* des blocs et des transactions\* sont propagées, affichées et traitées* » (P. Wuille<sup>327</sup>). La modification introduit que, en cas d'échec, le logiciel renvoie un « arrêt de programme » ("Assert") et non une simple erreur (Song, 2018). Cette PR 2224 donne lieu à la version Bitcoin Core 0.8.0. Les modifications présentées n'induisent encore aucune vulnérabilité. Ce sont celles qui suivront qui scelleront la crise en devenir.

---

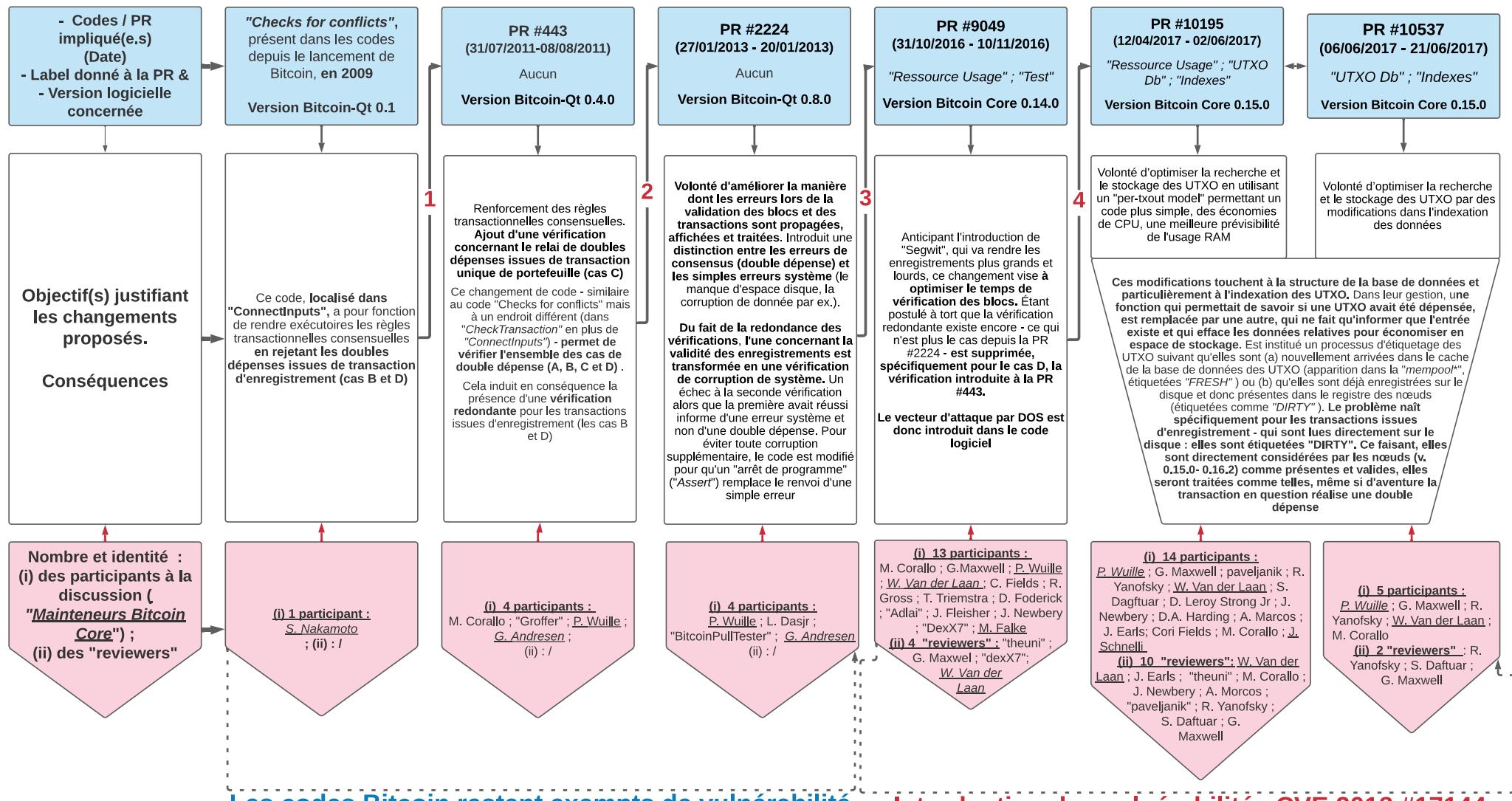
<sup>324</sup> Voir <https://github.com/bitcoin/bitcoin/pull/443> [consultation au 12/09/2021].

<sup>325</sup> Similaire à la fonction « *Check for conflicts* »/« *vSpent* », mais localisée ailleurs, dans « *CheckTransaction* » (Song, 2018).

<sup>326</sup> Suivant deux processus, une fois *via* « *CheckTransaction* » et une autre *via* « *ConnectInputs* » (Song 2018).

<sup>327</sup> Voir <https://github.com/bitcoin/bitcoin/pull/2224> et <https://github.com/bitcoin/bitcoin/pull/2224/files> [consultation au 12/09/2021].

**Figure 9 : D'une sédimentation de modifications des codes Bitcoin de 2011 à 2017 créant la faille**



Source : Rolland Maël

En octobre 2016, M. Corallo propose la PR 9049<sup>328</sup> qui vise à accélérer le temps de vérification pour des enregistrements voués à être plus lourds (en taille mémoire), après la mise à jour « SegWit » annoncée (cf. « Scaling Debate », Chap. II section II.3.3). Corallo postulant à tort que la vérification redondante précédente existe encore (ce qui n'est plus le cas depuis la PR 2224), il propose sa suppression, afin « *d'éviter une vérification coûteuse lors de la validation\* initiale du bloc pré-relais que les entrées multiples au sein d'une même transaction\* ne dépensent pas deux fois la même entrée, ce qui avait été ajouté en 2012 (PR #443)* » (Bitcoin Core 2018a). Dans la mesure où l'évaluation des PR erronées de Corallo est partagée entre les participants<sup>329</sup> et que « *les résultats du benchmark indiquent [une économie d']environ 0,5-0,7 ms* » (M. Corallo<sup>330</sup>), l'optimisation est acceptée et fusionnée au répertoire logiciel principal. La première itération du bogue CVE 2018 dans les versions Bitcoin Core 0.14.0 est introduite ainsi. Désormais, sans qu'aucun acteur n'y prête attention, les nœuds\* fonctionnant sur cette version sont devenus vulnérables (cf. Tableau 3 suivant pour une estimation) et toute « *tentative de dépenser deux fois la sortie d'une transaction\* au sein d'une transaction\* unique dans un bloc entraînera [...] un plantage* » (Bitcoin Core 2018). L'introduction de l'itération de « faux monnayage » par double dépense renvoie, elle, à l'articulation de deux PR distinctes : les PR n° 10195 et n° 10537, discutées entre avril et juin 2017<sup>331</sup>. La PR n° 10195, émanant de P. Wuille, sera discutée par 14 participants, dont 10 sont formellement relecteurs<sup>332</sup>. Elle vise à optimiser la recherche et le stockage des UTXO\* via un code plus simple (substitution de la base de données et du cache à un modèle « per-txout ») permettant des économies de CPU et une meilleure prévisibilité de l'usage de la mémoire RAM (P. Wuille<sup>333</sup>). La PR n° 10537 émane

<sup>328</sup> Voir <https://github.com/bitcoin/bitcoin/pull/9049> [consultation au 12/09/2021]. M. Corallo justifie cette PR comme suit : « *Bitcoin Core est très optimisé [...] quand votre nœud\* reçoit un bloc, il fait autant de vérifications que nécessaire et ensuite il transmet le bloc. [C'est] une partie clef de la résistance contre [certaines] attaques [...] pour la rentabilité du minage et pour avoir [...] une distribution équitable de la rentabilité du minage. [...] dans le contexte de la validation\* complète des blocs, il ne s'agit pas d'une optimisation majeure [...]. Mais entre le moment où Bitcoin Core reçoit un bloc et le relâche à ses pairs, il ne fait qu'une sorte de vérification initiale [...] de la preuve de travail. Il s'agit de s'assurer que la copie du bloc est en quelque sorte une bonne copie [...] non modifiée, donc il s'assure qu'il est comme le bloc canonique et qu'il a la preuve du travail [...]. C'est suffisant pour se rendre compte qu'il n'y a aucune raison de dire que j'ai besoin de valider complètement le bloc avant de le relayer parce qu'on sait avoir déjà vérifié [...]. C'est fondamentalement une vérification redondante et c'est quelque chose qui ralentit matériellement la propagation des blocs et donc il faut s'en débarrasser. [...] Cette bonne idée s'est avérée comporter plus de risques que nous l'avions prévu et les vérifications réelles, plus lointaines dans le code, se sont avérées ne pas protéger contre cela et n'ont tout simplement pas été prises en compte à l'époque.* » [Entretien n°15]

<sup>329</sup> Pour les acteurs, les PR impliquées sont floues : « *les développeurs\*, lorsqu'ils ont discuté du PR 9049, étaient prédisposés à penser qu'une double dépense simple-tx au niveau du bloc [...] était vérifiée ailleurs à partir du PR 443 sans tenir compte du PR 2224 [et ils n'ont] pas examiné aussi attentivement le PR 9049* » (Song 2018). Les échanges IRC « Bitcoin Core Dev » révèlent l'impact du temps long : « <Sipa> : Avons-nous même besoin de cette vérification ? <Bluematt> : Celui des entrées dupliquées ? Pas clair, probablement pas mais nous l'avons ajouté pour une raison. <BlueMatt> : Je ne me souviens pas de ce que c'était... <BlueMatt> : Je me souviens cependant que nous avions une raison. « <BlueMatt> : Oui, et je me rappelle avoir eu une raison [...] <BlueMatt> : Je veux dire que c'était il y a longtemps » (Song 2018).

<sup>330</sup> Voir le fil de discussion Github suivant <https://github.com/bitcoin/bitcoin/pull/9049> [consultation au 12/09/2021].

<sup>331</sup> Voir <https://github.com/bitcoin/bitcoin/pull/10195> et <https://github.com/bitcoin/bitcoin/pull/10537> [consultation au 13/09/2021].

<sup>332</sup> Les discutants sont : P. Wuille, il est à l'origine de la proposition et de la fusion de cette PR dans le répertoire principal ; G. Maxwell ; paveljanik ; R. Yanofsky ; W. Van der Laan ; S. Dagftuar ; D. Leroy Strong Jr ; J. Newbery ; D.A. Harding ; A. Marcos ; J. Earls ; Cori Fields ; M. Corallo ; J. Schnelli. Les relecteurs formellement reconnus sont : W. Van der Laan ; J. Earls ; "theuni" ; M. Corallo ; J. Newbery ; A. Marcos ; "paveljanik" ; R. Yanofsky ; S. Daftuar ; G. Maxwell ; voir <https://github.com/bitcoin/bitcoin/pull/10537> [consultation au 14/09/2021].

<sup>333</sup> Commentaire introductif du 12 avril 2017, <https://github.com/bitcoin/bitcoin/pull/10195> [consultation au 16/09/2021].

de M. Corallo. Elle sera discutée par 5 participants, dont 2 sont formellement relecteurs<sup>334</sup>. Il s'agit encore d'optimiser la recherche et le stockage des UTXO\* (*via* l'indexation des UTXO\* et la sémantique d'assertion « per-UTXO\* ») et, par-là, le traitement des données par les nœuds\*. Complémentaires, ces deux PR participent d'*« une refonte plus large visant à simplifier le suivi des sorties de transaction\* non dépensées et à corriger une attaque par épuisement des ressources »* (Bitcoin Core 2018) : pour économiser de l'espace de stockage, une fonction renseignant si une UTXO\* a été dépensée est remplacée par une se limitant à dire si l'entrée existe<sup>335</sup>. Ces deux PR rendaient « *le code autour du stockage UTXO\** » - une « *partie clé du code de consensus* » - « *beaucoup plus simple* » [et était] *aussi un peu plus efficace à [d'autres] égards* » [M. Corallo, Entretien n°15]. Elles sont ainsi acceptées et fusionnées dans les codes Bitcoin Core par P. Wuille, sans controverse. Mais, ce qui est « *beaucoup plus simple, [ne] signifie pas que c'est plus facile à auditer et beaucoup plus net* » [M. Corallo, Entretien n°15]. À l'insu de tous, l'itération de la faille de « faux monnayage » est introduite dans Bitcoin au sein des versions 0.15.0 (publiée le 14 septembre 2017) à 0.16.2 (publiée le 29 juillet 2018)<sup>336</sup>. Les nœuds\* concernés par les versions vulnérables traiteront toute transaction\* issue d'enregistrements passés comme valides : directement lue sur le disque, où toute transaction\* existante l'est par définition, un cas de double dépense sera valide, permettant « *à un mineur de gonfler l'offre de bitcoins [en] revendiqu[ant] la valeur dépensée deux fois* » (Bitcoin Core 2018).

Au temps long de cette phase d'insémination/gestation va répondre un déclenchement et une période de remise en ordre courte.

#### *D'un déclenchement confidentiel par « divulgation responsable »*

Le déclenchement renvoie au moment où des codes se voient reconnaître le statut de vulnérables par un ou plusieurs acteur(s). Ici, cette reconnaissance fut privée, secrète et silencieuse, comme le révèlent les conditions d'accès asymétrique aux informations concernant la faille (représentées dans la Figure 10 suivante). Ces conditions nous permettent de distinguer, d'un côté, un groupe d'initiés, numériquement réduit et bénéficiant d'un accès privilégié à des informations et, d'un autre, un ensemble large d'acteurs regroupant le commun des utilisateurs, qui dépend du premier groupe pour ce qui est de son accès à l'information et à la connaissance. J. Song [Entretien n°14] confirme cette distinction très naturellement quand nous en venons à expliciter les conditions par lesquelles il eut connaissance des évènements : « *j'en ai entendu parler de la même manière que n'importe qui d'autre, j'ai vu la divulgation faite par les développeurs\* de Bitcoin Core* ». Partant de la découverte de la faille, intéressons-nous à ce groupe d'initiés par qui l'entrée en crise se fait.

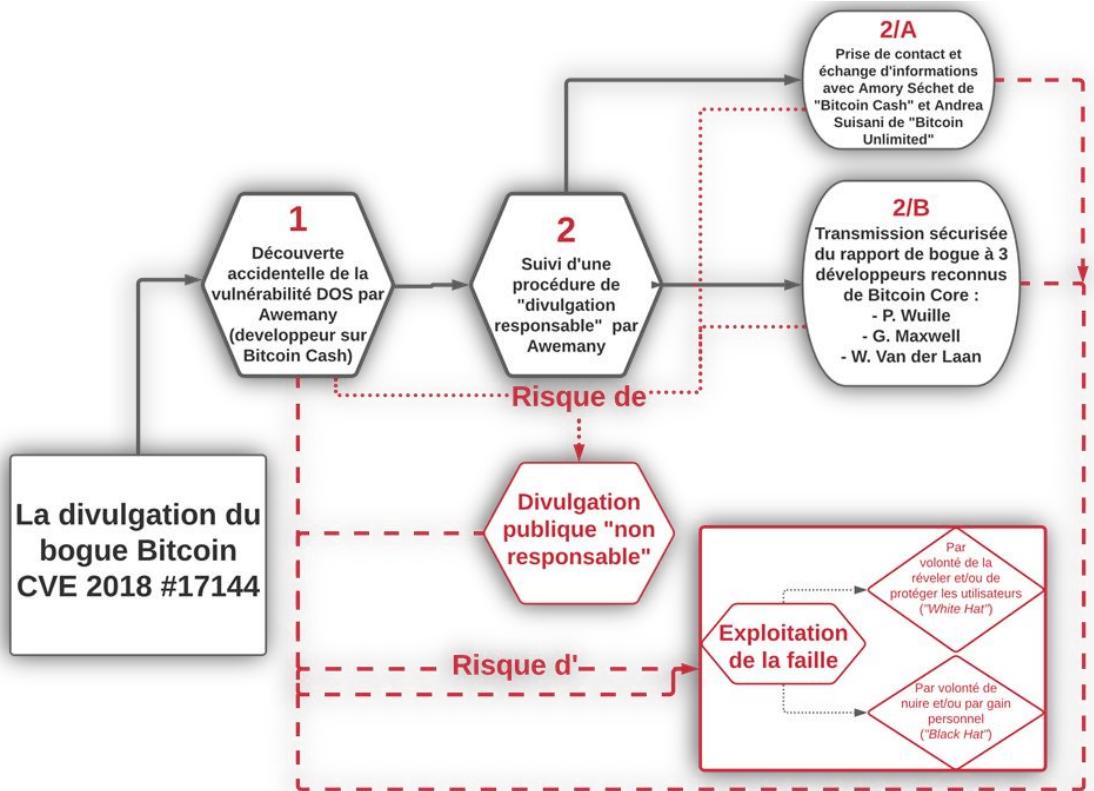
---

<sup>334</sup> Les discutants sont : P. Wuille, qui, en plus d'être à l'origine de la proposition, va être celui qui, disposant des droits d'administrateur\* sur le répertoire, fusionnera cette PR dans le répertoire principal ; G. Maxwell ; R. Yanofsky ; W. Van der Laan ; M. Corallo. Les relecteurs formellement reconnus sont : R. Yanofsky ; S. Daftuar ; G. Maxwell ; voir <https://github.com/bitcoin/bitcoin/pull/10195> [consultation au 16/09/2021].

<sup>335</sup> Par institution d'un processus d'étiquetage des UTXO les qualifiant de « *FRESH* », si elles sont nouvelles dans la mempool\*), ou de « *DIRTY* », si elles sont déjà présentes dans le registre\* des nœuds\*, ce qui permet de supprimer les données de transaction des secondes, dont la seule preuve de l'existence passée suppose leur validité (Anonyme 2018).

<sup>336</sup> Pour les versions précédentes, « *toute tentative de dépenser deux fois une sortie de transaction au sein d'une transaction unique dans un bloc où la sortie dépensée a été créée dans le même bloc, le même échec d'assertion se produira (comme cela existe dans le cas de test qui a été inclus dans le patch 0.16.3)* ». (Bitcoin Core 2018a)

**Figure 10 : La divulgation du Bogue CVE 2018, ses étapes, ses risques et ses acteurs**



Source : Rolland Maël

1– Le 17 septembre 2018, Awemany « *dans [s]a petite camionnette au bord de la mer, [...] travaillait à l'implémentation des nouveaux opcodes CHECKDATASIG/-VERIFY [...] pour Bitcoin (Cash)* [quand il a] remarqué que la validation\* de bloc saut[ait] [l]e test » vérifiant les entrées dupliquées lors d'une transmission de bloc<sup>337</sup> (Awemany 2018). C'est un vecteur d'attaque par DOS potentiellement grave<sup>338</sup>. Cette découverte implique des risques pour les CM concernées (en rouge). Le découvreur peut tout d'abord tenter d'exploiter la faille en secret : si le profit escompté est personnel, l'exploitation est considérée comme maligne, relevant de chapeau noir (ou « Black Hat ») ; dans le cas inverse, la qualification de chapeau blanc (ou « White Hat ») est retenue (comme dans la crise d'Ethereum, cf. section III.3.2). Ensuite, hors malice, la divulgation peut être qualifiée de « non responsable » si le découvreur diffuse largement les informations concernant la vulnérabilité, permettant que des acteurs mal intentionnés s'engagent dans son exploitation. Awemany ne choisit aucune des voies précédentes. En tant que « *citoyen responsable dans cet écosystème* » (*Ibid.*), il s'engage dans une « *divulgation responsable* » : il limite l'accès à cette information cruciale à un petit nombre d'acteurs reconnus, et réduit d'autant les risques que ferait courir sa diffusion au plus grand nombre. Au moment de sa découverte, il contacte d'abord ses collègues de l'équipe de

<sup>337</sup> Vérification « CheckRegularTransaction » pour Bitcoin ABC, « CheckTransaction » pour « Bitcoin Core » (Awemany 2018).

<sup>338</sup> Il décrit s'être dit : « "Oh putain, ça n'a pas l'air bon, je dois prévenir deadalnix et l'équipe de ce qui se cache dans ABC, ça n'a pas l'air bon du tout. \$@#% !!". Conscient du danger que cela pourrait peut-être être exploité plus avant vers un véritable bug d'inflation et de séparation de chaîne (mais je n'ai pas vérifié plus [...] car un bug de plantage de nœud\* avec échec de assert était déjà suffisant » (Awemany 2018).

développement Bitcoin ABC. C'est une fois l'alarme donnée « chez lui » qu'il s'engage dans une procédure de « divulgation responsable » à l'adresse d'équipes de développement extérieures, travaillant sur des implémentations de CM potentiellement exposées (*Ibid.*) : l'équipe de développement des implémentations « *Bitcoin Unlimited* » (client Bitcoin et Bitcoin Cash) et celle de « *Bitcoin Core* » (client référent pour Bitcoin).

2 – En s'engageant dans un processus de divulgation responsable, Awemany souhaite « *jouer franc jeu* » (Awemany 2018), ce qui n'a rien d'aisé dans le champ des CM (Fields 2018 ; Awemany 2018 ; Böhme et al. 2020). Son rapport sur la faille DOS rédigé, encore devait-il être en mesure de l'adresser aux bons acteurs (les « responsables » dans la communauté considérée) et ce, de manière confidentielle et sécurisée. Cette possibilité repose sur l'existence d'une liste de personnes contacts en charge de la sécurité, c'est-à-dire un groupe d'acteurs formellement reconnus comme étant en charge du développement et de la maintenance des implémentations logicielles. En plus d'identifier les contacts, il faut aussi utiliser les voies de communication sécurisées ouvertes (assurant la confidentialité, l'authenticité des informations transmises et des intervenants). Conventionnellement, c'est une page de contact sur le site web de l'implémentation logicielle considérée qui explicite les processus de divulgation de vulnérabilité établis. Dans tous les cas, il est attendu « *que les développeurs\* fournissent des clés publiques avec leur contact de sécurité*<sup>339</sup> et *qu'ils disposent de processus internes pour traiter les messages entrants* » : ce qui, dans le champ des CM, est loin d'être le cas, même pour des CM d'envergure (Fields 2018, repris par Böhme et al. 2020, p. 68). Fields (2018), lors d'une divulgation d'un bogue précédemment découvert sur l'implémentation Bitcoin ABC, disait s'être « *heurté à un mur* », car « *aucune clé n'était répertoriée [...] sur les serveurs de clés PGP publics où on les trouve habituellement, [ni] dans leur dépôt de code* ». Même problème pour Awemany, la liste de contacts trouvée est obsolète : il rejoint « *Cory Fields de Core* » sur la difficulté « *de trouver les adresses et les informations de divulgation nécessaires* » (*Ibid.*), et précise que le « *manque de clés PGP facilement accessibles* » pour Bitcoin ABC est aussi vrai pour Bitcoin Core, n'ayant « *pas trouvé à temps une clé non rétractée*<sup>340</sup> de Pieter Wuille » (Awemany 2018). Du fait de sa position de développeur\* sur Bitcoin ABC, Awemany n'a rencontré aucune difficulté à contacter les membres des équipes de « *Bitcoin Cash* »<sup>341</sup> et de « *Bitcoin Unlimited* »<sup>342</sup> (2/A, cf. figure précédente). Le contact avec les membres de l'équipe « *Bitcoin Core* » a été plus compliqué (2/B, cf. figure précédente). Le site Internet dispense des informations précises sur les procédures relatives à la divulgation de vulnérabilité. Deux processus sont distingués : si la faille ne touche pas à la sécurité du logiciel, un simple processus de suivi des problèmes publics (ou "Public Issue Tracking") est suffisant ; dans le cas inverse, une divulgation responsable s'impose et il est demandé de se reporter aux mails et clef de chiffrement donnés par la liste de contacts<sup>343</sup>, si tant est qu'elle soit à jour. Le rapport de divulgation sera finalement transmis le même jour, via « *message PGP crypté* » à l'adresse d'un « *ensemble de personnes de confiance* » (Awemany 2018 ; confirmé par Bitcoin Core 2018) : P. Wuille, G. Maxwell & W. Van der Laan, trois développeurs\*

---

<sup>339</sup> L'accès aux adresses mails et aux clefs publiques de chiffrement PGP garantit l'identité des acteurs, l'intégrité des informations échangées et leur confidentialité.

<sup>340</sup> Lors de la création d'une clef PGP, une date d'expiration est définie et un certificat de révocation est émis. La date d'expiration doit être prolongée par leurs détenteurs et, en cas de perte de la clef privée, il est possible de la révoquer.

<sup>341</sup> En l'espèce, Amaury Séchet travaillant sur l'implémentation « *Bitcoin ABC* » (voir Awemany 2018).

<sup>342</sup> En l'espèce, Andrea Suisani travaillant sur l'implémentation « *Bitcoin Unlimited* » (voir Awemany 2018).

<sup>343</sup> Voir <https://bitcoin.org/en/bitcoin-core/contribute/issues>. et <https://bitcoincore.org/en/contact/> [consultation au 17/09/2021].

Bitcoin Core reconnus<sup>344</sup>. À sa réception, Bitcoin et les membres informés de l'équipe Bitcoin Core entrent en crise. L'amorce d'une remise en ordre nécessite d'évaluer la vulnérabilité afin d'élaborer, de discuter et de tester les remédiations potentielles, avant qu'elles ne soient acceptées par la communauté.

## Une remise en ordre rapide

Après réception du rapport d'Awemany, les trois « Core Devs » doivent d'abord réaliser un diagnostic interne de la situation, avant de proposer, discuter, produire et tester des correctifs.

### *La phase d'évaluation : définition des problèmes, des solutions et d'une stratégie de résolution*

Le diagnostic de la faille Bitcoin CVE 2018 prend moins d'un jour à une poignée d'acteurs qui vont l'évaluer, puis développer un correctif logiciel et le faire évaluer en retour par des pairs, en vue de sa validation\*/fusion dans les codes source d'une nouvelle version logicielle. D'après le rapport de divulgation complet de Bitcoin Core (2018), cette phase d'évaluation renvoie à 8 étapes clefs.

(1) G. Maxwell, l'un des contacts de sécurité et destinataire du rapport le fait suivre à réception à quatre autres « Core Devs » pour évaluation approfondie : C. Fields, M. Corallo, S. Daftuar et A. Morcos. M. Corallo, qui travaille avec Daftuar et Morcos à « Chaincode Lab »<sup>345</sup>, rapporte l'avoir trouvé sur son bureau « *quand [il est] arrivé le matin de son signalement...* » et c'est ensemble qu'ils entreprennent son analyse [M. Corallo, Entretien n°15]. (2) Cette évaluation interne fait apparaître un bogue plus critique que rapporté, scellant du même coup la stratégie d'une libération graduelle des informations. Si « *à l'origine, il a été signalé comme un crash. [...]. [Après un] temps à l'examiner, à lire le code [...], nous avons découvert la véritable vulnérabilité d'inflation* [, dès lors] *il s'agissait de savoir comment minimiser le risque pour les utilisateurs de Bitcoin [et] la réponse immédiate est... d'écrire un patch [...]. Heureusement cela nous a été rapporté comme un crash et l'exploit évident était le crash et non la vulnérabilité d'inflation. Donc la décision était... [...], de publier le crash, de parler aux gens du crash et [...] de diffuser le patch [...] qui résout une vulnérabilité réellement critique sans nécessairement mentionner l'autre vulnérabilité, plus critique encore* » [M. Corallo, Entretien n°15]. Afin de minimiser les risques pour les utilisateurs, ces Core développeurs\* décident d'occulter le bogue de faux monnayage, en insistant uniquement sur le vecteur de DOS. Toute faille confronte les personnes en charge d'y remédier à un dilemme : publier un correctif, c'est avouer publiquement l'existence d'une vulnérabilité, ce que le processus de divulgation responsable vise à cacher. D'où le « *jeu d'annoncer la vulnérabilité la plus évidente* » (la faille

---

<sup>344</sup> Tous deux « Core Devs » de longue date, P. Wuille et W. Van der Laan sont des « Core Maintainers » disposant de droits d'administration sur le répertoire Bitcoin Core (Lopp 2018) et comptent parmi les plus actifs (voir Gaurav 2019) ; Wuille, avec G. Maxwell, fait partie des co-fondateurs de l'entreprise « Blockstream » (comme M. Corallo). Il a renoncé à ses priviléges d'administration en 2015, mais reste un développeur reconnu. Voir : <https://github.com/laanwj> , <https://github.com/sipa> (voir bit2me Academy 2021) , [https://www.reddit.com/r/Bitcoin/comments/3x7mrr/gmaxwell\\_unllc\\_no\\_longer\\_a\\_bitcoin\\_committer\\_on/cy29vkx/](https://www.reddit.com/r/Bitcoin/comments/3x7mrr/gmaxwell_unllc_no_longer_a_bitcoin_committer_on/cy29vkx/) et <https://github.com/gmaxwell> [consultation au 17/09/2021].

<sup>345</sup> « Chaincode Lab » est une entreprise de recherche et développement dans l'écosystème Bitcoin, créée en 2014, dont M. Corallo était à l'époque encore salarié. Cette compagnie fut fondée par A. Morcos et S. Daftuars, deux « Core Devs » actifs et reconnus qui sont aussi co-fondateurs d'une société de trading « Hudson River Trading ». Ils se décrivent comme « *passionnés par la progression du développement du réseau Bitcoin et par la fourniture de ressources aux innovateurs indépendants de l'écosystème Bitcoin* » ; ils sont « *financés par des fonds privés* » et existent « *pour soutenir et développer Bitcoin* ». En 2020, cette entreprise est « *le leader incontesté en termes de financement des développeurs\* de Bitcoin Core* » (BitMEX Research 2020). Voir : <https://github.com/morcos> , <https://github.com/sdaftuar>, et <https://chaincode.com/> [consultation au 17/09/2021].

de déni de service), ce qui est ensuite utilisé « comme un moyen de pousser les gens à mettre à jour aussi vite que possible [...] ce qui résout tous les problèmes [M. Corallo, Entretien n°15]. Cette stratégie de divulgation fait coup double : en plus d'éclipser la faille touchant au faux monnayage, ne parler que de risques de DOS permet d'inciter les opérateurs de nœuds\* (mineurs et/ou complets) à mettre à jour rapidement leurs logiciels clients : « obtenir immédiatement du hashrate de minage avec le patch » permet de sécuriser au plus vite le réseau\*, le protocole et ses règles canoniques contre les effets délétères de cette faille. D'où le fait que, à l'étape suivante (3), M. Corallo tente de transmettre en privé le correctif à « Slush pool », une pool de minage amie, « plus facile et fiable à contacter que beaucoup de pools chinoises », sans pour autant le diffuser publiquement. Cette volonté renvoie à deux objectifs. D'abord, une évaluation par les pairs du correctif dans le respect des principes contenus dans les slogans des *coiners*\* (« don't trust verify » et « Do Your Own Research ») : pour ne pas être « dans une position où Bitcoin Core dit de sauter et tout le monde saute », des développeurs\* extérieurs, reconnus et de confiance, doivent non pas « juste [l']exécuter aveuglément »<sup>346</sup> [M. Corallo, Entretien n° 15], mais l'analyser et le tester indépendamment afin de vérifier qu'il corrige l'attaque DOS annoncée sans introduire de nouveaux problèmes, la sécurité de leur activité en dépend. Ensuite, cela sécurise une partie du réseau\* avant même que soit révélé publiquement le correctif, car « Slush Pool » représentait près de 10% de la capacité de calcul du réseau<sup>347</sup>. Cette stratégie garantit que le réseau\* Bitcoin repose sur une puissance de calcul « patchée » avant la libération publique des informations, réduisant le risque d'exploitation par des individus mal intentionnés, qui auraient compris le périmètre réel des vulnérabilités corrigées par le correctif. Cependant, aucune communication n'a pu être établie avec son CEO. (4) Étape où G. Maxwell établit une preuve de la découverte de la vulnérabilité de « faux monnayage », sous la forme d'un horodatage\* du hash\* du test de la vulnérabilité réalisé (Bitcoin Core, 2018)<sup>348</sup>. La production de cette trace vérifiable et non falsifiable permettra de confirmer les annonces futures de l'équipe Bitcoin, renseignant une volonté des acteurs de documenter la gestion des événements afin d'offrir à la communauté des éléments de transparence *a posteriori*. (5) À cette étape, la propagation des informations au-delà du premier cercle des initiés commence. J. Newbery et J. O'Beirne (Bitcoin Core 2018), qui travaillent chez « Chaincode labs » avec Corallo, Daftuar, Morocos, sont informés de la faille DOS et chargés d'alerter en privé différentes entreprises du secteur, en les prévenant qu'un correctif sera bientôt disponible. (6) Cette étape voit Corallo établir le contact avec J. Capek et P. Moravec, respectivement CEO et CTO de Slush Pool. Le correctif leur est transmis et, par téléphone, eux aussi discutent uniquement du bogue DOS : « nous leur avons envoyé le patch et ils nous ont renvoyé des questions. [...] Ils ont regardé le patch, ils l'ont analysé et nous ont posé des questions à son sujet. Nous avons répondu et ils ont pu l'appliquer assez rapidement » [M. Corallo, entretien n° 15]. (7) Slush Pool met à jour ses logiciels clients dès la fin de journée du 17 septembre, sécurisant ainsi 10% de la puissance de calcul du réseau\* contre la vulnérabilité DOS et celle de « faux monnayage ». Le 18 septembre, l'équipe Core produit et

<sup>346</sup> Ces attendus étaient explicites dans le message envoyé à Slush Pool. Corralo déclare avoir essayé « d'être un peu précautionneux et de dire : voilà le patch, voilà ce qu'il fait, s'il vous plaît vérifiez, ne prenez pas juste le patch et exécutez-le aveuglément... non s'il vous plaît vérifiez qu'il fait quelque chose qui ressemble à ce que nous prétendons [...] d'autant plus que nous leur avons envoyé un patch qui n'était pas public et qui n'était pas audible. » [M. Corallo, Entretien n° 15]

<sup>347</sup> Au 17 septembre 2018, Slush Pool représentait 9,3% de la puissance de calcul du réseau Bitcoin, voir <https://web.archive.org/web/20180916150610/https://www.blockchain.com/pools> [consultation au 17/09/2021].

<sup>348</sup> Ce hash\* est le suivant a47344b7dceddff6c6cc1c7e97f1588d99e6dba706011b6ccc2e615b88fe4350 (Bitcoin Core 2018).

publie les binaires logiciels des versions correctives et des annonces publiques annoncent la mise à jour comme « urgente » (8).

La phase d'évaluation touche à sa fin. La résolution amorcée commande encore de produire, publier et publiciser les logiciels corrigés et d'informer l'ensemble de la communauté.

### *La phase de résolution : « mensonge blanc » contre « chapeau noir »*

La phase précédente est une amorce nécessaire mais non suffisante à toute remise en ordre définitive. Il importe maintenant qu'une majorité, si ce n'est la totalité des opérateurs de nœuds\* vulnérables, consente à les mettre à jour rapidement. C'est une phase nécessaire, car elle permet de fixer et discuter entre un petit nombre d'acteurs compétents des problèmes techniques existants et des solutions potentielles. Ce bogue « *très simple* » (equobleu 2018) ne prend que quelques heures à M. Corallo pour être corrigé. Les correctifs, publiés sous forme de Pool Request (les PR#14247 et PR #14249)<sup>349</sup>, n'impliquent qu'une modification de « 4 lettres (vrai au lieu de faux) » dans les codes sources et l'ajout d'un « *test automatisé [...] pour tester le scénario du bloc avec des pièces (en "entrée") dépensées en double* » (*Ibid.*)<sup>350</sup>. Reste que cela est insuffisant. La confidentialité offerte par la dimension *off chain*\* a permis de recourir, comme par le passé<sup>351</sup>, à des silences stratégiques et « mensonges blancs », visant à produire « *une tromperie délibérée des utilisateurs* » pour mieux les protéger contre les attaques potentielles, qu'une publicité large n'aurait pas manquée d'induire (Böhme et al. 2020, p. 68). Mais cette mise au secret n'a qu'un temps. Les informations dispensées ne concernent encore qu'un petit groupe de participants là où, pour une CM, toute résolution de crise passe par la sécurisation de l'ensemble du réseau\*, donc par une publicisation large et risquée des correctifs : les mensonges blancs précédents se doivent d'être éprouvés largement, une dernière fois.

Nous rencontrons là une problématique épingleuse de la gouvernance de crise de Bitcoin et des CM, ces « *systèmes distribués [...] ont été conçus pour être difficiles à modifier afin de fournir de solides garanties sur leur comportement futur.* » (Böhme et al 2020, p. 64). Par design, toute modification de code implique nécessairement un consentement - anonyme, organisé de manière lâche et informelle - de la multitude des participants la concernant (*Ibid.*). Toute modification de code est un « *coordination challenge* » puisqu' « *aucun développeur\* ou mainteneur n'a naturellement le rôle de coordonner la correction des bogues, et encore moins l'autorité de déployer des mises à jour contre la volonté des autres participants* » (*Ibid.*). Mais ce qui précède l'a révélé, Bitcoin et son implémentation « Bitcoin Core » disposent d'un groupe de mainteneurs Core plus que « *vaguement définis* », assumant formellement la gestion

---

<sup>349</sup>Les PR #14247 et #14249 voient deux modifications (« commits » dans le jargon des développeurs\* informatiques) être fusionnées dans la branche maître Bitcoin Core (« bitcoin :master »); voir <https://github.com/bitcoin/bitcoin/pull/14249> et <https://github.com/bitcoin/bitcoin/pull/14247> [consultation au 07/10/2021].

<sup>350</sup> La ligne de code 3125, “if (!CheckTransaction(\*tx, state, false))” devient “if (!CheckTransaction(\*tx, state, true))” et le test (test/functional/p2p\_invalid\_block.py) est ajouté à la ligne 81. Voir <https://github.com/bitcoin/bitcoin/pull/14247/files#> et/ou <https://github.com/bitcoin/bitcoin/pull/14249/files> [consultation au 07/10/2021].

<sup>351</sup> Böhme et al. (2020) rappellent que, en 2014, une incohérence entre différentes versions de la bibliothèque OpenS-SL présente au sein de version logicielle Bitcoin avait déjà donné lieu à ce type de « mensonge blanc » : « *la correction d'OpenSSL n'était pas une option, d'où la nécessité d'appliquer [d]es changements [...] de manière subtile et progressive afin d'éviter d'attirer l'attention sur le morceau de code concerné. Les utilisateurs ont procédé à une mise à niveau organique sur une période de 10 mois. Le bogue a été rendu public lorsque plus de 95% des mineurs l'ont corrigé* » (p. 68).

coordonnée de la résolution des bogues (*Ibid.*). Reste que ce groupe n'est pas capable d'imposer aux autres parties ces modifications, ses membres ne disposant que de leur connaissance et persuasion. Puisqu'ils travaillent sur un logiciel à code source ouvert, tournant de manière distribuée, les mainteneurs Bitcoin Core ne disposent d'aucun moyen pour imposer une nouvelle version logicielle aux opérateurs de nœuds\* mineurs ou complets. Pour faciliter le consentement éclairé *ex ante* nécessaire à ce que tous téléchargent et se mettent à jour *ex post*, il a été institué une procédure séquentielle. Premièrement, les modifications proposées doivent être accessibles publiquement *via* le répertoire Github de « Bitcoin Core » (le « *repo* »), publiées sous forme de PR ou de « *BIP* ». Cela permet qu'elles soient évaluées et discutées. Enfin, en cas de soutien majoritaire ou plus exactement d'opposition minoritaire<sup>352</sup>, ces PR sont ensuite fusionnées dans les codes sources d'une nouvelle version logicielle. De ceux-ci, il faut encore produire des binaires logiciels accessibles au téléchargement par l'ensemble de la communauté.

Aux coordinations challenges « intracommunautaires » s'ajoute, pour la CM et l'équipe de mainteneurs qui publient les correctifs, un challenge « extra-communautaire » du fait de la nature open source des codes vulnérables. Cela accentue l'ambivalence du moment crucial qu'est la publication d'un correctif dans la gestion de crise. La faille de « faux monnayage », pour l'heure tenue sous silence, pourrait être découverte. La coordination avec d'autres équipes de CM partageant les codes vulnérables de Bitcoin Core ajoute à la complexité, d'autant qu'il existe des liens d'amitié ou d'inimitié entre ces équipes. Dans l'idéal, les « *correctifs doivent être déployés aussi simultanément que possible dans tous les projets concernés, car l'application de correctifs et la publication d'informations sur la vulnérabilité laisseraient d'autres personnes exposées si aucune précaution n'était prise.* » (Böhme et al 2020, p. 70) Dans la réalité des crises, l'idéal fait place à des réponses plus contraintes. Dans ce cas, les mainteneurs Core ont d'abord, avant toute publicisation des correctifs, envoyé un mail à l'équipe de Bitcoin ABC, pour les avertir de la publication prochaine du correctif au public (Bitcoin Core 2018). De même, fut envoyée une réponse de remerciement à Awemany, auteur du rapport anonyme. Ces précautions prises, critiquables car insuffisantes pour certains<sup>353</sup>, les correctifs sont publiés dès la fin de journée du 17 septembre (*Ibid.*). Moins d'une heure après l'envoi des mails d'alerte aux équipes de projets différents<sup>354</sup>, la démonstration du test de l'attaque par DoS est publiée sur le « *repo* » public « Bitcoin Core » (la PR #14247). Dans la foulée, une campagne de communication visibilisant le bogue et son correctif est lancée à l'adresse de différentes listes de diffusion (*Ibid.*). Dans la soirée, une nouvelle version logicielle

---

<sup>352</sup> Comme nous le verrons, le consensus ne renvoie pas tant à un fait majoritaire selon une définition de la majorité, ni même à une unanimité, puisque s'abstenir correspond à ne pas s'opposer, qu'à l'absence d'opposition franche. La définition d'un consensus communautaire large et les outils de sa mesure sont problématiques, d'où l'existence de controverses et l'expérimentation de procédures d'expression des désaccords variés, toujours évolutives et mouvantes (cf. section III.3).

<sup>353</sup> Les acteurs de la communauté Bitcoin Cash sont critiques, considérant avoir été mis au pied du mur par une divulgation irresponsable de l'équipe Bitcoin Core (Awemany 2018, A. Sechet voir <https://github.com/bitcoin/bitcoin/pull/14247#issuecomment-422603346> ou encore « ftrader » voir <https://github.com/bitcoin/bitcoin/pull/14247#issuecomment-422499799>; [consultation au 12/10/2021]. Cette controverse est nourrie de ressentiments remontant au schisme communautaire consécutif au « Scaling Debate » (cf. Chap. II). D'autres projets vulnérables, non informés, ne sont pas corrigés et l'un d'eux (« PigeonCoin ») subit une double dépense exploitant la faille pour près de 235 millions d'UCN, soit 25% de l'offre en circulation (Esteves 2018 ; Hertig 2018).

<sup>354</sup> Le rapport de divulgation complète (Bitcoin Core 2018) établit que l'équipe Bitcoin Cash a publié son propre correctif une minute seulement après la publication du PR 14247 sur Bitcoin Core.

Bitcoin Core est « taggée » (version 0.17.0rc4<sup>355</sup>, *Ibid.*). La production des nouvelles versions logicielles téléchargeables doit attendre.

Au sein de Bitcoin Core, la création et la publication de nouveaux codes binaires logiciels suit une procédure collective de sécurité innovante, nommée « *Gitian Building* » (Wirdum 2018), nécessitant que plusieurs membres reconnus de la communauté produisent, chacun de son côté et de manière déterministe, des binaires similaires : « *les correctifs pour les branches master et 0.16 [...] soumis à l'examen public hier* » et « *la version 0.16.3 [...] étiquetée comme contenant le correctif [...]* », encore faut-il « *qu'un nombre suffisant de contributeurs connus [aient] reproduit la construction déterministe* » (Bitcoin Optech 2018). À ces conditions sont rendues disponibles au téléchargement les nouvelles versions logicielles, d'où l'importance des annonces réalisées visant une mobilisation communautaire large. Ainsi, la version 0.16.3, « taguée » tôt dans la matinée du 18 septembre, attendra le lendemain soir pour voir les premières versions être produites, publiées et ouvertes au téléchargement. Suite à cette publication, la publicisation s'intensifie. Au-delà des cercles techniciens premiers (exemple de la lettre d'information d'*« Optech »*<sup>356</sup>), des canaux de diffusion s'adressant à un public plus large sont mobilisés afin d'atteindre l'ensemble de la communauté : faille et correctif sont annoncés sur Reddit<sup>357</sup> et BitcoinTalk<sup>358</sup> ; le 19, une nouvelle campagne vise différentes listes de diffusion. Cette mobilisation de canaux d'information hétéroclites doit permettre la mobilisation large et rapide nécessaire à une mise à jour expresse, ordonnée et massive des clients logiciel, nombreux à l'époque des faits à être vulnérables. Les données montrent que ces campagnes d'information ont porté leurs fruits (voir le Tableau 3 ci-après).

---

<sup>355</sup> Ces « tagues » ou « balises » sont des références permettant de marquer/nommer des points d'étape de l'historique de développement du projet et ses versions (v1.0, v1.0.1, v2.0 etc.). Sur ces procédures de développement logiciel, voir pour GIT (<https://git-scm.com/book/en/v2/Git-Basics-Tagging>) ou, spécifiquement pour Github (<https://docs.github.com/en/desktop/contributing-and-collaborating-using-github-desktop/managing-commits/managing-tags>). L'ensemble des différentes versions « taguées » Bitcoin Core historiquement publiées est consultable ici : <https://github.com/bitcoin/bitcoin/tags> [consultation au 08/10/2021].

<sup>356</sup> Cette lettre d'information est adressée à des acteurs techniciens. L'édition du 18 septembre revient sur la vulnérabilité DOS et la publication des versions correctives Bitcoin Core 0.16.3 et 0.17rc4. Voir Bitcoin Optech (2018).

<sup>357</sup> Voir <https://web.archive.org/web/20180918221912/https://www.reddit.com/r/Bitcoin/> [consultation au 08/10/2021].

<sup>358</sup> Voir <https://bitcointalk.org/index.php?topic=5032424.0> [consultation au 08/10/2021].

**Tableau 3 : Nombre et parts relatives des nœuds vulnérables<sup>359</sup>**

| Date       | Nombre total de nœuds* Bitcoin | Somme & parts des versions vulnérables |                |                       |
|------------|--------------------------------|--|----------------|-----------------------|
|            |                                | Ensemble                               | Version 0.14.x | Version 0.15.x-0.16.x |
| 18/09/2018 | 9590                           | 82.56%                                 | 4,3%           | 78,3%                 |
| 23/09/2018 | 9831                           | 55.38%                                 | 0 %            | 55,38 %               |
| 23/10/2018 | 9847                           | 38.6%                                  | 0 %            | 38.6%                 |
| 01/01/2019 | 10162                          | 23.43%                                 | 0 %            | 23.43%                |
| 28/06/2019 | 10318                          | 11.24%                                 | 0 %            | 11.24%                |
| 07/01/2020 | 11204                          | 6.16%                                  | 0 %            | 6.16%                 |
| 23/09/2020 | 10000                          | 4.89%                                  | 0 %            | 4.89%                 |
| 25/06/2021 | 9909                           | 4,28 %                                 | 0 %            | 4,28 %                |

Source : Rolland Maël

En juin 2021 encore, on trouve de rares nœuds\* Bitcoin (moins de 5%) non encore mis à jour, restant exposés à ces vulnérabilités. Mais, à l'époque, la sécurisation du réseau\* va s'opérer relativement rapidement : au 18 septembre, ce sont près de 82% des nœuds\* qui étaient vulnérables (près de 4% pour la faille DOS et près de 78% pour celle de « faux monnayage » !!!!). Cinq jours après les premières annonces publiques, on ne trouve déjà plus aucun nœud\* tournant sur les versions 0.14.x ; ceux fonctionnant sur les versions 0.15.x-0.16.x vulnérables, encore majoritaires, voient leur part baisser de près de 23%. Cette réactivité importe pour la sécurité de Bitcoin, car, ce même jour du 20 septembre, le mensonge blanc s'évante enfin : sur un forum public, un post fait état de la faille de faux monnayage et même s'« *il [a] été rapidement rétracté, l'affirmation a continué à circuler* » (Bitcoin Core 2018). Mais cette première libération publique n'a plus de quoi inquiéter l'équipe Bitcoin Core : « *plus de la moitié du hash\*rate Bitcoin a été mis à niveau vers des nœuds\* corrigés* » et si « *aucune tentative d'exploitation de cette vulnérabilité* » n'avait été décelée jusqu'alors, les possibilités de réussir une telle attaque s'amenuisent au fur et à mesure que le réseau\* voit la part des

---

<sup>359</sup> Ces estimations sont imparfaites. Tout d'abord, car notre première source, le site <https://coin.dance/nodes#nodeVersions> [consultation au 25/06/2021] ne décompte que le nombre de nœuds\* Bitcoin publiquement accessibles. L'estimation est basse par construction, excluant les nœuds\* non publics (passant par TOR par exemple, voir Luke Dashjr, [luke.dashjr.org/programs/bitcoin/files/charts/](http://luke.dashjr.org/programs/bitcoin/files/charts/)). A. Le Calvez [Entretien n°20] précise que les données relatives aux implémentations et aux versions sont déclaratives et qu'il est impossible d'en prouver la véracité : « l'affichage du numéro de version c'est quelque chose d'optionnel, enfin d'optionnel, c'est dur à vérifier finalement. Puisque je peux faire croire que je suis un 0.14 alors qu'en fait je suis un programme qui n'est pas du tout un nœud\* » (Entretien n°20). Puisque les données plus anciennes nous intéressent n'étaient pas accessibles sur « Coindance », nous avons mobilisé en complément la « Wayback Machine » d'« Internet Archive ». Cet outil dépendant des instantanés réalisés, nous n'avons pas pu choisir les dates. Nos estimations coïncident avec celle donnée par Bitcoin Core (2018).

nœuds\* corrigés augmenter. (*Ibid.*). Au 20 octobre 2018, soit un mois après, la part des nœuds\* vulnérables au « faux monnayage » tombait à 38 %, pour chuter, entre juin 2019 et janvier 2020, à moins de 10% du réseau\*. Ce 20 septembre, alors que le secret bien gardé a commencé à s'éventer<sup>360</sup> et puisqu'une part importante du réseau\* a déjà été patché, l'équipe Bitcoin Core va mettre un point final à la crise : est publié le rapport de divulgation complète. Avec lui, est reconnue pour la première fois publiquement l'existence d'une faille impliquant un « faux monnayage » par double dépense (Bitcoin Core 2018). Le 21 septembre, Awemany sort de son silence et de l'anonymat, par la publication d'un billet de blog retraçant son implication dans les évènements (Awemany 2018). Ce texte prendra part, avec d'autres, à la controverse entourant la gestion de cette crise par l'équipe Bitcoin Core, qui, nous le verrons, est nourrie de ressentiments passés. Néanmoins, la crise traversée par Bitcoin et sa communauté est close : les vulnérabilités sont corrigées et révélées publiquement à tous, et le réseau\* est déjà prémuni contre elles.

### III.1.2 Restituer cette crise dans l'histoire de celles traversées par Bitcoin

Mettre en perspective les événements entourant la faille Bitcoin CVE 2018 nous forçait à ne pas s'arrêter à eux. Le questionnement sur la nature de cette crise pointait vers d'autres crises appelant à être démêlées : « ce n'est pas la première vulnérabilité à l'inflation [...] peu importe 0.1 ; 0.2, je ne me souviens pas des bogues de l'époque » [M. Corallo, Entretien n°15]. Impossible de ne pas voir ce que le Chapitre I a pris soin d'introduire : des crises nombreuses et diversifiées ont concouru au développement infrastructurel de Bitcoin, qu'elles aient été directement protocolaires (comme avec Bitcoin CVE 2018) ou plus largement infrastructurelles, touchant à des composants socio-techniques clefs à leur fonctionnement et usage (cf. bourse, portefeuilles\* ; cf. Chronologie 2 Chap. I). D'où notre affirmation : non, la confiance et ses trois dimensions (éthique, hiérarchique et méthodique ; cf. Chap. II) ne se cristallisent pas tout entières dans le code ou seulement dans son *algorithme cryptographique*. Toutes les lignes de codes Bitcoin, comme l'ensemble des pathologies qui peuvent les toucher, n'ont pas la même importance pour son fonctionnement. Cela renvoie à l'existence de ce qui est pourtant nié explicitement (Dupré, Ponsot et Servet 2015) : une structuration sociale où se tiennent des débats politiques *hors chaîne\**, au sein desquels se jouent aussi, et de manière complémentaire, les trois types de confiance.

En outre, de nombreuses informations concernant ces différentes crises étaient accessibles en ligne. Certaines émanent très directement d'un groupe d'acteurs pour qui ces préoccupations sécuritaires sont centrales (et dont Corallo fait partie). Même si nombreux sont les *coiners\** à se désintéresser des crises que leurs CM pourraient rencontrer, il serait excessif, partial et faux de laisser penser que l'ensemble des « *bitcoiners\** » partage une même « *foi dans le bitcoin* » et aurait une « *confiance aveugle exprimée [...] dans le code et l'algorithme* », alors que ceux-ci sont le produit d'acteurs éminemment conscients des risques et qui savent que toute technologie, en particulier celle qu'ils développent, est loin d'être « *infaillible* » (Ponsot 2021, p. 2). Dès l'origine, les CM sont conçues pour fonctionner dans un *environnement adverse* (Nakamoto 2008). Cela est même un critère définitionnel propre (Rauchs et al. 2018, cf. Chap. II). La sécurité de Bitcoin est suspendue à des conditions jamais données. Au-delà des seules « attaques 51% » sur lesquelles insiste le WP\* de Nakamoto (2008), une variété de

---

<sup>360</sup> En plus de la publication d'un premier message explicitant le bogue de consensus, le 20 septembre voit un autre développeur extérieur - David Jaenson, qui travaille sur le projet Qtum - découvrir indépendamment cette vulnérabilité (Bitcoin Core 2018, Hacker News Forum 2018). Il la rapporte à l'équipe Bitcoin Core le même jour, via la liste des e-mails de contact sécurité (Bitcoin Core 2018) et publiera le correctif sur le github du projet Qtum (Bitcoin Core 2018).

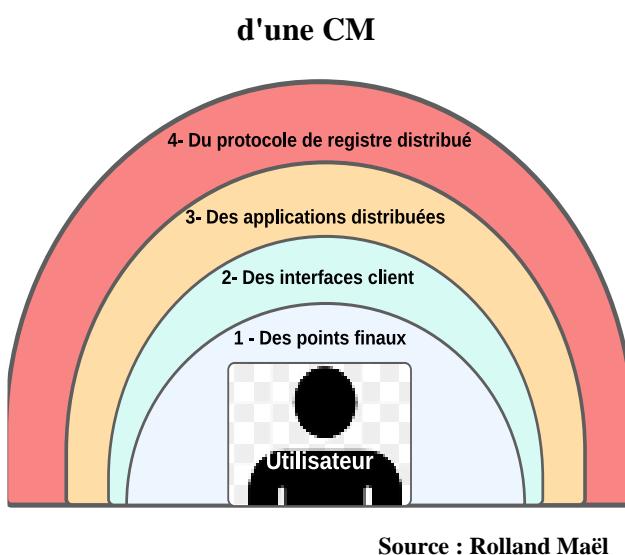
dysfonctionnements, voire d'attaques, existent, pouvant compromettre ses propriétés désirées (décentralisation, résistance à la censure\*, pseudonymat, etc.).

## De la diversité des crises aux crises protocolaires des CM

Bitcoin, comme infrastructure monétaire, repose primordialement sur l'articulation complexe de dispositifs techniques et informatiques. Le maintien de la viabilité infrastructurelle ne se réduit pas à la seule maintenance du protocole, comme le visibilise la crise précédente, loin s'en faut. Si notre intérêt partira des crises protocolaires, n'oublions pas que, en tant qu'infrastructure, une CM se décompose en différents sous-systèmes articulés, mobilisant des composantes et des interactions à la fois *au sein de la chaîne\** et en *dehors de celle-ci* : Bitcoin et Ethereum sont des mille-feuilles d'acteurs, d'arrangements et de dispositifs hétérogènes, et leurs propriétés de sécurité, de stabilité et de confiance relèvent d'une multi-dimensionnalité où le technique, le légal, le réglementaire et le socio-économique s'enchevêtrent (cf. Chap. I, section I.2). Bitcoin et ses parties prenantes sont ainsi exposés à des risques et crises pouvant revêtir des formes très différentes.

Une CM et sa communauté peuvent être ébranlées par des crises affectant non seulement le protocole de la CM, mais aussi tout autre composant et domaine participant de leur infrastructure. Pour utiliser une CM, l'usager fait d'emblée face à sa dimension infrastructurelle et, à chaque étape ou couche, peut voir s'installer le bogue ou l'attaque informatique : il doit mobiliser une machine (ordinateur ou téléphone), avoir un accès internet, un navigateur et d'autres applications tierces médiatisant ses interactions *on chain*, et chacun peut être dysfonctionnel ou avoir été compromis. Chacun des quatre domaines de sécurité informatique distingués dans le champ de la science informatique (Lee 2019, p. 38-39, Figure 11 suivante) peut connaître des crises, renvoyant à 6 grandes familles de menaces et 17 risques de sécurité associés (*Ibid.* p.34-36)<sup>361</sup>.

**Figure 11 : Les quatre grands domaines de crise**



**1- Domaine des points finaux**, correspondant à l'ensemble des éléments machines (dit « *hardware* ») dont l'usager a besoin afin d'interagir avec le protocole ou avec les interfaces clients en question (ordinateurs et mobiles, portefeuilles\* physiques, terminaux de paiement, etc.).

**2- Domaine des interfaces client**, renvoyant à l'ensemble des éléments logiciels (dit « *software* ») servant d'interface entre l'usager et le protocole (application tierce et leur « *front end* », cf. interfaces de plateforme d'échange, de DEX et autres « *Dapp* », etc.).

**3- Domaine des applications distribuées**, renvoyant à l'ensemble des

<sup>361</sup> À la granularité académique très fine de Lee (2019, p.37 et 61-64), nous avons préféré pour la suite nous en tenir aux labellisations indigènes que nous avons rencontrées, et que cette section vise à présenter.

scripts à exécution programmatique (cf. *Smart Contract*<sup>\*</sup>) mobilisés et qui peuvent contenir des vulnérabilités ou avoir été économiquement mal conçus.

**4- Domaine des protocoles de registre distribué**, couvrant l'ensemble des éléments constitutifs du protocole de registre<sup>\*</sup> distribué, qu'ils relèvent de la couche protocolaire, de la couche réseau<sup>\*</sup> P2P ou de la couche base de données (cf. Annexe n°V.6).

Bien que chaque domaine puisse entrer en jeu et/ou participer d'une crise de CM, suivant le tropisme des *bitcoiners*<sup>\*</sup>, notre attention s'est portée spécifiquement sur les crises Bitcoin relevant du domaine du protocole de registre<sup>\*</sup> distribué. Aucune volonté de minimiser les conséquences importantes sur l'écosystème et la valeur d'échange de l'UCN<sup>\*</sup>, que les réglementations et annonces légales, les attaques et vols de plateforme d'échange, perte/vol individuel, arnaques, exploitation de vulnérabilité dans des SC, peuvent induire (en témoigne notre chronologie du chapitre I). Mais nous avons voulu cibler l'objet central des *coiners*<sup>\*</sup>, pour qui les domaines non protocolaires n'ont pas en soi de pertinence, du fait justement qu'ils renvoient à un ailleurs protocolaire duquel ils se revendiquent autonomes. De cette manière, cela permettait d'interroger frontalement les CM et leur communauté sur les conditions nécessaires au maintien de la sécurité, des propriétés fonctionnelles désirées et de la confiance qui leur est accordée.

### Enjeux des crises Bitcoin : labélisations indigènes et exemples historiques

Nos recherches sur le Bogue CVE 2018 #17144 nous ont conduit à mettre au jour le nombre important de crises protocolaires que Bitcoin et sa communauté ont eu à essuyer. Une requête en ligne associant les mots « Bitcoin », « CVE », « vulnerability » nous fit rencontrer une base de données tenue par des volontaires, sous forme d'un wiki Bitcoin communautaire<sup>362</sup>, où est consigné l'ensemble des bogues protocolaires Bitcoin (c'est-à-dire perçus comme tels). La réalisation de la chronologie suivante et le défrichage netnographique associé nous confrontèrent au fait que traiter des crises, c'est d'abord traiter les marques de leur fabrication et de leur gouvernance. Nous avons découvert des documents d'information, des acteurs, des dispositifs, des lieux et arènes hétérogènes. Ces documents et le jargon usité (« *affect* », « *severity* », « *attack is..* », « *flaws* », « *fix* », « *fix deployment* », voir Bitcoin Wiki) déployait des distinctions entre types de failles, associés à des dispositifs d'informations/publicisation, des catégories et labélisations (comme CVE ou BIP), des dates d'annonce pas forcément publique, des informations concernant les implémentations logicielles (« *wxBitcoin* », « *bitcoind* », « *Bitcoin-QT* ») et les versions affectées et corrigées (0.3.4 ;0.3.5, etc.), l'établissement de niveaux de sévérité, de procédures de résolution, etc. Le numéro d'identification CVE renseigne sur le fait que les *bitcoiners*<sup>\*</sup> ont intégré à leur infrastructure des artefacts existants, en l'espèce la procédure d'étiquetage/publicisation normalisée du système « *Common Vulnerabilities & Exposures* » (ou CVE). Ce système suppose la mise à disposition d'une base de données publique contenant une référence publique, une date et un numéro d'identification, qui doit permettre de reporter, d'annoncer, de référencer, donc d'informer le public des failles de sécurité informatique<sup>363</sup>. Ce système étant ancien et généralement utilisé dans le développement informatique, les *bitcoiners*<sup>\*</sup> ont ajouté une labélisation *ad hoc*, mieux taillée pour leur besoin, qu'ils mobilisent conventionnellement (Tableau 4 suivant, *Ibid.*).

---

<sup>362</sup> Voir [https://en.bitcoin.it/wiki/Common\\_Vulnerabilities\\_and\\_Exposures](https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures) [consultation au 20/10/2021].

<sup>363</sup> Voir <https://nvd.nist.gov/vuln/detail/CVE-2018-17144#VulnChangeHistorySection> [consultation au 20/10/2021].

**Tableau 4 : Labérisation indigène des vulnérabilités de Bitcoin**

| Label « indigène »                           | Définition   |
|--|--|
| <b>Scission du réseau*   « Netsplit »</b>    | L'unicité du réseau* et du registre* canonique est remise en cause : apparition d'un ou plusieurs réseau*(x) différent(s), avec des nœuds* travaillant sur des historiques de transactions* différents, sans convergence possible. |
| <b>Attaque par Déni de Service   « DOS »</b> | L'accès au réseau* est plus ou moins perturbé, des nœuds* rencontrant des problèmes (crash, difficulté de traitement des données entrantes, etc.).   |
| <b>Vol   « Theft »</b>                       | Un ou plusieurs acteur(s) peu(ven)t prendre le contrôle d'UCN* en dehors des règles protocolaires consensuelles.   |
| <b>Faux monnayage   « Inflation »</b>        | Un ou plusieurs acteur(s) peu(ven)t créer des UCN* en dehors des règles de monnayage protocolaire canonique.   |
| <b>Exposition   « Exposure »</b>             | Un ou plusieurs acteur(s) peu(ven)t accéder à des données d'un ou plusieurs utilisateur(s) en dehors de ce qui est conventionnellement prévu.  |
| <b>Inconnue   « Unknown »</b>                | L'étendue des abus potentiels n'est pas connue précisément.  |
| <b>Fausse confirmation   « Fake Conf »</b>   | Un ou plusieurs acteur(s) peu(ven)t réaliser des doubles dépenses avec une confirmation*.  |
| <b>Tromperie   « Deception »</b>             | Un ou plusieurs acteur(s) peu(ven)t propager des informations erronées au sein du réseau*.   |

Source : Rolland Maël

Construite pratiquement, cette labérisation permet de catégoriser l'ensemble des bogues/failles passés ou futurs de Bitcoin. Chaque label dessine les frontières de grands types de crises protocolaires et des actions pathologiques induites. Pour chaque crise, les *bitcoiners*\* ajoutent à ces labels des informations concernant le degré de gravité (« *easy* », « *hard* », « *very hard* ») et/ou des acteurs concernés (« *miners* », « *Keyholders* », « *RPC access* », etc.). Cet étiquetage permet de caractériser et de publiciser les différents bogues et d'en informer l'ensemble des membres de la communauté. Cette normalisation indigène constitue le fond et la forme des crises répertoriées, qui a servi de matériau à la réalisation de la chronologie que nous avons construite.

Grâce aux données de Bitcoin Wiki croisées avec d'autres sources, nous avons répertorié<sup>364</sup> pas moins de 38 crises entre 2009 et la fin 2019 (cf. Chronologie 4 suivante). Chaque crise répertoriée est représentée par un rectangle contenant, de haut en bas : (i) un identifiant, renvoyant à deux systèmes d'identification différents, présentant soit le numéro CVE de la vulnérabilité, soit celui du « BIP » impliqué dans la survenue et/ou la résolution du problème, ces deux types d'identification pointant une distinction franche entre deux familles génériques de crise et l'existence concomitante de procédures de résolution différencierées (cf. code couleur); (ii) le type de crise, en suivant la labélisation indigène constituée de 8 labels (cf. section prochaine) permettant de couvrir l'ensemble des risques de vulnérabilité protocolaire potentiels, auquel (iii) nous ajoutons des informations les concernant ; enfin, (iv) la date de divulgation publique d'abord, si elle ne coïncide pas avec la date de la première divulgation (privée). Cette dernière est toujours présentée en dernier et conçue comme date de déclenchement effectif ; les deux dates éclairent sur la durée, parfois prolongée, des actions correctives entreprises, pendant laquelle la communauté n'a pas d'information les concernant. Étant donné la faible diversité logicielle sur Bitcoin, nous n'avons pas listé les différentes implémentations et versions affectées. Nous avons pour finir utilisé un code couleur<sup>365</sup>. L'encadrement du texte vise à différencier les labels/types de vulnérabilité au cœur de nos cas d'étude de ceux qui y sont étrangers, regroupés ensemble : encadrées en rouge, les crises induisant un risque de « faux monnayage » (ou « *inflation* », il y en a 3); en marron, les crises induisant un risque de scission du réseau\* (« *Netsplit* », il y en a 4) ; et en bleu, celles induisant un risque de DOS (elles sont au nombre de 13). Celles restantes (« vol », « exposition », « inconnue », « fausse confirmation\* », « tromperie ») ont été regroupées, en vert.

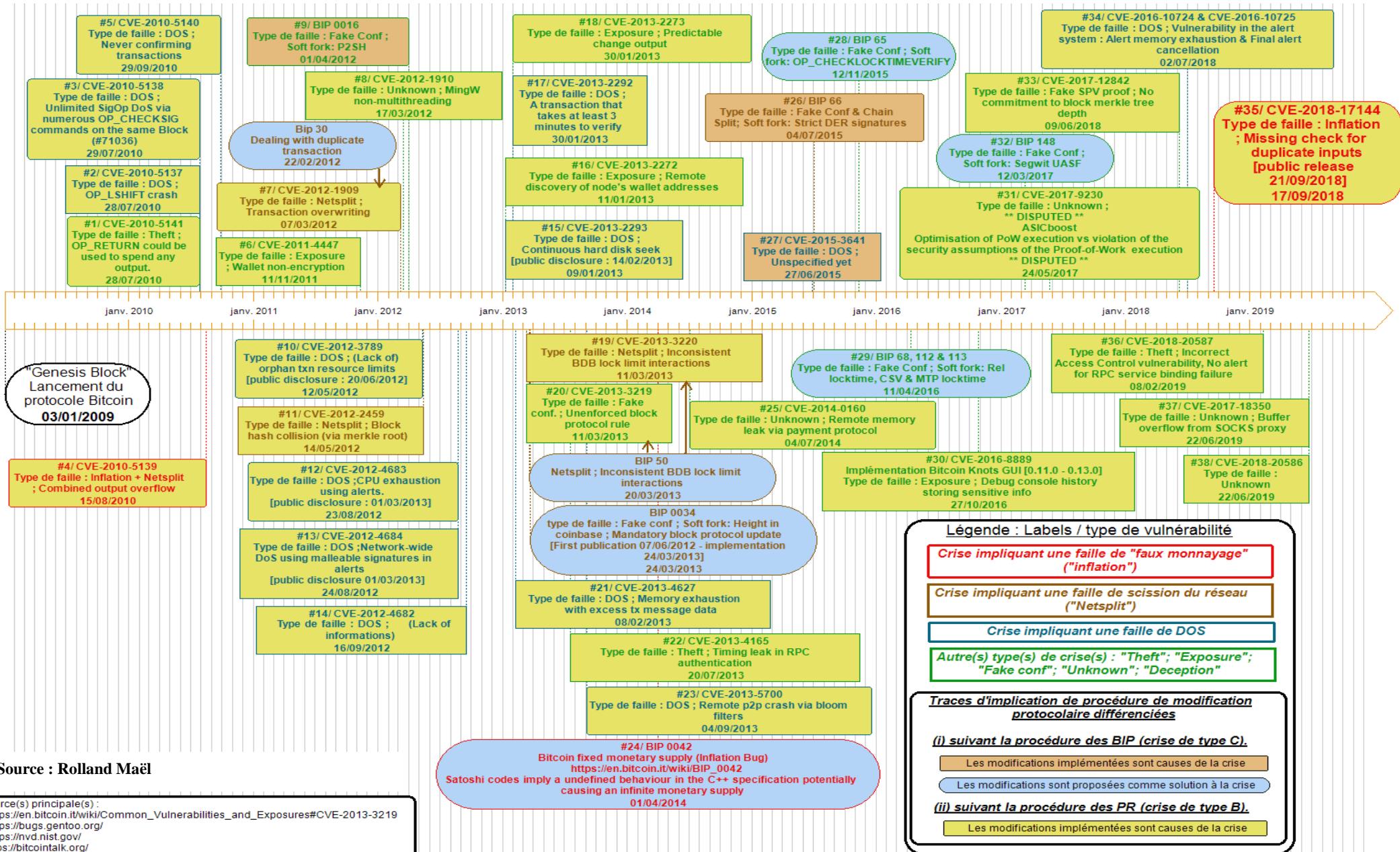
La couleur du fond encadré souligne quant à elle les procédures de modifications protocolaires impliquées (dans l'insémination ou la résolution) des vulnérabilités : en cas d'implication de la procédure appelée BIP, pour « *Bitcoin Improvement Proposal* » (cf. section n°I.2.3 suivante), le fond bleu clair indique que la vulnérabilité a été introduite par un BIP (comme cela s'est produit 3 fois), là où le fond orange foncé dénote au contraire que c'est la résolution (« *FIX* ») qui est passée par cette procédure (les flèches précisant le lien entre la faille et son BIP de résolution). Dans le cas inverse, c'est la procédure des « *Poll request* » qui est impliquée, soit dans la mise en crise, soit dans la résolution (en jaune, comme ce fut le cas de la crise Bitcoin CVE 2018). Cet ensemble va nous permettre de mettre en perspective les enjeux de la crise CVE 2018.

---

<sup>364</sup> Ce recensement ne prétend pas à l'exhaustivité. Tout d'abord, car certaines crises ont un statut controversé, comme c'est le cas de la crise n°31/ CVE-2017-9230 concernant l' « ASICboost » : pour certains, cette méthode de traitement des transactions\* dans la production des enregistrements correspond à une violation des hypothèses de sécurité posées par Nakamoto [Anon , Entretien n°3] ; pour d'autres, c'est une méthode qui, bien que non envisagée à l'origine, est possible, d'où son absence sur le site [https://en.bitcoin.it/wiki/Common\\_Vulnerabilities\\_and\\_Exposures](https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures), [consultation au 29/10/2021]. Ensuite, en vue de simplification et suivant la circonscription de nos terrains, notre recensement est limité aux vulnérabilités affectant le protocole Bitcoin et ses logiciels canoniques, celles affectant le protocole « Lightning Network » ou les logiciels et services tiers ayant été laissées de côté.

<sup>365</sup> En cas d'itérations multiples de faille, la couleur renvoie à la gravité la plus élevée. Par exemple, la crise n°26 labélisée « *Fake conf* » a failli causer une « scission de chaîne » (Light 2019), d'où l'utilisation du marron.

## Chronologie 4 : Bitcoin, une histoire rythmée de crises à gérer



## Crise de « faux monnayage », ou l’immutabilité des règles de monnayages en question

Les bogues portant l’étiquette « inflation », bien que rares (3 recensés, crises n° 4, 24 et 35, en rouge dans notre chronologie), sont particulièrement critiques. Ils touchent à la confiance éthique et hiérarchique en remettant en cause l’« immutabilité » et la prévisibilité du monnayage comme des règles transactionnelles : leur présence introduit un doute sur le fait que l’offre monétaire suive les modalités d’émission reconnues comme canoniques, puisque des UCN\* peuvent être émises en dehors des limites protocolaires. Du fait de leur gravité, ces bogues représentent l’une des principales préoccupations des développeurs\*, qui doivent tout « faire pour que le système Bitcoin fonctionne comme attendu par les utilisateurs, c'est-à-dire que la masse monétaire soit limitée à 21 millions d'unités, que personne ne puisse imprimer de l'argent, toutes ces choses standards que l'on peut souhaiter, hehehe [cela le fait sourire], avec [...] Bitcoin » [M. Corallo ; entretien n° 15]. Historiquement, « ce n'est pas la première fois que Bitcoin est vulnérable à l'inflation mais, hum [...] c'est la première depuis Satoshi » [M. Corallo ; entretien n° 15]. La crise CVE 2018 #17144 est même, suivant notre décompte, la troisième occurrence de ce type de crise et la deuxième depuis le départ de son/ses créateur(s). Mais seule la première a conduit à l’émission effective d’UCN\* en dehors des règles de monnayage qu’aurait fixées Nakamoto.

La première crise de faux monnayage dont parle Corallo est la faille CVE 2010 #5139 (crise n° 4) d’août 2010, communément appelée « *Bitcoin bug Value Overflow* ». Arrivée dans l’enfance de Bitcoin, c’est S. Nakamoto et les premiers développeurs\* qui se chargeront de la remise en ordre. Le 15 août, un « *enregistrement étrange* [, le] 74638 »<sup>366</sup> est pointé par J. Garzik sur *Bitcointalk*. Les *bitcoiners*\* présents échangent leurs analyses. Ce bloc aurait subi « *un débordement d’entier* » (« *integer overflow* ») où la « *somme des deux sorties déborde sur un négatif. C'est un bug dans les contrôles de transaction*\* qui ne l'ont pas rejeté, puis quelqu'un l'a remarqué et l'a exploité. On peut supposer qu'une nouvelle version sera en mesure de la rejeter et de lancer un nouveau Fork\* valide. » (« *Ifm* »<sup>367</sup>). Bien au-delà du cap des 21 millions d’UCN\*, l’exploitation en crée plus de 184 milliards. Pour les acteurs, le code fautif n'est pas loi, les résultats qu'il produit sont « *un sérieux problème* » (« *Theymos* »<sup>368</sup>), expliquant une remise en ordre réalisée en quelques heures et mobilisant la grosse artillerie. G. Andresen rend un premier correctif « *disponible avant le réveil de Satoshi* » (« *myzerydearia* »<sup>369</sup>), « *jusqu'à ce qu'il y ait une meilleure solution...* »<sup>370</sup>. Dès la découverte du problème, Nakamoto s’attèle au correctif. S’il publie rapidement un « *changement préliminaire* », il a « *d'autres changements à faire* »<sup>371</sup> et, pour gagner du temps, il enjoint les mineurs à stopper leurs opérations. L’utilisateur « *imf* » l’a anticipé, la solution est de faire un *Fork*\*, « *refaire une branche autour de la branche actuelle* », aussi « *cela aiderait si les gens arrêtaient de générer* [de nouveaux blocs, NdA] » car « *moins vous générerez, plus vite ce sera fait* »<sup>372</sup>. La remise en ordre suppose de remplacer/supprimer l’enregistrement pathologique du registre\* canonique en le rendant orphelin (cf. chap. I) afin de revenir dans le temps des enregistrements. La solution implique le développement et la publication d’une version logicielle corrigée (la v0.3.10<sup>373</sup>) et que les opérateurs de nœuds\* (mineurs ou complets) se mettent à jour et

---

<sup>366</sup> Voir le post original et la discussion ouverte ici : <https://bitcointalk.org/index.php?topic=822.0>, qui s'est ensuite reportée sur le fils du forum des développeurs\*, là : <https://bitcointalk.org/index.php?topic=823> , (consultation au 02/11/2021).

<sup>367</sup> Voir <https://bitcointalk.org/index.php?topic=822.msg9487#msg9487> [consultation au 02/11/2021].

<sup>368</sup> Voir <https://bitcointalk.org/index.php?topic=822.msg9481#msg9481> [consultation au 02/11/2021].

<sup>369</sup> Voir <https://bitcointalk.org/index.php?topic=822.msg10348#msg10348> [consultation au 02/11/2021].

<sup>370</sup> Voir <https://bitcointalk.org/index.php?topic=823.msg9524#msg9524> [consultation au 02/11/2021].

<sup>371</sup> Voir <https://bitcointalk.org/index.php?topic=823.msg9530#msg9530> [consultation au 02/11/2021].

<sup>372</sup> Voir <https://bitcointalk.org/index.php?topic=823.msg9531#msg9531> [consultation au 02/11/2021].

<sup>373</sup> Voir <https://bitcointalk.org/index.php?topic=827.0> [consultation au 03/11/2021].

remplacent leurs versions locales du registre\* pour une version d'« *avant le bloc 74000* ». Dans ce cas, ce n'est pas le consensus de Nakamoto en PoW\* qui « *résout le problème de la détermination de la représentation dans la prise de décision à la majorité* » (Nakamoto 2008c, p. 3), mais l'homme Nakamoto qui fait consensus autour de son correctif, grâce à une coordination à l'opposé de « *minimale* » (*Ibid.*, p. 8) : la convergence de tous les nœuds\* sur un historique ne contenant pas l'émission surnuméraire ne passe pas par l'application automatique d'un consensus technique, elle se fait contre lui, par consensus social et coordination *off chain*\*, « *environ cinq heures après l'incident [...] avant que la « bonne » chaîne ne reprenne la tête du PoW\** ». Bien que d'autres le contestent (Bitmex Research 2017a), la remédiation de cette crise est conçue par certains *coiners*\* comme une remise en ordre de type « *RollBack* » (Dino Mark, cité par Shin 2022, p. 144), un type de modification protocolaire hautement problématique pour une CM et les *coiners*\* les plus rigoristes, car il correspond à une remise en cause du principe de l'inviolabilité des données endogènes\* consignées dans la chaîne (cf. section III.3.). Cette crise est la seule à avoir conduit effectivement à sortir, pour un temps, du cadre de monnayage reconnu de tous les *bitcoiners*\*.

Ce que ceux-ci savent moins, c'est que ce cadre et le cap des 21 millions d'UCN\* bitcoin, *soi-disant* fixés dans le marbre dès l'origine, Nakamoto, faillible, l'avait mal programmé à l'origine, et il ne fut effectivement « fixé » dans le code qu'en 2014, à l'occasion de la seconde crise étiquetée « faux monnayage ». Elle renvoie au « *Bitcoin Improvement Proposal #0042* » (crise n°24) d'avril 2014, qui la corrigera. Latente, cette vulnérabilité n'a pas conduit à une émission surnuméraire, mais, sur le temps long, elle y conduisait programmatiquement. En effet, les codes de Nakamoto visant à fixer la limite des 21 millions d'UCN\* étaient défaillants, sans que personne n'y ait jamais prêté attention. La propriété la plus vantée des *bitcoiners*\* dut attendre près de 5 ans après le lancement de Bitcoin avant d'être réellement implémentée dans ses codes logiciels, en 2014. L'erreur fut découverte par P. Wuille, qui joint à l'annonce publique une proposition de remédiation, sous la forme du BIP n°0042. Pour coller à l'énormité de l'erreur, le tout est réalisé le 1<sup>er</sup> avril, avec un ton volontairement humoristique<sup>374</sup> : « *bien que l'on pense généralement que Satoshi était un goldbug détestant l'inflation, il n'a jamais dit cela et a en fait programmé la masse monétaire du bitcoin pour qu'elle augmente indéfiniment, pour toujours. Il a modélisé la masse monétaire comme 4 mines d'or découvertes par millénium (1024 ans), avec des intervalles égaux entre elles, chacune étant épuisée au cours de 140 ans.* »<sup>375</sup> L'erreur qui devait conduire à ce que de nouveaux cycles d'émission de 21 millions d'UCN\* « *recommence[nt] tous les 250 ans* » repose sur une erreur d'utilisation du langage C++ (« *the code was just illegal C++* », P. Wuille<sup>376</sup>). Renvoyant à un temps long (140 ans), excédant la vie d'un individu ; la corriger ne semblait pas controversé, d'où l'ironie de Wuille qui dit proposer « *un changement controversé : rendre l'offre monétaire de Bitcoin limitée* »<sup>377</sup>.

La faille Bitcoin CVE 2018 est la troisième occurrence d'une crise de ce type, et sa singularité tient à ce que le risque de production d'UCN\* surnuméraires résidait, nous l'avons vu, dans les mécanismes entourant la double dépense et non ceux entourant les récompenses, comme les crises précédentes. Précisément, l'itération de « faux monnayage » concerne les versions « Bitcoin Core »

<sup>374</sup> N'étant pas technicien, nous sommes d'abord passé à côté de cette ironie, d'où l'épisode, déjà rappelé en note dans l'introduction générale, d'un *bitcoiner*\* français contestant l'existence de ce bogue, affirmant que nous étions tombé dans un poisson d'avril (voir <https://twitter.com/daboloskov/status/1246527105627635713?s=20> et suivant). Luke Dash Jr, P. Wuille et M. Corallo nous en ont confirmé la véracité.

<sup>375</sup>Voir [https://en.bitcoin.it/wiki/BIP\\_0042](https://en.bitcoin.it/wiki/BIP_0042) [consultation au 03/11/2021].

<sup>376</sup> Voir <https://twitter.com/pwuille/status/1246564993400635395?s=20> [consultation au 03/11/2021], cette « illégalité » fait référence aux normes d'usage du langage de programmation\* C++, comme m'en a informé Anon n°4 [Entretien n°10].

<sup>377</sup> Voir [https://en.bitcoin.it/wiki/BIP\\_0042](https://en.bitcoin.it/wiki/BIP_0042) [consultation au 03/11/2021].

0.15 à 0.16.2 qui considèrent valide un enregistrement, pourtant « invalide » du point de vue des clients non vulnérables (cf. cas D, Tableau 2). Cette transgression des règles contourne le monnayage et ses mécanismes d'émission, les UCN\* doubles dépensées sont doublement comptabilisées, créant « *des BTC à partir de rien* » (Song 2018).

En pratique, en plus d'une augmentation discrétionnaire/arbitraire de la masse monétaire de bitcoin, l'activation de ce bogue aurait entraîné un autre risque important pour toute CM : une « scission de chaîne » (un « *chain split* »).

### Crise de « scission de chaîne » : l'unicité des paiements mise en péril

Comme les bogues de faux monnayage, les « scissions de chaîne » (ou « *chain split* ») sont rares (4 recensées, crises n°7, 11, 19 et 26, en marron) et, comme eux, leurs conséquences sont critiques. Elles peuvent en effet causer un effondrement de la confiance éthique, hiérarchique, mais aussi méthodique. Alors que la situation normale est celle d'une unicité du réseau\* et du registre, ces crises impliquent que le protocole et le réseau\* se scindent en deux ou plusieurs versions concurrentes, sans que le consensus par PoW\* de Nakamoto soit capable de faire converger les nœuds\* sur un historique unique. L'établissement de frontière nette entre le normal et l'anormal n'est jamais donnée en soi et évolue au gré des interprétations : souvenons-nous que la cohabitation à un instant t de deux historiques n'est pas pathologique en soi. En temps « normal », en cas d'occurrence de deux enregistrements candidats valides, la règle stipulant aux nœuds\* de converger vers la chaîne la plus longue permet une réconciliation rapide de l'ensemble du réseau\* sur un même registre\* canonique, par réorganisation de chaîne (cf. Chap. I) : le consensus par PoW\* ne peut fixer techniquement une norme de finalité des transactions\*, celle en vigueur, établie à 6 cycles de mise à jour du registre\* (*dit confirmation\**) est une convention de pratique<sup>378</sup>.

En cas de « scission de chaîne », le consensus de Nakamoto échoue, car une incompatibilité logicielle empêche la réconciliation entre des nœuds\* aux règles divergentes : le réseau\* de paiement s'est séparé en deux mondes clos. Ces situations renvoient originellement à des situations d'indomptabilité involontaire<sup>379</sup>. Pour qu'une scission de chaîne advienne, il suffit qu'un « *bug [...] dans une nouvelle version du logiciel fasse qu'une transaction\* est considérée comme valide* [là où l'ensemble des autres] *la rejette comme non valide.* [...] *Seul le sous-ensemble des participants qui ont mis à jour leur logiciel [l']acceptera [et] comme les transactions\* et les blocs sont enchaînés, les deux sous-ensembles seront en désaccord sur chaque transaction\* qui suivra. Sans une action rapide des développeurs\* et une campagne [off chain\*] visant à aligner tous les participants d'un côté ou de l'autre de la scission, les deux camps [...] ne pourront plus jamais se mettre d'accord [,] la monnaie [est] divisée en deux monnaies incompatibles* » (Fields 2018). Dans une telle situation, le « *timing joue un rôle crucial* ». La difficulté de résolution dépendra de la gravité de la situation et de son évaluation : « *si la chaîne est divisée de telle sorte que 99% des participants sont d'un côté et seulement 1% de l'autre, se ranger du côté de la majorité est la solution évidente. Cependant, si environ 50% des participants sont passés à la nouvelle version, il n'y a pas de choix facile.* » (Ibid.)

---

<sup>378</sup> Rappelons que les « *attaques 51%* », visant à créer des doubles dépenses, correspondent à une situation où un acteur en capacité de produire des enregistrements rapidement détourne à son profit cette dimension transitoire et sa définition conventionnelle, produisant en privé une chaîne d'enregistrement concurrente, qu'il publiera en temps voulu afin que l'ensemble du réseau converge vers son historique et annule les transactions qu'il a inscrites dans la chaîne ainsi rendue orpheline (cf. Annexe n°V.5).

<sup>379</sup> L'intentionnalité dessine le cas particulier des « *Hard Forks contentieux* » où un groupe monétaire différencie ces codes pour s'autonomiser de sa communauté de paiement d'origine (cf. « *Scaling Debate* », Chap. II section II.3.3 et section II.3.3, suivante).

Si ces solutions apparaissent évidentes pour les 99% il n'en est sûrement pas de même pour ceux qui font partie du 1%.

Avec une coordination technique mise en défaut, le consensus *par* le protocole n'implique aucun retour à la normale, et la seule remise en ordre possible relève d'une coordination sociale, une action coopérative et « *off chain*\* » entre les opérateurs de noeuds\* (mineurs et complets). Ce type de coordination suppose des négociations entre opérateurs, car cette convergence forcée a des enjeux économiques importants pour les participants à la chaîne minoritaire rendue orpheline : les transactions\* qui y sont consignées - les échanges économiques des usagers et les subsides des mineurs – n'ont plus d'existence une fois la réconciliation advenue, ce qui n'est pas le cas des contreparties de ces transactions\* engagées dans les échanges. Les crises historiques qui ont impliqué des « scissions de chaîne » ont bien conduit à l'*« action rapide des développeurs\* et [à des] campagnes visant à aligner tous les participants »* (Fields 2018) sur la même branche. La gravité de ce type d'événements est réelle ; ils dégradent l'expérience des usagers et peuvent conduire à des pertes pécuniaires : durant ces crises, avoir accepté des transactions\* revient à encourir le risque de doubles dépenses, avec de mêmes UTXO\* dépensées dans chacune des branches concurrentes (cas de la crise n° 19 de 2013) et des annulations de paiements confirmés (lorsque la scission se termine et que tous les noeuds\* convergent sur un même historique, rendant orphelin l'historique concurrent). D'où la création d'outils d'observation et d'analyse, un site comme « Fork\*Monitor.info » mis à disposition par « BitMEX research » monitorant en temps réel l'occurrence de deux enregistrements candidats valides comme la présence ou non de tentative de double dépense, ou d'augmentation de frais de transaction\*. La gravité de ces crises s'apprécie finalement aussi par les voies correctives utilisées, et les remises en ordre passent souvent par des BIP (BIP 30, 0034 et 50).

Le « Bug Value Overflow » (crise n° 4, CVE 2010 5139) est un cas de « scission de chaîne ». L'apparition de l'enregistrement à émission surnuméraire a produit une séparation du réseau\* entre les noeuds\* acceptant cet historique et ceux le refusant. La scission fut longue de 51 blocs, avant que la « chaîne légitime », au sens des attendus sociaux, réclame sa victoire en termes de PoW\*, grâce au travail de remise en ordre coordonné de Nakamoto, Andresen et Garzik, (Redman 2021). La crise n° 19 (CVE 2013 #3220), déclenchée en mars 2013, illustre tant la gravité des problèmes posés que la coordination nécessaire (c'est l'une des controverses analysées par Musiani, Mallard et Méadel 2018, p. 138 à 142) : « *les 11 et 12 mars 2013, un mineur exécutant la version 0.8 [...] a créé un gros bloc invalide [conduisant à] une scission ou une "bifurcation" involontaire dans la blockchain Bitcoin, puisque les ordinateurs équipés de la version la plus récente du logiciel à l'époque (0.8) ont accepté le bloc invalide et ont continué à construire sur la chaîne divergente, tandis que les anciennes versions du logiciel l'ont rejeté et ont continué à étendre la blockchain ancienne/originale sans le bloc incriminé. Cette scission a entraîné la formation de deux journaux de transactions\* distincts sans consensus clair ni même connaissance de l'existence de l'autre événement, ce qui a permis aux mêmes fonds d'être dépensés deux fois sur chaque chaîne - l'acte même de double dépense dont l'évitement était censé être la principale amélioration du bitcoin par rapport aux monnaies numériques précédentes* » (*Ibid.*). Cette crise, plus courte, avec seulement 21 blocs rendus orphelins (Bitmex Research 2017a; Redman 2021), fut malgré tout plus controversée que la précédente. Sa résolution a reposé sur une coopération active entre les développeurs\* et les pools de minage, qui permit la remise en ordre en alignant « *tous les participants d'un côté ou de l'autre de la scission* » (Fields 2018) et ce, en dehors du consensus de Nakamoto : une pool de minage importante est revenue à la version logicielle antérieure afin de suivre l'historique défini socialement comme canonique.

Pour le bogue Bitcoin CVE 2018 que nous étudions, seule l'absence d'exploitation effective justifie que l'étiquette de « scission de chaîne » ne lui ait pas été assignée. Un bloc contenant une transaction\* réalisant une double dépense eut été accepté par des nœuds\* et rejeté par d'autres, nous aurions été dans le cas extrême décrit par Fields (2018). Les versions 0.15.0 à 0.16.2 acceptant l'enregistrement « pathologique » comme canonique auraient étendu la chaîne d'enregistrement à partir du bloc avalisant la double dépense et les « nouvelles » règles transactionnelles et de monnayage, là où les nœuds\* tournant sur des versions non vulnérables l'auraient rendu « orphelin », continuant à travailler sur un registre\* au sein duquel les transactions\* sont valides du point de vue des « anciennes » règles. L'exploitation de cette vulnérabilité sur le réseau\* testnet de Bitcoin quelque mois après, profitant du fait que « certains mineurs étaient encore vulnérables » le prouve (Straw Hat 2019) : « *boom, le réseau\* s'est divisé* » [...] « *pendant des heures* » avant qu'un acteur active « *une puissance de hachage importante* [...] afin de reconstituer quelques centaines de blocs et de réorganiser la chaîne honnête » (Straw Hat 2019). Reste que, dans le cas de la crise Bitcoin CVE 2018, la gravité théorique de ce bogue est nuancée par ses conditions pratiques. Song (2018) et Straw Hat (2019) soulignent qu'exploiter cette vulnérabilité n'est offert qu'au producteur d'enregistrement. Cela implique des coûts (directs et d'opportunités) importants, pour ne pas dire rédhibitoires (aux dépenses afférentes à la découverte d'un hash\* valide s'ajoute la perte de 12,5 BTC de récompense, Song 2018). Au capital économique nécessaire s'ajoute un capital culturel de haut niveau (savoir et savoir-faire dans la programmation de Bitcoin)<sup>380</sup>. Finalement, à l'époque, si près de 82,5% du réseau\* était vulnérable au bogue CVE 2018 #17144 (4,3% à l'itération DOS et 78,3% pour celle de « faux monnayage », Tableau 3 ci-dessus), près de 17,5% des nœuds\* du réseau\* n'étaient pas concernés par cette vulnérabilité. En cas de « *bifurcation de chaîne* », « *le consensus social [...] concernant la bonne chaîne aurait commencé à être discuté et la chaîne créant une inflation inattendue aurait probablement perdu. S'il y avait eu un blocage, il y aurait probablement eu un retour en arrière volontaire pour punir l'attaquant.* » (Song 2018) Difficile, en l'absence d'exploitation effective, de savoir la tournure qu'aurait prise cette crise en cas de « scission de chaîne » (Song 2018), d'où l'intérêt de l'expérience de Straw Hat (2019) sur le testnet Bitcoin.

### **Crise de « DOS » : dégradation de l'accessibilité au réseau et de la praticité des paiements**

Les vulnérabilités de déni de service (DOS) sont les plus fréquentes (13 décomptées ; crises n° 2, 3, 5, 10, 12, 13, 14, 15, 17, 21, 23, 27 et 34 ; en bleu) mais moins critiques, en ce qu'elles n'impliquent qu'une érosion de la confiance méthodique : seule la praticité des paiements est remise en cause, du fait de la congestion du réseau\*. S'en prémunir est nécessaire afin que le réseau\* soit accessible et disponible à tous, et les problématiques entourant leur régulation sont au cœur du design des protocoles de registre\* distribué. En outre, toute « attaque » DOS n'est pas due à la présence d'un bogue « à proprement parler » (cf. les cas recensés dans notre chronologie). La dimension normative et politique supportant la normalisation des frontières du phénomène ressort ici. Bitcoin a été la cible de nombreuses « tempêtes » de spam (Lopp 2021 en a décompté 14, étaillées entre 2011 et 2021). Celles-ci ont contribué à faire évoluer les régulations protocolaires encadrant des « *transactions\* de spam* » qui « *d'un certain point de vue [...] n'existent pas - si elles sont valides et qu'elles paient les frais appropriés, elles doivent être confirmées* » (Lopp 2021; la taille

---

<sup>380</sup> L'utilisateur moyen est exclu, car créer cette transaction exige de tout faire manuellement, en lignes de commande via un client mineur. Utiliser un client de portefeuille\* est impossible, car il l'empêcherait par défaut. Si certains considèrent qu'un bon *bitcoiner/coiner\** ne peut « *comprendre Bitcoin* » que s'il a « *construit une transaction [...] avec [se]s mains [...] avec du code* » [P. Noizat, Entretien n°24], notre expérience démontre que ces compétences sont rares chez les *bitcoiners\**, et l'expérience de *Straw Hat (2019)* confirme le haut degré de spécialisation et d'expérience nécessaire.

des blocs à 1 Mo, le mécanisme des frais de transaction\* et des frais relais, cf. Chap. I, section I.2.1). À leur fréquence renvoient des effets relativement peu critiques, puisqu'une crise de DOS n'est que transitoire et partielle, ne touchant que certains acteurs.

Tout d'abord, « *si le nœud\* Bitcoin de quelqu'un se déconnecte [...] dans la plupart des cas, vous ne perdez pas d'argent [simplement,] vous ne pouvez pas accepter un paiement, c'est nul pour votre entreprise mais au moins vous n'avez pas perdu d'argent.* » [M. Corallo, Entretien n°15] Ensuite, pour les DOS de « *tempêtes de spam* », bien qu'incommodes, elles se régulent par le mécanisme même qu'elles attaquent, celui des frais de transaction\* : « *remplir la "mempool" avec un grand nombre de transactions\* crée une plus grande compétition pour l'espace des blocs, ce qui augmente les frais requis pour une confirmation\* plus rapide.* » (Lopp 2021) Ces situations de crise impliquent des problèmes de synchronisation des nœuds\* et de latence, perturbant la disponibilité\* et la vivacité du réseau\* P2P pour certains acteurs seulement<sup>381</sup>. Comme l'illustre l'itération « *DOS* » de la faille Bitcoin CVE 2018 concernant les versions 0.14 à 0.14.3 (non incluse) des implémentations « *Bitcoin Core* » (Bitcoin Core 2018 ; Song 2018 ; Awemany 2018) qui permettait d'« *appeler le nœud\* à planter, si* » un mineur diffusait un enregistrement pathologique pour faire planter les pairs qui le réceptionneraient : appliquant leur règle canonique de validité des enregistrements, le bloc ne serait pas accepté et le nœud\* planterait/s'arrêterait. La distribution du réseau\* se fait garante d'un accès minimum, des nœuds\* non vulnérables continueront le traitement et la maintenance du registre\* en l'absence des autres. Reste une expérience usagers qui se dégrade, c'est plus cher et la finalité du paiement est incertaine<sup>382</sup> [A. Le Calvez, Entretien n° 20].

## D'autres types de crises passées et encore à découvrir

D'autres types de vulnérabilités peuvent exister et leur gravité (et leurs conséquences en termes de confiance) s'apprécie à leur caractéristique idiosyncratique. Les vulnérabilités de type « *Theft* » sont rares (au nombre de 4 ; crises n° 1, 22, 36 et 39), mais critiques, renvoyant à des situations où un attaquant peut prendre le contrôle d'UTXO\* en dehors des règles consensuelles canoniques (cf. avoir la bonne signature). Heureusement pour la sécurité de Bitcoin – et plus particulièrement pour la perception qu'en ont les utilisateurs –, de telles failles n'ont jamais donné lieu à exploitation effective. Comme pour la codification du monnayage, il est intéressant de noter que, à l'origine, Bitcoin « *contenait deux bogues totalement fatals qui rendaient le système entier sans valeur [,] heureusement, ils ont été découverts et corrigés avant qu['il] n'ait une valeur sérieuse* » : le premier, de type « *Theft* », permettait à « *n'importe qui [d'] écrire un scriptSig qui s'évaluait toujours à true et [ainsi, de] réclamer les pièces de n'importe qui d'autre [, et fut] corrigé dans la v0.3.2* » (Hearn 2013 ; Apodaca 2015). Les autres cas recensés reposaient sur des pratiques

---

<sup>381</sup> À l'extrême, une attaque par DOS peut être utilisée pour réaliser une « attaque par éclipse » en direction d'un opérateur de nœuds\* cible. Cela peut permettre à un attaquant de faire planter les pairs de sa cible afin de « *monopoliser l'ensemble des connexions entrantes et sortantes de la victime, isolant ainsi cette dernière du reste de ses pairs dans le réseau* » (Goldberg 2015). Ce type d'attaque, outre le fait qu'il perturbe le réseau ou qu'il permet de filtrer les informations entrantes et sortantes de la victime, ouvre aussi à des attaques plus complexes : « course aux blocs » ; « fractionnement de la puissance de minage », « minage égoïste » ou encore « double dépense sans confirmation\* », voir (*Ibid.*; Saad et al. 2019).

<sup>382</sup> L'étude de l'épisode de juillet 2015 montre que « *cette attaque a eu un impact négatif sur les transactions non spam, augmentant les frais moyens de 51% (de 45 à 68 satoshis/octet) et le délai de traitement de 7 fois (de 0,33 à 2,67 heures). Cela a montré qu'un adversaire qui est prêt à dépenser des montants modestes en bitcoins (au moins 49 000 USD) peut avoir des effets sur le reste des utilisateurs du réseau.* » (Lopp 2021)

non conseillées (partage physique ou à distance<sup>383</sup> d'un ordinateur entre plusieurs utilisateurs) et ces vulnérabilités ont été « *considérée[s] comme un risque faible* » (Dashjr 2019). Celles étiquetées « *Exposure* », comme les précédentes, sont peu communes (au nombre de 4 ; crises n° 6, 16, 18 et 30) et n'ont pas donné lieu à exploitation. Elles renvoient à la possibilité pour un « *attaquant* » d'accéder à des données utilisateurs « sensibles » (clef privée stockée en clair<sup>384</sup>) et remettent en cause les propriétés attendues de la sécurisation de ses avoirs numériques. Les « *Fake conf* » (au nombre de 6 ; crises n° 9, 20, 28, 29, 32 et 33) correspondent aux situations où un « *attaquant* » peut potentiellement réaliser, en direction d'un acteur cible, une double dépense avec une confirmation seulement<sup>385</sup>. Bien que difficilement réalisables, des exploitations effectives ont été constatées<sup>386</sup>. Si l'expérience utilisateur est dégradée, particulièrement pour le receveur floué, le protocole n'est pas en cause. La convention du nombre de confirmations attendues pour considérer le paiement finalisé l'est. Les vulnérabilités étiquetées « *Deception* » voient un « *attaquant* » avoir le pouvoir de propager des informations erronées au sein du réseau\* - une seulement a été décomptée, la crise n° 38 et ses conséquences potentielles étaient peu critiques : cette vulnérabilité permettait d'injecter à distance des données arbitraires dans le journal de débogage de la cible<sup>387</sup>. Enfin, le label « *Unknown* » est une catégorie valise où sont regroupées des vulnérabilités dont l'*« étendue des abus possibles est inconnue »*<sup>388</sup> (nous en avons décompté 5 ; les crises n° 8, 25, 31, 37 et 38). Au sein de cette catégorie, l'évaluation de la gravité et des conditions effectives d'exploitation nécessite de s'intéresser à chacune des vulnérabilités concernées<sup>389</sup>, soulignant l'existence d'incertitudes et de risques émergents comme d'une normalisation encore partielle<sup>390</sup>.

Ce qui précède montre que le concept de crise est une « *catégorie indigène autant qu'un concept analytique* » : les matériaux disponibles pléthoriques, sur la crise Bitcoin CVE 2018 et les

<sup>383</sup> Voir respectivement, <https://medium.com/@lukedashjr/cve-2018-20587-advisory-and-full-disclosure-a3105551e78b> pour la crise n° 36 ; [https://en.bitcoin.it/wiki/Common\\_Vulnerabilities\\_and\\_Exposures#CVE-2010-5141](https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures#CVE-2010-5141) pour la crise n° 1 ; et <https://github.com/bitcoin/bitcoin/issues/2838> pour la crises n° 22 [consultation au 08/11/2021].

<sup>384</sup> Voir <https://bitcointalk.org/index.php?topic=51604.0> pour la crise n° 6, ou <https://github.com/bitcoinknots/bitcoin/blob/v0.13.1.knots20161027/doc/release-notes.md> pour la crise n° 30 [consultation au 03/11/2021].

<sup>385</sup> Andresen explique cette attaque dans l'exposé des motifs du BIP 0016 relatif à la crise n° 9 : « *L'attaquant crée une transaction pay-to-script-hash qui est valide selon l'ancien logiciel, mais invalide pour la nouvelle implémentation, et s'envoie quelques pièces en l'utilisant. L'attaquant crée également une transaction standard qui dépense la transaction pay-to-script, et paie la victime qui utilise l'ancien logiciel. L'attaquant mine un bloc qui contient les deux transactions. Si la victime accepte le paiement à confirmation\* unique, l'attaquant gagne, car les deux transactions seront invalidées lorsque le reste du réseau écrasera le bloc invalide de l'attaquant. L'attaque est coûteuse, car elle nécessite que l'attaquant crée un bloc dont il sait qu'il sera invalidé par le reste du réseau.* » (voir [https://en.bitcoin.it/wiki/BIP\\_0016](https://en.bitcoin.it/wiki/BIP_0016) [consultation au 03/11/2021]).

<sup>386</sup> Comme l'explique Andresen dans le BIP 0050, « *pendant ce temps, il y a eu au moins une grande double dépense* » réussie de près de 10 000€ de l'époque, ciblant la bourse d'échange OKPAY, voir <https://bitcointalk.org/index.php?topic=152348.0> [consultation au 15/11/2021].

<sup>387</sup> Voir <https://nvd.nist.gov/vuln/detail/CVE-2018-20586> [consultation au 15/11/2021].

<sup>388</sup> Voir [https://en.bitcoin.it/wiki/Common\\_Vulnerabilities\\_and\\_Exposures](https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures) [consultation au 15/11/2021].

<sup>389</sup> Lors de la crise n° 8, Matt Corallo a trouvé un bogue rare et « *difficile à reproduire concernant le plantage de Bitcoin-QT* », qui laisse beaucoup d'interrogations : « *Est-il exploitable ? Un attaquant pourrait-il créer des messages de protocole bitcoin qui déclenchaient le bogue et compromettaient les ordinateurs Windows ? A-t-il déjà été exploité ?* » Les « Core Devs » d'avouer : « *Nous n'en savons rien* », même si « *nous pensons qu'il serait extrêmement difficile de créer un exploit utilisable* » (voir <https://gavintech.blogspot.com/2012/03/full-disclosure-bitcoin-qt-on-windows.html> [consultation au 15/11/2021]).

<sup>390</sup> Ce qui transparaît dans ce mail : « *Quelqu'un garde-t-il une trace des bogues et des correctifs liés à la sécurité, [...] dans l'affirmative, cette liste peut-elle être partagée [...] ?* » Car « *aucun nouveau CVE n'a été publié depuis près de trois ans, [et] aucune information ne semble avoir été rendue publique. [...] Il serait très avantageux pour les utilisateurs finaux que la communauté des clients et des altcoins\* dérivés de Bitcoin Core puisse être protégée contre les risques de fraude.* » (Liu 2017)

autres, permettent d’interroger les conditions présidant à ce que des événements soit *fabriqués comme crises et gouvernés* comme tels (Aguiton, Cabane et Cornilleau 2019, p. 11-12). Nous allons l’ expliciter par la suite.

### III.2 DES MARQUES D’UNE POLITIQUE DE CRISES : UNE GOUVERNANCE DE HUIS CLOS ROUTINIÈRE

Bitcoin est vendu par certains comme un objet autonome et autorégulatoire, arguant du fait que ses codes protocolaires contiennent l’ensemble des règles et incitations nécessaires à son fonctionnement pérenne et soutenable. Pourtant, les codes Bitcoin, constituant sa gouvernance *par le protocole*, sont faillibles et dès qu’ils sont reconnus comme ne correspondant pas aux attentes de la communauté des usagers, ils entrent en crise. Dans cette situation où la gouvernance *par le protocole* est mise en défaut, il ne faut pas attendre d’elle qu’elle se remette en ordre. Cette situation nécessite une gouvernance *sur le protocole*, renvoyant à des activités humaines, médiatisées des dispositifs socio-techniques en dehors de la chaîne\* : la gouvernance du répertoire logiciel Bitcoin Core qui, si elle n’épuise pas la gouvernance *sur l’infrastructure* de Bitcoin, y tient une place centrale. L’administration des codes s’inscrit pour bonne part dans des pratiques anciennes, initiées pour le développement des logiciels libres/ouverts, et suppose un enchevêtrement de relations interpersonnelles plus ou moins formelles, entre des volontaires souvent bénévoles (De Filippi et Loveluck 2016, p. 9). Ce constat d’humidité de codes moins « secs » contredit l’antienne de l’immutabilité de Bitcoin des *coiners*\*. L’histoire des crises montre que les codes sont modifiés continuellement, de manière incrémentale, mais aussi radicale. Cela soulève des questions. Qui, comment et pourquoi des acteurs non humains sont pointés comme défaillants ? Que recouvrent matériellement les codes protocolaires de Bitcoin ? Où, comment et par qui ce code peut-il être modifié ?

Chercher la matérialité des codes, c’est découvrir leurs dispositifs de production et de maintenance collaborative, et les acteurs qui en ont la charge. Dans notre cas d’étude et en l’absence d’activation de la faille, c’est la gouvernance *sur le protocole* qui fut prépondérante et qu’il nous faut éclairer. Ce terrain offre l’occasion d’aller au-delà des analyses réductrices, insistant sur les seuls acteurs non humains présents *on chain*\* – les nœuds\* mineurs et complets – et leurs relations protocolaires automatiques et mécaniques. Il permet d’opérer un décentrement vers la dimension *off chain* et de mettre en exergue les acteurs, institutions, normes et conventions, les dispositifs et les arènes de débats prenant part activement à la résolution de cette crise, comme plus généralement à la maintenance et à l’évolution des codes sources Bitcoin. Il permet de décrire et d’analyser plus avant les statuts, rôles et fonctions de chacun, comme les modalités de leurs articulations pratiques : d’une part, comment les acteurs non humains sont autant des ressources mobilisées par les acteurs humains que des contraintes pesant sur leurs actions ; d’autre part, comment les interactions entre acteurs humains dépendent, pour bonne part et en plus de leurs fonctions relatives au sein du protocole, de leur insertion dans des réseaux\* sociaux qui leur sont propres. La présentation que nous avons faite du bogue Bitcoin CVE 2018 et de sa résolution a fait apparaître une grande hétérogénéité d’acteurs non humains, « *on chain*\* » (les implémentations et versions logicielles variées structurant réseaux\* et protocole), mais aussi et surtout « *off chain*\* », avec une grande multiplicité de dispositifs socio-techniques mobilisés. Nous avons aussi montré que des acteurs humains, peu nombreux et au statut particulier, ont pris part tant à la mise en crise qu’à la remise en ordre. Ce point souligne l’existence de sous-groupes (comme les développeurs\*) structurant la communauté et de modalités d’interrelations particulières.

Il existe donc bien une gouvernance pour Bitcoin. L'analyse systématique des crises en offre une image incarnée, à rebours des analyses réifiantes que nous critiquons. Comme protocole, Bitcoin est régulé idéellement et matériellement : un cadre normatif l'enserre, composé des attendus des *bitcoiners*\* et dessinant l'*« état du monde considéré comme "normal" à partir [duquel] "est construit et alimenté»* un autre état du monde considéré comme critique (Aguiton, Cabane et Cornilleau 2019, p. 11). Concrètement, ces normalisations supposent que Bitcoin porte au sein de sa communauté un/des groupe(s) de normalisateur(s), dont l'activité repose sur des outils et dispositifs de diagnostic, de contention et de remédiation. Cette fabrique des crises et de leur gouvernance, faite d'interactions hétérogènes reposant sur un ensemble composite d'espaces, d'interlocuteurs, de dispositifs techniques, nous allons l'expliciter.

### III.2.1 Des acteurs au cœur de la gouvernance sur le protocole

Si un acteur non humain aussi essentiel qu'un client Bitcoin et ses codes fait défaut et entre en crise, c'est la gouvernance *par* le protocole qui est remise en cause. L'état de crise révèle ce que les acteurs considèrent comme « *normal* » et ce qui ne l'est pas (Aguiton, Cabane et Cornilleau 2019) : est reconnu, plus ou moins brutalement, un hiatus entre les actions prescrites par la conception (et les concepteurs) et les actions effectivement réalisées (Akrich, 2010). Ce hiatus interroge les dichotomies opposant la routine au dysfonctionnement, le bogue à l'attaque, le normal à l'exceptionnel, comme il éclaire les acteurs et dispositifs participant de leur établissement.

#### De l'âme des acteurs non humains : d'un « esprit du code » excédant sa « lettre »

Au titre de l'interrogation précédente, l'acception rigoriste du slogan « *code is law* » vide de tout fondement les concepts mêmes de failles, de vulnérabilités, de bogues, voire d'attaques. Du point de vue qui voudrait que la gouvernance d'une CM doit relever d'une « loi de Szabo » où le code informatique est souverain (Zamfir 2019, cf. Chap. II section II.3.3), la « déférence au code » (Hinkes 2021) et à l'*« autorité algorithmique »* (Lustig et Nardi 2015) est totale et sans limites : tous les résultats d'un code sont par définition normaux, indiscutables et légitimes. Cela signifie-t-il que près de 83% des nœuds\* vulnérables (Tableau 3 ci-dessus) et leurs utilisateurs avaient « *fondamentalement opté pour les règles de consensus de Bitcoin telles qu'elles existent* » [Corallo, Entretien n° 15] dans leurs codes de versions ? D'après Awemany (2018), critiquant au passage la centralité de Bitcoin Core, avec le Bogue Bitcoin CVE 2018 « *certaines choses ont complètement disparu [...] par exemple l'idée de Core selon laquelle "le code est la loi". Si le code est la loi, cela signifie-t-il que vous devez accepter l'inflation maintenant ? Ou est-ce en fait les développeurs\* de Core qui dirigent le navire ?* ». Non, la remise en cause du consensus sur la validité des transactions\* et le monnayage induit par ces codes n'est ni volontaire, ni souhaitée, seulement le résultat de l'incertitude radicale et de la rationalité limitée des acteurs inhérente à leurs activités. D'où le paradoxe. De nombreux *coiners*\* se revendiquent du camp de la règle radicalisée, notamment Satoshi : ce qui est écrit dans le code est/doit être indiscutable et immuable. Pourtant, les mêmes mobilisent une terminologie de crise – parlant de faille, d'attaque, de l'*« honnêteté »* attendue des nœuds\* (Nakamoto 2008) par exemple - qui ajoute à ces codes un supplément d'âme, une normativité sans laquelle ils n'ont sens. À la question de savoir pourquoi Song qualifie de « *pathologiques* » les transactions\* incriminées dans la faille CVE 2018 et s'il faut considérer le changement des versions vulnérables comme une mise à niveau des règles de consensus (cf. un *Fork*\*, cf. section III.3 suivante), Song de nous répondre : « *Hum, Code, Code, donc ça dépend, c'est une version multiple du code, et ça a affecté une gamme particulière de versions [qui] allait à l'encontre de ce qui était là avant donc, ils... ce ne serait pas... un Fork... c'est vraiment une correction d'un code qui est sorti du consensus... si ça a un sens [...] et le code est la loi dans le sens où, ce n'est pas seulement le code maintenant. C'est tout le code d'avant et pour le code d'avant* »

*cette transaction\* pathologique aurait été rejetée [...], ce n'est pas nécessairement que nous avons brisé le principe du "Code is Law" » [J. Song, Entretien n° 17]. Cela a un sens : ces codes et ses attendus d'« avant », bien que minoritaires dans la structuration du réseau\*, devaient primer sur le cadre formel devenu majoritaire.*

S'il faut prendre au sérieux le slogan « Code is Law », c'est dans le sens originel qu'il revêt chez Lessig (2000), et qu'aurait « *un petit peu mal interprété* » beaucoup de *bitcoiners\** [L. Thiébault, Entretien n° 21, rejoint par Roussel, Entretien n°11]. À revenir au texte de Lessig (2000), l'un des juristes en première ligne de la contre-offensive contre « *la privatisation croissante du patrimoine intellectuel et culturel de l'humanité* » (avec J.Litman, Y.Benkler, L.Lessig, J.Boyle ; Coriat et Broca 2015, p. 273, cf. Chap. I, section I.1.1), il semble que les *coiners\** lui donnent un sens opposé. Sa formule « Code is Law » mettait en garde contre l'idée que le *gouvernement* est le seul danger pour les libertés. Contrairement à l'interprétation qui prévaut chez les *coiners\**, Lessig affirmait que la technique dissimule des « *régulations* », que le cyberspace a « *son propre régulateur* » et qu'ils sont tout aussi menaçants : « *le code[,] le logiciel et le matériel qui font du cyberspace ce qu'il est* » définissent qui peut avoir « *un impact sur qui* », « *voire quoi, ou sur ce qui est surveillé* » et, plus généralement, « *la manière dont nous vivons le cyberspace* » (Lessig 2000). Code et développeurs\*, architecture et architectes, s'imposaient comme un cadre para-légal produit par de nouveaux législateurs. Ce slogan impose une mise en parallèle du code et de la loi, non l'hypothétique substitution de l'une, défaillante et arbitraire car « *humide* », par de la technique efficace et neutre car codée « *en sec* », substitution que suppose N. Szabo (2008b). Quoiqu'en dise cette figure de l'interprétation rigoriste du « *Code is Law* », si le droit est conflictuel du fait de sa dimension interprétative, il en est de même pour le « *code informatique et [les] fichiers lisibles par ordinateur (dans la mesure où : [si en temps normal] un ordinateur les traite de manière cohérente)* » (Szabo 2008b), en temps de crise justement, il les traite de manière non cohérente . Sa distinction entre les normes légales et réglementaires, considérées comme du « *code humide* » « *interprété par le cerveau* » et celles informatiques, relevant de « *code sec* » interprété « *par les ordinateurs* » ne tient pas. La dimension interprétative inhérente au droit l'est aussi pour les codes : la distinction clef en philosophie du droit, opposant les concepts de « *lettre de la loi* » à celui de « *son esprit* », reste utile. L'application d'une loi suppose une activité interprétative du juge, mêlant la lettre de la loi (les textes législatifs et l'interprétation littérale qu'ils permettent) et l'esprit de la loi, censé saisir les intentions sous-jacentes d'un texte législatif. Lorsque les textes sont flous ou mal taillés pour couvrir explicitement certaines situations, l'esprit de la loi peut être mobilisé afin de combler ce vide juridique formel. De même, les règles protocolaires canoniques de Bitcoin vont au-delà de leur syntaxe et de leur sémantique (la lettre des codes), englobant les intentions des développeurs\*, les débats communautaires et leurs compromis, qui se traduiront dans l'inclusion/exclusion de nouvelles fonctionnalités, la publication de nouvelle version, voire de *Fork*\*. Les promoteurs de la « *loi de Szabo* » confondent le légal et le légitiment, suivant une acceptation rabattant l'esprit du code sur sa seule lettre : aucun dysfonctionnement, seulement des fonctionnements. Néanmoins, ces représentations idéales (et stéréotypiques) n'épuisent pas l'éventail des vues présentes dans la communauté sur ce qu'est une bonne gouvernance de CM. Dans le sens de la conception idéal-typique opposée (cf. la « *loi crypto* » ou « *crypto law* » de Zamfir concernant la gouvernance d'une CM 2019, Chap. II section II.3.3), des *coiners\** accordent une importance centrale à la lettre du code, dont ils soulignent en creux les processus qui en supportent mise en forme et expression. Pour A. Roussel (juriste lui aussi), l'esprit du code prime : [Nous] « *Tu viens du milieu juridique, tu distingues la lettre de la loi de l'esprit de la loi ?* » [Lui] « *Oui, voilà exactement. Et beaucoup de gens qui ont la position très stricte dans "Code is law", ils n'ont pas cette notion [,] le code a quand même été fait par des gens, et [...] le contrat social qui se cristallise dans le code peut évoluer avec le temps [induisant] un décrochage entre le code et le contrat social,*

*ce qui fait qu'à un moment donné [...] on abolit le code [, ] le contrat social [est] plus fort que le code, de toute façon.* » (Entretien n° 11).

Paradoxalement, les *coiners*\* les plus rigoristes, qui rejettent l'idée qu'une CM dispose d'une gouvernance autre que ses codes, par le jargon et les catégories qu'ils mobilisent, peuvent en mettre en cause la légitimité de certains résultats. Tout en l'invisibilisant, ils mobilisent eux aussi une normativité supposant un « contrat social » et des dispositifs variés, sans lesquels aucun décalage problématique entre le produit désiré d'un code (son « esprit ») et le résultat de sa « lettre » ne peut être reconnu. Ce hiatus et sa reconnaissance renvoient à un processus de normalisation à partir duquel les *coiners*\* dessinent différents types de crises/modifications de règles protocolaires consensuelles canoniques.

Quatre situations apparaissent possibles, suivant que coïncident ou non « les codes » logiciels protocolaires (« leur lettre ») et les attentes qu'en ont les membres de la communauté (leur « esprit »), comme représenté dans le Tableau 5 suivant.

**Tableau 5 : Les deux grandes familles de crises protocolaires**

|                                 | ...ce qui est attendu = considéré comme légitime par le consensus social  | ...ce qui n'est pas attendu = considéré comme illégitime par le consensus social  |
|---------------------------------|---|---|
| <b>Le code permet ...</b>       | <p style="text-align: center;"><b>[a] Situation normale</b></p> <p><u>Action : <i>Statu quo</i></u></p> <p><i>Ex. : contrôle de la double dépense, création monétaire qui suit l'échéancier prévu, etc.</i></p>   | <p style="text-align: center;"><b>[b] Crise « de vulnérabilité »</b></p> <p><u>Action : Correction d'un bogue (lettre du code) pour retrouver le caractère exécutoire des normes passées, toujours légitimes (esprit du code)</u></p> <p><i>Ex. : double dépense et régulation de la création monétaire suivant les règles et l'échéancier prévu (Cas CVE 20182).</i></p> |
| <b>Le code ne permet pas...</b> | <p style="text-align: center;"><b>[c] Crise « d'évolution »</b></p> <p><u>Action : Application de nouvelles règles protocolaires (lettre du code) pour sortir des normes passées, devenues illégitimes et s'adapter à l'évolution des attentes communautaires (esprit du code)</u></p> <p><i>Ex. : SegWit et le Scaling Debate; The DAO hack.</i></p> | <p style="text-align: center;"><b>[d] Situation normale</b></p> <p><u>Action : <i>Statu quo</i></u></p> <p><i>Ex. : rejet des doubles dépenses, invalidation de toute création monétaire qui ne suit pas les règles et l'échéancier prévu, etc.</i></p>   |

Source : Rolland Maël

Deux situations normales, en bleu, se dégagent : le cas [a] se caractérise par le fait que le code permet/produit des résultats considérés comme légitimes par le consensus social en vigueur dans la communauté de paiement (pouvoir réaliser/recevoir une transaction\* en temps voulu, par exemple). Le cas [d], à l'inverse, voit les codes interdire les actions et résultats considérés comme illégitimes du même point de vue (empêcher la réalisation d'une double dépense, par exemple). En contrepartie de cette normalité apparaissent deux cas « anormaux », où lettre et esprit des codes ne coïncident pas. Le cas [b] correspond à une situation caractérisée par le fait que les codes permettent des actions/résultats considérés comme manifestement illégitimes à consensus social inchangé (permettre la réalisation d'une double dépense, par exemple). La mise en crise, l'étape de déclenchement qui renvoie à la prise de conscience de l'existence d'une vulnérabilité, est brutale et située (que ce soit par exploitation publique ou par divulgation responsable privée). Nous la qualifions pour cela de « crise de vulnérabilités ». À l'inverse, le cas [c] renvoie à des situations plus latentes, où la lettre du code perd en légitimité chez certains, ce qui les conduit à vouloir l'amender : la légitimité des codes est remise en cause en ce qu'ils ne permettent pas – en l'état – des actions/résultats pourtant souhaités par les membres de la communauté. Cette crise est qualifiée de « crise d'évolution », la reconnaissance d'une transgression de la lettre des codes à leur esprit n'a rien d'évident et, contrairement au cas précédent, la mise en crise peut prendre du temps, voire ne jamais advenir. Cela passe par l'ouverture de négociations communautaires, supposant la construction préalable d'un problème public, par des acteurs et groupes plus ou moins minoritaires,

inaudibles et/ou invisibilisés. Ces acteurs devront convaincre les autres franges communautaires du bien-fondé de leurs modifications (cf. « Scaling Debate », Chap II. Section II.3.3).

Il existe différents types de crises dont nous construisons deux familles génériques : les « crises de vulnérabilité » et les « crises d'évolution ». Elles renvoient à un travail de normalisation, permettant de standardiser et classifier, au-delà des crises, les différents types de modifications de codes protocolaires et leur forme attendue. Ce travail suppose l'existence de lieux, cadres et dispositifs dédiés à la fabrication de ces codes, et, finalement, l'existence d'une chaîne de montage, articulant des ouvriers plus ou moins spécialisés. Intéressons-nous d'abord à l'objet de cette normalisation des crises, ces implémentations et versions de clients Bitcoin jugés défaillants.

### **La diversité des acteurs non humains en question : l'hégémonie de « Bitcoin Core » en crise ?**

Que la faille CVE 2018 soit multiforme, impliquant deux types de bogues selon les implémentations et les versions des clients Bitcoin concernées, illustre la dimension infrastructurelle et écosystémique de Bitcoin. En tant que protocole, Bitcoin (et toute CM) doit pouvoir être implanté suivant différents codes logiciels. Qu'il soit structuré matériellement par des logiciels hétérogènes (différences d'architecture, de langage de programmation\*, d'options), tant que ses clients sont compatibles entre eux et respectent les règles canoniques consensuelles, le réseau\* sera unitaire et cohérent. Dans le champ des CM et de leur protocole de registre\* distribué, deux types d'« *implémentations concurrentes* » sont à distinguer : les implémentations incrémentales simples qui « *ne modifient pas les règles de consensus et ne réimplémentent pas la base de code* » et les « *implémentations indépendantes* » qui, radicalement différencieront, sont « *réimplémentées sans utiliser le code de Bitcoin Core* », par exemple avec « *un nouveau langage de codage [...] afin d'essayer d'exploiter [c]es avantages* » (Bitmex Research 2018).

La crise que nous avons choisi d'étudier dévoile le travail de maintenance, quotidien et de longue haleine, qu'impose Bitcoin à certains membres de sa communauté, et pointe la centralité de « Bitcoin Core ». Les implémentations indépendantes ont toujours été très minoritaires dans la structuration du réseau\* et la majorité n'est que de type incrémental : peu différencieront, ces implémentations reposent sur « Bitcoin Core » qui tient lieu de « spécification protocolaire »<sup>391</sup>. Cette présence de l'implémentation Bitcoin Core s'explique par les choix et développements historiques qui, par un effet de sentier, ont conduit à privilégier une implémentation logicielle unique. Dès l'origine, Bitcoin se présente comme un logiciel dont les codes sources sont ouverts (sous licence MIT, cf. Chapitre I). Par ce choix, Nakamoto rend les codes sources du logiciel Bitcoin qu'il publie facilement auditables, copiables, modifiables, ouvrant à la production d'autres clients par d'autres équipes d'acteurs. Mais Nakamoto ne publia jamais à proprement parler de cahier des charges (« *specs* ») explicitant précisément son protocole. Il est peu probable de voir émerger un tel cahier des charges « *car personne n'a l'autorité pour en écrire* » (Lopp 2018) : « *les specs, c'est le code de Bitcoin Core, enfin, de manière implicite finalement. Parce que même pas le "White Paper" ben, il n'y a pas de "specs" du tout, il n'y a rien, il n'y a pas de détails. Du coup, c'est la première implémentation et les changements qui ont été faits après [...]* » qui tiennent ce rôle [A. Le Calvez, Entretien n°20]. La première implémentation du logiciel Bitcoin (Bitcoin v0.1) de

---

<sup>391</sup> « Bitcoin Knot », par exemple, développé dès décembre 2011 sous le nom de Bitcoin Next-Test par Luke jr, fut concernée par la faille CVE 2018. Cette implémentation dérive directement de la branche « master » de Bitcoin Core et implémente en avant-première les fonctionnalités qui y sont proposées à la fusion.

Nakamoto fut publiée sur la forge logicielle\* « sourceforge », le 8 janvier 2009 (Nakamoto 2009<sup>392</sup>). Elle prenait la forme d'un fichier « .rar », sans gestion de contrôle des sources, et les développeurs\* souhaitant échanger des correctifs avec Nakamoto devaient le faire par mail<sup>393</sup> (Lopp 2018). « Sirius-m »<sup>394</sup>, le second développeur\* Bitcoin après Nakamoto (bit2me Academy) créa le 30 octobre 2009 la première version du répertoire logiciel (ou « repo ») sur « sourceforge »<sup>395</sup> (*Ibid.*). Le logiciel de Nakamoto allait servir de base au développement de deux implémentations : « bitcoind »<sup>396</sup> et « BitcoinQt », qui seront fusionnées et renommées BitcoinQT à partir de la version 0.5.0, publiée fin 2011<sup>397</sup>. Dès lors, BitcoinQt tint lieu d'implémentation référente et, la même année, la gestion du projet fut migrée de la plateforme « sourceforge » à « Github » (Lopp 2018). Finalement, en 2014, elle est renommée Bitcoin Core (*Ibid.*) au prix d'une controverse<sup>398</sup>.

En effet, la position de monopole de Bitcoin Core et le statut subordonné des autres implémentations ne s'expliquent pas seulement par cette absence de spécifications. Elle est délibérée et organisée dès l'origine, l'unicité des règles et la stabilité du protocole en dépendraient : « *la nature du bitcoin est telle qu'une fois la version 0.1 publiée, la conception de base était gravée dans la pierre pour le reste de sa vie. [...] Je ne pense pas qu'une seconde implémentation compatible de Bitcoin soit une bonne idée. Une si grande partie de la conception dépend de l'obtention par tous les nœuds\* de résultats exactement identiques et synchronisés qu'une seconde implémentation serait une menace pour le réseau\** ». » (Nakamoto 2010e)<sup>399</sup> De plus, cela doit faciliter la maintenance car la « *version officielle* » implique déjà une charge de travail importante, en particulier suivant les contraintes de rétrocompatibilité que Nakamoto s'impose<sup>400</sup>. Dès cette origine, Bitcoin Core s'est donc imposé comme « *le point central de développement* ». Accumulant tous les talents et le travail accompli, son code serait « *le plus performant, le plus robuste et le plus sûr* », d'où le fait que les opérateurs de nœuds\* l'utilisent lui : « *il est un peu plus sûr [...] car vous avez plus de chances d'être compatible, bogue pour bogue, avec la majeure partie du reste du réseau\** » (*Ibid.*, comme confirmé par JF. Augusti, Entretien n° 18). Ainsi, l'existence d'implémentation incrémentale, comme « *forme de concurrence, qui ne modifie pas délibérément les règles de consensus et ne réimplémente pas le code, n'est pas du tout controversée* » (BitMEX 2018), contrairement aux implémentations indépendantes, un « *sujet très controversé et qui divise* » (Bitmex Research 2018) de longue date : visible lors du « Scaling Debate » (cf. Chap II section

<sup>392</sup> Voir le mail original ici : <https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html> [consultation au 11/10/2021].

<sup>393</sup> Les échanges entre Nakamoto et Finney sont consultables ici : <https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf> (Consultation au 11/10/2021)

<sup>394</sup> Marty Malmi de son vrai nom, que l'on a déjà rencontré dans le chapitre II pour le premier achat en BTC dans le monde réel avec la désormais fameuse Pizza (bit2me Academy).

<sup>395</sup> <https://sourceforge.net/p/bitcoin/code/1/> [consultation au 11/10/2021].

<sup>396</sup> Bitcoind est une implémentation logicielle qui met en œuvre le protocole Bitcoin pour l'utilisation de l'appel de procédure à distance (RPC). Elle correspond historiquement à la deuxième implémentation du client Bitcoin. Voir <https://en.bitcoin.it/wiki/Bitcoind> [consultation au 11/10/2021].

<sup>397</sup> <https://bitcoin.org/en/release/v0.5.0> [consultation au 11/10/2021].

<sup>398</sup> <https://github.com/bitcoin/bitcoin/pull/3408> [consultation au 11/10/2021].

<sup>399</sup> Discussion originale : <https://bitcointalk.org/index.php?topic=195.msg1611#msg1611> [consultation au 12/10/2021].

<sup>400</sup> Dans cet échange, il déclare : « *une deuxième version serait un énorme problème de développement et de maintenance pour moi. Il est déjà assez difficile de maintenir la compatibilité ascendante tout en mettant à niveau le réseau sans qu'une deuxième version ne vienne verrouiller les choses. Si la deuxième version se plantait, l'expérience de l'utilisateur se répercuterait négativement sur les deux, même si cela renforcerait au moins auprès des utilisateurs l'importance de rester avec la version officielle. Si quelqu'un se préparait à intégrer une seconde version, je devrais diffuser beaucoup d'avertissements sur les risques liés à l'utilisation d'une version minoritaire. C'est une conception où la version majoritaire l'emporte en cas de désaccord, et ça peut être assez moche pour la version minoritaire. Je préfère ne pas m'y attarder, et je n'ai pas à le faire tant qu'il n'y a qu'une seule version* » ; <https://bitcointalk.org/index.php?topic=195.msg1617#msg1617> [consultation au 12/10/2021].

II.3.3), cette division était apparue dès 2014, dans la controverse entourant le changement de nom en « Bitcoin Core »<sup>401</sup>. L'objectif du changement de nom était de « *supprimer la confusion entre le réseau\* Bitcoin et l'implémentation du client de référence que nous maintenons dans ce dépôt, tous deux nommés confusément "bitcoin"* » (Van der Laan)<sup>402</sup>. Mais certains développeurs\* reconnus (P. Todd, Luke Jr et G. Maxwell<sup>403</sup>) voyaient dans le qualificatif « Core » une dénomination vectrice d'une centralisation symbolique trompeuse<sup>404</sup>. Le problème était que cela « *implique que vous en ayez besoin....* » (Todd)<sup>405</sup>, laissant croire qu'elle est nécessaire à l'utilisation de Bitcoin, les autres clients étant « *traité[s] comme une sorte de client de "seconde classe"* » (Luke JR<sup>406</sup>) : ce « *terme "core" devrait être utilisé pour la partie critique du consensus, et non pour tout le code supplémentaire de portefeuille, de relais, etc. que l'implémentation de référence ajoute* » (Todd<sup>407</sup>). La critique de la domination exercée par Bitcoin Core sur le réseau\* n'est pas que sémantique. Contre Nakamoto et ses suiveurs, certains développeurs\* estiment que cette exclusivité représente une menace pour la sécurité de Bitcoin. C. Jeffrey, développeur\* de l'implémentation indépendante « Bcoin »<sup>408</sup>, fit polémique en 2017. Cherchant à alerter sur le risque systémique posé par ce qu'il considère comme une monopolisation du développement de Bitcoin, il révéla publiquement une faille de Bitcoin Core non encore patchée<sup>409</sup> (Jeffrey 2017; Apodaca 2017 ; Entretien n°21 ; Observation participante n° 15 Bitcoin 2017, Annexe n°III.2 et III.4). Comme la crise Bitcoin CVE 2018 l'illustre parfaitement, l'hétérogénéité des versions logicielles au sein de « Bitcoin Core » implique que « *chaque révision de Bitcoin Core introduit le risque d'un bug de consensus de rupture de chaîne, [soit] exactement la [situation] que les implémentations de noeuds\* alternatifs sont accusées de promouvoir* » (Apodaca 2017). Sans réellement gagner en sécurité du côté de la compatibilité, cela réduira la résilience du réseau\*. Les besoins de sécurité et de décentralisation de Bitcoin commanderaient à ce qu'il soit fondé sur plusieurs implémentations indépendantes assurant que des implémentations continuent à fonctionner indépendamment des failles rencontrées par une implémentation particulière. Cela conduit certains à déceler dans ce monopole Bitcoin Core l'existence d'« *une structure de pouvoir invisible qui prive de ressources les équipes extérieures à cette structure* », avec « *une mafia qui squatte le core dev et empêche les autres équipes de développement de concourir* », selon les mots extrêmes d'A. Taaki<sup>410</sup>.

<sup>401</sup> Voir les discussions : <https://github.com/bitcoin/bitcoin/pull/3408> ; <https://github.com/bitcoin/bitcoin/issues/3203> ; <https://github.com/bitcoin/bitcoin/pull/3400> [consultation au 11/10/2021].

<sup>402</sup> <https://github.com/bitcoin/bitcoin/pull/3408> [consultation au 11/10/2021].

<sup>403</sup> N'ayant pas « *d'avis tranché* », la proposition obtiendra son « accord » (<https://github.com/bitcoin/bitcoin/issues/3203#issuecomment-28133803>) [consultation au 12/10/2021].

<sup>404</sup> [https://en.bitcoin.it/wiki/Bitcoin\\_Core#Naming\\_Controversy](https://en.bitcoin.it/wiki/Bitcoin_Core#Naming_Controversy) [consultation au 12/10/2021].

<sup>405</sup> [https://www.reddit.com/r/Bitcoin/comments/60jqm2/a\\_proposal\\_for\\_and\\_demo\\_of\\_a\\_new\\_bitcoin\\_address/df73k2h/](https://www.reddit.com/r/Bitcoin/comments/60jqm2/a_proposal_for_and_demo_of_a_new_bitcoin_address/df73k2h/) [consultation au 12/10/2021].

<sup>406</sup> <https://github.com/bitcoin/bitcoin/issues/3203#issuecomment-27787010> [consultation au 12/10/2021].

<sup>407</sup> <https://github.com/bitcoin/bitcoin/pull/3408> [consultation au 12/10/2021].

<sup>408</sup> Bcoin est une implémentation indépendante de Bitcoin écrite en JavaScript, publiée en 2014 par Fedor Indutny. Portefeuille léger de navigateur, son développement a été réalisé ensuite par Jeffrey, pour Purse.io.(Apodaca 2017; Chiang 2017).

<sup>409</sup> La présentation de Chris Jeffrey démontrait ce point via une faille DOS. Cette divulgation a engendré des débats et critiques, parfois véhémentes, son caractère « responsable » et « légitime » est contesté, puisque la présentation n'a pas attendu le patch alors que les organisateurs de l'événement avaient demandé de ne pas la faire pour cette raison [L. Thiébaut, Entretien n° 21]. Lui argue que l'équipe Core a été informée plusieurs mois en avance et n'a pas réagi, justifiant des problèmes de disponibilité\* qui vont dans le sens de ce que sa démonstration visait à démontrer (<https://diyhpl.us/wiki/transcripts/breaking-bitcoin/2017/2017-09-10-christopher-jeffrey-consensus-pitfalls/>) [consultation au 12/10/2021].

<sup>410</sup> <https://twitter.com/Narodism/status/1445335283533242370> [consultation au 12/10/2021].

Il est temps de présenter les acteurs humains ayant à leur charge maintenance et sécurité de Bitcoin, qui sont apparus dans l'histoire du bogue analysé.

## **Qui peut modifier Bitcoin ? Bitcoin Core, un groupe en charge de maintenir et sécuriser Bitcoin ?**

Comme rappelé en introduction du chapitre, il n'est pas erroné de dire, comme certaines critiques, que la plupart des *bitcoiners*\* sont peu préoccupés des bogues qui pourraient toucher Bitcoin : les *bitcoiners*\* le concèdent, « *la menace des bogues logiciels est sévèrement sous-estimée dans le monde des cryptomonnaies*\*. » (Fields 2018). Mais ce n'est sûrement pas parce que les utilisateurs auraient « *une confiance aveugle* [...] *dans les codes et l'algorithme* » Ponsot (2021, p. 2) : leur *foi* est moins « *dans le bitcoin* » que dans les « *super codeurs* » qui en ont la charge (« *In Super Coders We Trust* »)<sup>411</sup>. Bitcoin est construit autour de préoccupations sécuritaires. À l'origine, Nakamoto avait même intégré à Bitcoin un système d'alerte visant à informer l'ensemble des *nœuds*\* d'un problème éventuel, système rapidement supprimé, car il correspondait à « *un point de contrôle unique* » (Hertig 2018b). Nos analyses dévoilent une communauté Bitcoin fragmentée, selon une division sociale du travail distribuant confiance, délégations et comptes à rendre entre groupes composant sa communauté. La surprise qui a entouré le bogue CVE 2018 (Song 2018c) reflète en partie cette spécialisation, en mettant au jour des membres en charge d'administrer les codes et les crises qu'ils rencontrent. Cette surprise dénote en creux des attentes déçues : ils s'attendent à ce que des audits et « *relectures du code* [soient] *faites* » (*Bitcoin Q&A* 2018). L'anticipation et l'administration des crises, qu'elles soient « de vulnérabilité » ou « d'évolution », est déléguée à un groupe d'acteurs plus techniciens dont c'est « *définitivement une grande préoccupation* [...] *pendant les premières années où j'ai travaillé sur Bitcoin Core et sur le logiciel Bitcoin* [dès 2011, NdA], *notre plus grande préoccupation était* [la survenue d'] *un bogue et [...]* *que tout d'un coup, tout s'écroulait et qu'il n'y avait rien qui puisse être sauvé du système* » (McCormack et Corallo 2019).

Difficile de ne pas voir que le groupe des « Core Devs » dont fait partie Corallo, au centre des évènements restitués, tient effectivement le rôle d'« *autorité* [pouvant] *intervenir et sauver la situation* » (Varoufakis 2013) quand elle s'écarte des attendus communs. Ces membres volontaires disposent de capitaux culturels (savoir et savoir-faire) *ad hoc* hautement spécialisés. Ils ont la charge, plus ou moins formelle (comme avec les « Core mainteneurs », cf. section suivante), de maintenir et corriger le logiciel Bitcoin (Lopp 2018 ; Song 2019). L'optimisation des codes et la gestion des failles sont pour eux des activités quotidiennes. À la manière des pierres de l'église de Sainte-Anne étudiées par Edensor (2011, cité par Denis 2020)<sup>412</sup>, si, pour de nombreux *bitcoiners*\*, Bitcoin apparaît d'abord comme extrêmement « sécurisé », « stable » et « immutable », du point de vue des techniciens chargés de sa maintenance, il leur apparaît fragile et jamais stabilisé/ossifié : « *le logiciel chargé de faire respecter les règles de validation*\* *devra toujours évoluer. Des changements sont constamment apportés pour améliorer les performances, ajouter des fonctionnalités, renforcer la sécurité, etc.* » (Fields 2018). « *Bitcoin Core est très optimisé* » et il doit le rester : d'où une PR 9049 proposée et acceptée. Et ce travail quotidien implique que « *nous continuerons à voir des bogues. Tous les logiciels ont des bogues. Il n'existe pas de logiciel sans*

---

<sup>411</sup> Voir le tweet original : <https://twitter.com/APompliano/status/1420095187578195974?s=20> [consultation au 14/10/2021].

<sup>412</sup> Edensor (2011), étudiant la matérialité de la pierre de l'église Sainte-Anne, saisit comment cette entité, apparaissant « comme la chose la plus immuable qui soit », porte néanmoins « aux yeux et aux mains des ouvriers » qui la restaurent « des propriétés instables [...], la pierre est sujette à de nombreuses détériorations (ex. décoloration, effritement, fissuration...) » qui compromettent les « caractéristiques esthétiques de l'édifice patrimonial [et] sa pérennité même » (Denis 2020, p. 287).

*bogue* » (Antonopoulos 2018). Ce regard d’expert met en exergue la relativité de représentations et des attendus des *coiners*\*<sup>413</sup>.

Le « *plus grand défi de Bitcoin* » du groupe des « Core Devs » est d’« *éviter les bugs logiciels catastrophiques* » (Fields 2018). Si leurs pratiques empruntent au secteur de la production logicielle et de la sécurité informatique, ils sont conscients des enjeux spécifiques posés par les CM et leur protocole ouvert. Travailler sur Bitcoin s’apparenterait à de l’ingénierie à haut risque. Son logiciel « *est extrêmement complexe, en particulier le code au niveau du consensus [qui] est la forme la plus difficile de développement logiciel qui existe aujourd’hui [,] probablement proche de l’ingénierie aérospatiale, du fait que [...] chaque changement minuscule dans le code peut avoir des effets considérables.* » (Antonopoulos\_2018). M. Corallo abonde, ajoutant que les pratiques de développement de Bitcoin gagneraient à s’inspirer de logiciels comme ceux « *de sécurité vitale, les appareils médicaux, les avions, ce genre de logiciels* » (McCormack et Corallo 2019). Il reste des contraintes spécifiques posées aux CM. Encore expérimental, leur caractère « *décentralisé* » ou tout du moins « *distribué* »<sup>414</sup> et le caractère hautement monétisable des failles font des CM « *un défi d’ingénierie unique* » (*Ibid.*) et « *un "Far West" virtuel* » exposant à « *un risque élevé de bogues* » (Böhme et al. 2020, p. 3) : une CM repose « *sur des systèmes distribués [et des] outils cryptographiques complexes, [...] issus de la recherche de pointe qui n’ont pas été largement évalués* » ; la concurrence « *féroce* » entre CM induit des mauvaises pratiques, pouvant pousser « *les développeurs\* à sauter des étapes importantes nécessaires pour sécuriser leur base de code* » ; enfin, « *la forte prévalence des bogues est exacerbée par le fait qu’elles sont si facilement monétisables [...] les exploits qui volent des pièces sont à la fois lucratifs pour les cybercriminels et préjudiciables pour les utilisateurs et les autres parties prenantes.* » (Böhme et al. 2020, p. 3)

Corallo [Entretien n°15] et ses collègues de bureau font partie des développeurs\*, peu nombreux, ayant réussi à se faire financer. À l’exception de l’entreprise de Corallo et ses collègues, « *ChainCode labs* », ou encore de « *Blockstream* », qui offrent des contrats de travail permettant de financer leurs travaux sur Bitcoin Core<sup>415</sup> (BitMEX Research 2020a), bien peu nombreux sont les

---

<sup>413</sup> Corallo, par exemple, partant du risque de bogue et de scission de chaîne, critique la convention entourant la finalité de paiement de Bitcoin fixée à 6 confirmations\* (cf. section III.1.2 précédente), car elle ignore le temps nécessaire à cordonner une remise en ordre : « *effectuer des transactions à 3 confs, 6 confs, 12 confs est vraiment risqué [car] effectuer des transactions dans un délai inférieur au temps que les gens peuvent raisonnablement consacrer à répondre à un problème, à en identifier la cause et à le résoudre, ce qui n'est certainement pas deux heures. Vous introduisez beaucoup de risques.* » (Annexe IV.2, Observation participante n°25, retranscrit chez Osuntokun et al. 2019).

<sup>414</sup> Dans ce passage, Corallo revient sur le fait que, au sein de ces industries, la centralisation facilite les procédures de développement et de tests : « *leur solution est généralement de tout exécuter trois fois ; sur trois implémentations différentes et sur trois processeurs différents fonctionnant sur trois systèmes différents et vous choisissez juste celui qui est répété, d'accord. Donc vous avez les différents systèmes pour voter sur ce qu'est la solution.* » (McCormack et Corallo 2019)

<sup>415</sup> « *C'est tous des gens qui sont de leur côté, qui font des trucs, tu peux en avoir quelques-uns chez Blockstream mais c'est... et même, enfin je veux dire, Blockstream aujourd'hui je considère que c'est plus une boîte de recherche, tu vois* » [N. Bacca, Entretien n° 8]. Blockstream faisait partie des sponsors des évènements « *Breaking Bitcoin* » (Observation participante n° 14 et 25, Annexe n°IV.2), dont l’une des organisatrices nous apprend que « *Chaincode Lab* » organise aussi des formations « *sur plusieurs semaines de « "relecture" ("review") autour de la proposition de modification "Taproot" [...] organisée par des core devs. [...] Et en fait c'était sur 7 semaines normalement, c'était quatre fois par semaine, 40 heures par semaine. J'ai arrêté parce que c'était trop... trop chronophage, j'étais un petit peu larguée et en fait c'était une review avec toutes les semaines un sujet différent sur un petit peu de tout : "« Taproot", "», "« Grassroot", "», "« Schnorr", "», "« MAST" [...]. On était 160 au début, je crois que ça a terminé avec beaucoup moins [...]. J'étais déjà extrêmement contente que leurs initiatives au groupe 160 personnes, j'ai trouvé que c'était vraiment génial, ils ont organisé ça mais de manière incroyable, les mails, les machins... on sentait vraiment qu'il y avait un énorme investissement de la part des organisateurs pour faire en sorte de rendre le travail fluide pour tout le monde ».*

développeurs\* Bitcoin à pouvoir en vivre [Stéphane Roche, Anon 1, 2 et 3 ; Entretien n° 23, 1, 2 et 3]. Le financement des personnes en charge de la maintenance et de la sécurité de la couche protocolaire de Bitcoin est « *un problème [...] intéressant [...] à regarder* » : malgré la valeur générée, il n'y a finalement que « *très peu de gens en fait, dans les boîtes autour de l'écosystème, qui sont impliqués dans les couches protocolaires, en tout cas sur Bitcoin [...] Ethereum c'est un peu l'exception avec Consensys [(entreprise du co-fondateur d'Ethereum Joe Lubin) et] la fondation Ethereum [en comparaison] Blockstream [...] c'est ce qui pourrait se rapprocher le plus [...]* d'un truc comme l'Ethereum Foundation dans le monde de Bitcoin » [N. Bacca, Entretien n° 8, rejoint par Léa Thiebaut, Entretien n° 21]. Rapporté à d'autres projets à codes sources ouverts, ce problème structurel s'expliquerait par l'absence d'« *une culture qui va fonctionner un petit peu comme tu peux avoir sur Linux aujourd'hui. Les choses s'y sont extrêmement professionnalisées et au final tu as toutes les grandes distributions qui participent aussi au noyau. Tu n'as pas du tout cette équivalence en fait aujourd'hui dans les cryptomonnaies\**. Donc tu as extrêmement peu [...] de développeurs\* Bitcoin sur le... au niveau du protocole et du consensus qui sont dans une boîte. » [N. Bacca, Entretien n° 8] Ainsi, la grande majorité du financement « *envers les devs provient de propositions d'emploi [et de] systèmes de bourse ou de sponsor, ce qui me plaît énormément en fait. Moi j'aime bien ce côté indépendance [...] des Devs* ».

Une telle situation pose des questions. Si l'établissement de « *la hauteur des passerelles\** à l'intérieur du parc de Long Island a été choisie afin d'interdire le passage des cars, moyen de transport privilégié des Noirs, de telle sorte que la fréquentation de ces zones de loisir reste l'apanage des Blancs » (Akrich 2010, p. 219, note 1), que dire du design d'un système monétaire, même distribué et du rôle de ces concepteurs<sup>416</sup> : Bitcoin ? « *Évidemment que c'est politique [et] il faut être un petit peu naïf pour considérer que ça ne l'est pas* », impossible de ne pas reconnaître des « *enjeux politiques [et] de gouvernance au sens large* » dans cette situation. « *Cela soulève des questions sur leur neutralité* » et la présence de conflits d'intérêts potentiels : « *comment cela se passe si [...] une idée pour améliorer le protocole Bitcoin [implique de rendre] incompatible, voire obsolète tous les produits issus d'une de ces entreprises [...]. Viendrait[-on] à discuter de cette mise à jour [...] ou pas ? Je ne dis absolument pas [que ces conflits d'intérêts existent] mais [...] c'est des questionnements qui sont ouverts.* » [L. Thiébault Entretien n° 21] A. Walch a questionné sur Twitter cette neutralité<sup>417</sup> : « *Serait-ce un problème si [Chaincode Labs] ou toute autre entité payant les développeurs\* principaux #Bitcoin ont tenté d'influencer le développement ? Et s'ils menaçaient de licencier les développeurs\* principaux qu'ils paient à moins que les développeurs\* ne préconisent une trajectoire particulière pour le protocole ? Le développeur\* devrait-il divulguer publiquement cette pression ? Quelles attentes ont les gens par rapport à un tel scénario ?* ». Le CEO de Blockstream, A. Back, assurera que non, leur indépendance est formellement garantie : « *À [Blockstream] nous avons négocié avec des investisseurs pour l'indépendance des développeurs\* de bitcoins. Si une nouvelle direction essayait de faire pression sur un développeur\* principal pour qu'il apporte un changement qu'il jugeait mauvais pour Bitcoin, il pourrait démissionner et l'entreprise serait tenue de payer un an de salaire pendant qu'il trouve un nouveau financement [. J]e pense [Digital Currency Initiative] et peut-être [Chaincode Labs] doivent avoir quelque chose de similaire (mais probablement sans parachute). Il existe également quelques développeurs\* indépendants "no strings" financés par des bourses. [...] Je sais qu' [Angela\_Walch] semble essayer de construire un argument sur la centralisation du contrôle[...]. Mais les gens ont 5 ans*

<sup>416</sup> Léa Thiebault, en explicitant le « *Slogan Code is Law* », fait référence au texte de Lessig et à l'exemple de la construction d'un pont dont le design servait des fins racistes. Sans trouver cette référence dans le texte cité, nous reconnaissons les travaux de L. Winner (cité par Akrich 2010).

<sup>417</sup> [https://twitter.com/angela\\_walch/status/1230239961045241856](https://twitter.com/angela_walch/status/1230239961045241856)

[https://twitter.com/angela\\_walch/status/1230239962336985093](https://twitter.com/angela_walch/status/1230239962336985093) [Consultation au 24/06/2023].

*d'avance pour reconnaître et se défendre contre de tels risques. Et il y a des expériences antérieures à #bitcoin dans les FOSS [et puis] les gens ne sont pas très motivés par le salaire : ils sont poussés à travailler sur des choses utiles à la société, et non sur des choses qu'ils considèrent comme défiant l'éthique »*<sup>418</sup>. A. Back reproche à Walch de chercher par ces questions à dresser l'image d'une gouvernance de Bitcoin centralisée, comme pour démontrer que de ne pas parler de politique de Bitcoin relèverait moins de la naïveté que d'une invisibilisation stratégique : les crises révèlent au grand jour ce qui, pour certains *bitcoiners\**, relève de « *tabous [et de] questions qui ne sont pas posées !* » [L. Thiébaut, Entretien n°21]. Il ne faudrait pas s'aventurer à le faire (cf. Non-Entretien n°27). D'autres *coiners\** considèrent que ces stratégies d'évitement et d'occultation de la gouvernance des CM prive leur développement d'un professionnalisme et d'une transparence nécessaires : il faut « *faire en sorte de créer un écosystème qui soit plutôt défavorable [aux conflits d'intérêts]. Après heureusement qu'il y a ces entreprises dans l'écosystème[,] c'est incroyable ce qu'ils font ! Le tout c'est de trouver en fait une sorte d'éthique de communauté [comme] pour Linux cela ne s'est pas créé non plus en une journée* » [L. Thiébault, Entretien n° 21, rejoint par Bacca, Entretien n° 8]. Selon ce prisme, la méconnaissance par le grand public de ces crises est en partie le produit d'une faible publicité servant à cacher une gouvernance moins *invisible* qu'indicible.

Cette fragilité ontologique (perçue ou non des *bitcoiners\**) se lit aussi dans le répertoire logiciel « Bitcoin Core » qui témoigne de l'activité de maintenance quotidienne<sup>419</sup>. Cet arrangement sociotechnique clef de l'administration des codes logiciels Bitcoin Core permet d'établir tout à la fois les rôles et statuts de « Core Dev », le cadre de cette activité de production, et les dispositifs de contrôle et de consignation assurant traçabilité, transparence et auditabilité en vue d'information communautaire.

### III.2.2 Où modifier Bitcoin ? Un « repo Bitcoin Core » encadré et hiérarchisé

Codes et codeurs apparaissent centraux lors des crises, comme pour le fonctionnement routinier de Bitcoin. Leur mise en relation nécessite un lieu et des modalités d'interactions. Cette activité de production des codes d'une CM est hautement critique, et les modifications de code sont précisément encadrées. Ces dispositifs d'encadrement renvoient à un lieu particulier qu'il nous faut présenter.

#### Le répertoire « Bitcoin Core » et son administration

L'espace ordonné du face-à-face entre codes et codeurs, central tant dans les mises en crise que dans les remises en ordre, est la forge logicielle\* « Github » (voir Encadré n°5 suivant), la plateforme d'hébergement référente du répertoire logiciel « Bitcoin Core » (le « *repo* »). Le type de dispositif qu'est une forge n'est pas spécifique au développement de CM, mais emprunté au champ de la production de logiciels libres et ouverts, dans lequel Nakamoto s'inscrit (Cf. Chap. I).

---

<sup>418</sup>

Voir

<https://twitter.com/adam3us/status/1233309387646697483>;

<https://twitter.com/adam3us/status/1233310168831709186>

<https://twitter.com/adam3us/status/1233310814783844352> <https://twitter.com/adam3us/status/1233311769692721158> [Consultation au 24/06/2023].

<sup>419</sup> <https://github.com/bitcoin/bitcoin/graphs/contributors?from=2009-10-14&to=2021-10-21&type=c> permet d'observer l'activité sur le répertoire logiciel « Bitcoin Core » [consultation au 14/10/2021].

### Encadré n°5 : Les forges logicielles, un système de production collaboratif de logiciels libres

Le développement logiciel de Bitcoin et des CM repose sur la création distribuée de ressources. L'agrégation de contributions librement accessibles y suit un « *modèle d'action collective et de production de biens publics qui intègre l'utilisation de réseaux\* de communication numérique et des technologies de l'information* » (Benkler 2006 cité par Shaw et Hill 2014). Les objectifs de la liberté logicielle, tels que définis par Stallman (1999 ; cf. Chap. I), nécessitaient des moyens. Apparues à « *la faveur de l'accès public à l'Internet [...] des années 1990* », les forges logicielles sont de ceux-ci, en tant qu'environnements de développement logiciel collaboratif (Elie 2013). Leur développement s'est fait en trois temps. Le premier est celui du « *free software* », où une « *communauté proche de l'esprit académique [valorisant] l'efficacité de la coopétition* » (Elie 2013) est intéressée par la production de savoir mais non par la vente, d'où la création d'outils libérant « *les couches basses de l'informatique [...] les couches systèmes et réseaux\** » (protocole IP de V.Cerf et B. Kahn en 1974, ou http, de T.B. Lee ; *Ibid.*). Le tournant 2000 correspond au « *moment open source* » (*Ibid.*) à la tête duquel sont des industriels. Produisant pour vendre, ils reconnaissent l'efficacité de la collaboration (exemple de la fondation Apache), et cela va conduire au développement de logiciel de plus haut niveau et à une meilleure interopérabilité. C'est l'absence de répercussion pour les utilisateurs de ces logiciels qui les poussera à se constituer en une troisième communauté. Les utilisateurs se mettent à « *gouverner la production, [...] piloter la feuille de route des logiciels qu'ils utilisent et achètent, en particulier les logiciels métier* » (*Ibid.*, p. 12). Ces temps et communautés ont développé des dispositifs qui, bien qu'*ad hoc*, « *convergent vers les mêmes outils de production* » (*Ibid.*, p. 15). La forge logicielle\* « *Github* » est une héritière de cette convergence et ces anciennes communautés y cohabitent aujourd'hui (McMillan 2012).

Les forges contemporaines sont tout à la fois des plateformes d'hébergement web pour les codes sources logiciels, un ensemble d'outils de développement logiciel et des plateformes de discussion et d'échange pour les contributeurs. Portail communautaire accessible via un site Internet, elles offrent une série de services de gestion de projet, avec : un système de gestion des versions (de type Git ou mercurial) ; des systèmes de *tracker*, pour faire remonter les demandes de fonctionnalité, gérer l'attribution et le suivi des bogues, ou encore la gestion/répartition des tâches ; un service de publication/livraison des paquets et fichiers (nous verrons que les *bitcoiners\** innovent dans ce domaine) ; des outils d'intégration continue ; des gestionnaires de listes de discussion (et/ou forums) et de documentation (de type wiki) permettant les discussions et échanges d'information entre les participants (Creatis 2017). Ces outils et procédures normalisés permettent, en les encadrant, la production/gestion de codes sources logiciels. L'administration du répertoire d'un logiciel repose sur une pyramide hiérarchisée de droits. Sont formellement définis des statuts, des rôles et des niveaux de priviléges, des plus réduits aux plus étendus (dans l'ordre, « *read* », « *triage* », « *write* », « *maintain* » et « *admin* ») dessinant une configuration particulière des sept « *faisceaux de droits* » d'Hess et Ostrom 2007, déjà présentés (cf. Chap. II, section II.3.3 ; voir Tableau 7 suivant concernant l'administration de Bitcoin Core). Au sommet, les « *maintainers* » jouissent de tous les droits : contrôlant l'accès aux droits et permissions, ce sont les seuls à pouvoir ajouter, supprimer ou promouvoir d'autres membres à différentes positions ; ils peuvent changer le nom et la description de l'équipe ; éditer/supprimer des discussions, etc. Ainsi, si tout un chacun est théoriquement libre de Fork\*er un répertoire, c'est-à-dire de créer une nouvelle branche, produire un correctif et proposer sa fusion dans la branche principale (« *Pull Requests* » ou demande d'extraction), l'implémentation dans les codes suit des procédures définies (cf. section 1.2.3 suivante), qu'entérinent ou non les *administrateurs\** disposant des droits associés (« *commit right* » & « *merge* ») via *commit* (cf. sauvegarde constituant une étape du développement de la version). L'encadrement est à la fois formel et informel, puisqu'au droit d'administration s'ajoutent des ordres de statuts où la réputation, jamais stabilisée, est primordiale (Stewart 2005). Formellement ouvertes, ces plateformes le sont moins pratiquement : aux compétences impliquées d'écriture de codes s'ajoute une maîtrise des différents outils à disposition (Git, etc.) et du jargon associé (« *ACK* » pour « *Acknowledge* », « *utACK* » pour « *Untested Acknowledge* », « *NACK* » pour « *No Acknowledge* », « *RFC* » pour « *Request for Comment* », etc.<sup>420</sup>). Ces communautés de production distribuée tendent à se présenter comme des « *oligarchies* » aux « *élites et [...] leaders puissants* », contredisant « *l'idée qu'[elles] impliquent des formes organisationnelles démocratiques* » en soi.

Aujourd'hui, au sein du « *repo Bitcoin Core* » est hébergée la majorité des activités entourant la production des codes sources de Bitcoin Core. Les *bitcoiners\** y trouvent un lieu d'hébergement des différentes versions logicielles, un ensemble d'outils de développement et un lieu de communication entre développeurs\*. La forge leur permet d'encadrer de manière procédurale et ordonnée les interactions des acteurs, que ce soit par les dispositifs génériques offerts par la

<sup>420</sup> Voir <https://docs.github.com/en/get-started/quickstart/github-glossary> [consultation au 18/11/2021].

plateforme, ou par ceux spécifiquement développés par les *bitcoiners*\*. Mais cette situation n'a pas toujours existé. Nakamoto « était un codeur brillant » mais « excentrique » (G. Andresen cité par Simonite 2014), maîtrisant peu les outils de gestion logicielle moderne de ce type : loin des standards logiciels, les codes originaux prenaient la forme d'« une énorme base de code désordonnée » (McCormack et Corallo 2019). M. Corallo abonde en soulignant le travail déjà accompli et celui qu'il reste à faire : « le logiciel original de Bitcoin était très monolithique. Il était très... Tout le code est dans un seul fichier. Le truc du portefeuille pour les utilisateurs interagit fortement avec le code de validation\* et le code de consensus. C'est devenu beaucoup mieux. Nous l'avons beaucoup nettoyé. La séparation entre les différentes parties de Bitcoin Core s'est considérablement améliorée au fil des ans. Il y a encore du chemin à parcourir. Rien n'est parfait, et il y a encore beaucoup de nettoyages et de compartimentages que les gens veulent faire, et cela continuera à se produire lentement [...] en fin de compte, nous avons beaucoup appris et nous avons tellement amélioré le logiciel au fil des ans » [Entretien n° 15]. Comme le chapitre I l'a présenté, au départ Nakamoto coordonne les efforts de développement par mail, puis M. Malmi va créer le « dépôt subversion » de « Bitcoin sur SourceForge », lui-même migré sur GitHub en 2011 (Lopp 2018) pour offrir un espace plus ordonné mais aussi distribué au développement des codes logiciels Bitcoin.

Sur GitHub, le répertoire Bitcoin Core est public, donc « ouvert à tous ». Mais la liberté formelle de contribuer est cadrée par différents dispositifs. Il est attendu pour commencer des volontaires qu'ils respectent un code de conduite stipulant les « comportements acceptables » et « inacceptables »<sup>421</sup>. Ce code de conduite des *bitcoiners*\* est lui-même évalué (positivement) au regard des standards de la plateforme GitHub (servant à évaluer les projets et leurs mainteneurs)<sup>422</sup>, et sera clarifié et sanctionné par les mainteneurs du répertoire (« Project maintainers ») et les contributeurs en temps voulu. Les contributions, quant à elles, recouvrent des activités très hétérogènes, allant de simples traductions à des propositions d'innovation dans les codes. Une nomenclature identifie cinq catégories pour lesquelles sont définis des attendus formels, permettant aux volontaires de facilement définir leur niveau d'engagement, selon leur motivation et leur disposition en capitaux culturels (voir le Tableau 6 ci-après).

---

<sup>421</sup> Voir [https://github.com/bitcoin-dot-org/developer.bitcoin.org/blob/master/CODE\\_OF\\_CONDUCT.md](https://github.com/bitcoin-dot-org/developer.bitcoin.org/blob/master/CODE_OF_CONDUCT.md) [consultation au 25/11/2021].

<sup>422</sup> Le respect de ces standards, la présence d'un code de conduite, ou l'existence de règles de contribution sont présentés (absent ou présent) pour tout projet déposé sur Github dans un onglet spécifique des « Insights ». S'y trouvent de nombreuses informations sur les activités hébergées sur le répertoire en question. Pour Bitcoin Core, voir <https://github.com/bitcoin/bitcoin/community> [consultation au 25/11/2021].

**Tableau 6 : Nomenclature des contributions possibles aux répertoires « Bitcoin Core »**

| Type de contribution <sup>423</sup> | Type de procédure et attendu(s) des contributions  |
|-------------------------------------|--|
| Rapport de Bogue                    | <p><b>Le signalement de bogue renvoie à deux procédures distinctes :</b></p> <p>(i) <b>La « divulgation responsable »</b> pour les bogues de sécurité. Elle doit être réalisée en privé, via la « page de contact de sécurité ».</p> <p>(ii) <b>Le « suivi des problèmes publics »</b> (pour les autres bogues). Le contributeur doit rechercher des « problèmes » similaires à ceux rencontrés pour les y incorporer, ou ouvrir un « nouveau problème », en produisant les informations nécessaires<sup>424</sup>.</p>  |
| Code                                | <p><b>Écrire et relire les propositions de modification du logiciel « Bitcoin Core »</b> : les développeurs* se voient proposer deux types d'activités<sup>o</sup>:</p> <p>(1) <b>Rédaction</b> : en veillant « à fournir un code de bonne qualité et à respecter toutes les directives » décrites dans un fichier du répertoire ;</p> <p>(2) <b>Audit</b> : les « développeurs* expérimentés » peuvent examiner les modifications de code reçues.</p> <p>Sont aussi listés : des problèmes en attente de correctifs et des procédures de test à développer.</p> |
| Documentation                       | <b>Écrire la documentation (utilisateurs et développeurs*)</b> : amélioration de la documentation disponible (corriger les incohérences de terminologie, de style, mettre à jour, etc.) suivant un guide stylistique et deux procédures : ouverture d'un nouveau problème (« new issue ») ou d'une demande d'extraction (« Pull Request »).  |
| Traduction                          | <b>Travaux de traduction pour l'interface utilisateur</b> : les contributeurs doivent créer un compte « Transifex » avant de se rendre sur la page web traduction de « Bitcoin Core » où ils devront s'inscrire. Ensuite, ils peuvent choisir leur langue et proposer des traductions qui, une fois acceptées, seront intégrées à la nouvelle version logicielle.  |
| Support technique                   | <b>Offrir un support aux autres utilisateurs</b> : aider les utilisateurs débutants en répondant aux demandes en ligne ; à cette fin, sont répertoriés les sites et forums informatifs utiles, et leur niveau d'accessibilité.   |

Source : Rolland Maël

<sup>423</sup> Pour une présentation générale, voir <https://bitcoin.org/en/bitcoin-core/contribute/>; chaque activité est décrite dans une page dédiée : Rapport de bogue, voir <https://bitcoin.org/en/bitcoin-core/contribute/issues> ; Code, voir <https://bitcoin.org/en/development> ; Documentation, voir <https://github.com/bitcoin-dot-org/developer.bitcoin.org> ; Traduction, voir <https://bitcoin.org/en/bitcoin-core/contribute/translations> ; Support technique, voir <https://bitcoin.org/en/bitcoin-core/contribute/support> [consultation au 25/11/2021].

<sup>424</sup> Les contributeurs sont invités à suivre les recommandations générales stipulées dans la documentation de Mozilla. La documentation « Bitcoin Core » précise que sont attendus : une description claire du problème, voire une description des conditions de sa reproduction ; la version « Bitcoin Core » utilisée ou le « commit » utilisé pour sa construction (git log -1), ainsi que les éventuels correctifs appliqués ; enfin, le contributeur peut ajouter toute entrée pertinente de son fichier « debug.log » (en faisant attention aux informations privées qu'il peut contenir). Voir <https://bitcoin.org/en/bitcoin-core/contribute/issues> [consultation au 25/11/2021].

Ces intitulés et leur attendus dessinent une grammaire institutionnelle (Ostrom 2005) permettant de mieux comprendre la diversité des interactions des *bitcoiners*\* au sein du « repo Bitcoin Core » : des règles, normes et stratégies partagées se distinguent à travers ces attendus plus ou moins prescriptifs (on retrouve les différents types d'opérateurs logiques - « doit », « requiert », « interdit », « permet » - qui les caractérisent, Ostrom et Basurto 2013, p. 11). À leur lecture, on comprend que ces activités reposent sur des compétences, savoir et savoir-faire différenciés : les *bitcoiners*\* réalisant des traductions sont différents de ceux qui rédigent les rapports de bogue, de ceux qui s'occupent de la rédaction de nouveaux codes ou en réalisent les audits et relectures. Aussi, les membres de la communauté Bitcoin participant à ce type d'activité sont peu nombreux. Si Bitcoin Core, en tant que projet open source\* suit un modèle de contribution ouverte, où tout un chacun peut proposer une évolution, l'administration de son répertoire, elle, relève d'une poignée d'acteurs désignés, qui ont le pouvoir de les approuver et de les intégrer dans une nouvelle version.

#### **D'une hiérarchie formelle selon le principe « du moindre privilège » à la désignation informelle des mainteneurs « Core »**

Le chapitre II a conclu que la gouvernance d'une CM comme Bitcoin se présentait comme polycentrique : en tant que système de ressources, une CM est constituée de sous-systèmes de ressources propres, articulés entre eux (Hess et Ostrom 2003 ; cf. Chap. II, section II.3.3). Le répertoire Bitcoin Core GitHub constitue l'un de ces sous-systèmes essentiels de l'infrastructure Bitcoin et les « unités de ressources » produites et distribuées, bien qu'immatérielles (les *codes open source*\* et les informations les concernant) n'en sont pas moins critiques. Aussi, ce système et son administration sont fortement régulés. Ces régulations renvoient à la présence des sept composantes

structurelles<sup>425</sup> qui, dans le cadre IAD d’Ostrom, s’articulent singulièrement pour définir le système institutionnel ayant cours dans une arène d’action (Ostrom Bazurto 2011 ; Chanteau et Labrousse, 2013). Cette régulation passe d’abord par l’identification de statuts d’acteurs à rôles spécifiques, comme les « Core Mainteneurs », disposant de priviléges d’administration divers.

Les *bitcoiners\** reconnaissent qu’une « *certaine hiérarchie est nécessaire à des fins pratiques* » (Bitcoin Core 2018b<sup>426</sup>). Elle se justifie par les contraintes de coordination importantes qu’implique la gestion d’une multitude d’activités et d’acteurs : « *si n’importe qui pouvait fusionner dans la branche master, cela [correspondrait] à un scénario du type "trop de cuisiniers dans la cuisine"* » (Lopp 2018), pouvant dégénérer en des corruptions volontaires ou du vandalisme. N’importe qui ne peut pas faire n’importe quoi suivant que l’administration du répertoire Bitcoin Core repose sur une structure hiérarchique formelle avec : « *des "mainteneurs" de répertoire qui sont responsables de la fusion des demandes de retrait* [les « Pull Requests »], *ainsi qu’un "mainteneur principal" qui est responsable du cycle de publication, de la fusion globale, de la modération et de la nomination des mainteneurs* » (*Ibid.*).

**Tableau 7 : Les priviléges d’administration du répertoire Bitcoin core**

| Privilège / Rôle accessible sur le repo Bitcoin Core <sup>427</sup> (s)   | Maint. Princ. | Maint. Simple | Autres contrib. |
|---|---------------|---------------|-----------------|
| <b>1 - Lecture (« Read »)</b><br><i>Accès à l’information</i>   | Oui           | Oui           | Oui             |
| <b>2 -Triage (« Triage »)</b><br><i>Gestion active des problèmes et des PR sans accès en écriture</i>                 | Oui           | Oui           | Oui             |
| <b>3 -Écriture (« Write »)</b><br><i>Contribution active au code</i>  | Oui           | Oui           | Non             |
| <b>4 - Maintenance (« Maintenance »)</b><br><i>Gestion du dépôt sans accès aux actions sensibles ou destructrices</i> | Oui           | Oui           | Non             |
| <b>5 - Admin (« Admin »)</b><br><i>Accès complet au projet, y compris les actions sensibles ou destructrices</i>      | Oui           | Non           | Non             |

Source : Rolland Maël

L’administration du système de ressources qu’est le « repo Bitcoin Core » relève d’une pyramide de droits, plus ou moins subordonnés, suivant l’application du principe de moindre privilège, devant permettre une gestion efficace, assurant que chaque acteur dispose du niveau d’accès approprié à sa fonction sans lui donner plus de priviléges que nécessaire. En son sein, cinq familles de droit/privilège existent (cf. Tableau 7 ci-contre), chaque niveau ajoutant aux droits précédents de nouveaux droits. On y trouve : la « lecture », qui correspond au rôle par défaut et ses droits afférents permettent de voir et discuter du projet sans contribuer au code - dans l’ordre des faisceaux de droits (Hess et Ostrom 2007, p. 52-53), ce statut recouvre les droits d’accès (tout le monde peut y venir, observer, voire échanger), de prélèvement (rien n’empêche de copier les codes qui s’y trouvent) et de contribution (puisque tous

<sup>425</sup> Les sept composantes structurelles d’un système de règles sont : les règles de définition des rôles (ou « position rules ») ; les règles d’accès au rôle (ou « Boundaries rules ») ; les règles d’allocation des ressources (ou « Allocation / choice rules ») ; les règles sur les procédures de décision collective (ou « Aggregation rules ») ; les règles d’information (ou « Information rules ») ; les règles de contribution/rétribution (ou « payoff rules ») ; les règles délimitant les usages possibles des ressources (ou « Scope rules »). Voir Ostrom et Basurto (2013, p. 10-11).

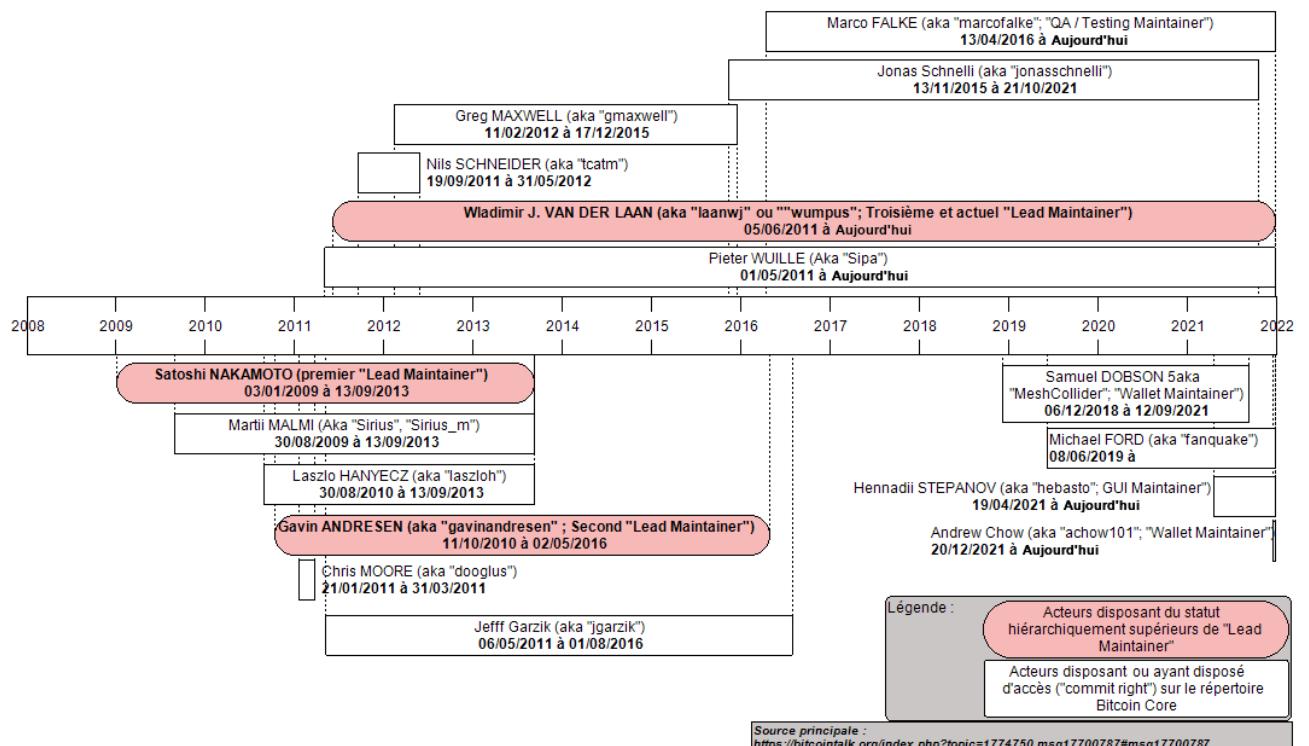
<sup>426</sup> <https://github.com/chaintope/tapyrus-core/blob/master/CONTRIBUTING.md> [consultation au 25/11/2021].

<sup>427</sup> Nous nous sommes limités aux catégories génériques, au sein de chacune se trouve une multiplicité de combinaisons de priviléges et d’actions potentielles, voir <https://docs.github.com/en/organizations/managing-access-to-your-organizations-repositories/repository-permission-levels-for-an-organization> [consultation au 29/11/2021].

ici peuvent se lancer dans des propositions) ; le « triage » ajoute aux droits précédents des droits liés à la gestion active des problèmes et des « *Pull Requests* » sans pour autant avoir un accès en écriture ; l’« écriture » et ses priviléges, plus critiques que les précédents rôles, sont réservés aux contributeurs actifs et reconnus. Ce rôle ajoute aux droits précédents des droits de management et de gestion ; la « maintenance » va encore plus loin : ces droits permettent de gérer le dépôt, mais aussi l'accès aux actions sensibles ou destructrices n'est pas donné. Ici comme précédemment, on trouve des acteurs reconnus, de type « mainteneurs simples ». Enfin, les droits hiérarchiquement supérieurs d'« Administration », touchant à tout, y compris aux actions sensibles ou destructrices (donc ajoutant aux précédents ceux d'exclusion et de suppression, *Ibid.*), sont le privilège exclusif d'un mainteneur principal unique.

Ce groupe de mainteneurs simple, avec le mainteneur principal au centre, est aussi essentiel que restreint. Depuis 2009, nous avons décompté 16 acteurs ayant tenu ou tenant ce rôle de « mainteneurs » (cf. Chronologie 5 suivante). Le nombre de développeurs\* dits « Core Devs » excède ce décompte, car il est construit à partir de l'organigramme général du repo Bitcoin Core : sont exclus les contributeurs actifs et reconnus qui, à la manière d'un acteur aussi central que M. Corallo, disposent de priviléges en lien avec leur activité, sans pour autant porter la casquette de mainteneur simple. Dans tous les cas, l'usage de priviléges d'administration et de gestion donne lieu à consignation en vue de traçabilité et d'information.

### Chronologie 5 : Les différents acteurs disposant ou ayant disposé de droits spécifiques d'accès (« commit right ») et du rôle de « Core Mainteneurs » sur le répertoire Bitcoin Core



Source : Rolland Maël

Au sommet de la hiérarchie, le « mainteneur principal » jouit des rôles d'« *Admin* », donc, de la plénitude des priviléges et pouvoirs offerts par la plateforme. Trois individus se sont succédé à

ce rôle depuis 2009 : S. Nakamoto, qui fut remplacé par G. Andresen, lui-même remplacé par W.J. van der Laan, mainteneur principal actuel. Au niveau intermédiaire, on trouve les « mainteneurs simples » et les « Core Devs » à la Corallo, qui disposent à différents degrés (en fonction de leurs activités), des priviléges afférents aux rôles de « *triage* », d’« *écriture* » et de « *maintenance* », comme le droit d’administration (ou « *commit right* ») sur tout ou partie (« portefeuille », « questions/réponses et testing », etc.) du répertoire Bitcoin Core. Le dernier niveau correspond au commun des utilisateurs, avec le rôle par défaut de « *lecture* ». Toute contribution émanant de la base se doit d’être avalisée par un échelon supérieur. Le droit à proposition d’évolution des codes est donc suspendu à l’aval des « mainteneurs simples » ou du « mainteneur principal ». Ce sont eux qui, *in fine*, ont le pouvoir de les accepter et de les intégrer dans les codes d’une nouvelle version. Au sommet de la pyramide, le « mainteneur principal » peut, comme tout mainteneur simple, être appelé à accepter/refuser des modifications proposées par la base, mais son rôle est de superviser l’ensemble des aspects du projet et d’être « *responsable de la coordination des versions* » (Lopp 2018). Il jouit d’un pouvoir discrétionnaire sur les codes sources ou sur les nominations/révocations des autres mainteneurs.

Si les droits sur le répertoire Bitcoin Core sont formels, les dispositifs et critères présidant à la désignation de ces acteurs clefs sont, eux, informels. Comme souvent dans les communautés open source, cette désignation relèverait « *de la méritocratie, où les contributeurs à long terme gagnent davantage la confiance de la communauté des développeurs\** » (Bitcoin Core 2018b). La désignation des mainteneurs « Bitcoin Core » relève de la pratique, sans qu’aucun critère, ni processus formel de désignation ne soit explicité, ni publicisé. Cette élection concernerait « *des contributeurs qui ont construit un capital social suffisant au sein du projet en apportant des contributions de qualité sur une période donnée* » (Lopp 2018). Elle apparaît fondée sur un mécanisme de cooptation donnant un poids important aux affinités électives, aux proximités sociales, aux relations de confiance de long terme, donc à une certaine homogénéité en valeurs. Que ce soit pour le statut de « mainteneur principal », qui a été « *transmis volontairement au fil des ans* » (*Ibid.*), ou pour les « mainteneurs simples », qui sont nommés par « *le groupe existant de mainteneurs* », décidant discrétionnairement « *d'étendre le rôle à un contributeur qui a fait preuve de compétence, de fiabilité et de motivation dans un certain domaine* » en lui accordant « *un accès de commit au compte GitHub* » (Lopp 2018). Et il faut que le mainteneur principal accepte, car, en dernière instance, il est le seul à pouvoir donner ou reprendre les droits d'accès à un compte « *Github* ».

Est-ce à dire que le « mainteneur principal » est un dictateur qui, « éclairé » ou non, fait ce qui lui plaît ? Cela interroge le cadre des relations entre le « mainteneur principal » et les « mainteneurs simples » et, finalement, les modalités des prises de décision. Il ressort de ce dispositif un cadre ni transparent, ni fixé une fois pour toutes, qui évolue suivant la personnalité du « mainteneur principal », soulignant du même coup le poids pris par ce rôle et l’acteur qui le tient. Au commencement de Bitcoin, l’administration des codes relevait d’une logique de « dictateur éclairé » et « *tout était vraiment plus simple [...] : on avait un code source et une personne sous pseudonyme qui prenait toutes les décisions [...]* » (Andresen cité par Ailleurs 2015). Suite au retrait de Nakamoto et sa transmission des priviléges d’administration à Andresen, ce dernier va « *essayer de décentraliser tout cela* » en établissant cinq autres mainteneurs à ses côtés<sup>428</sup> (*Ibid.*). Décentralisation pour le moins relative, car Andresen le concède, en l’absence de consensus : « *je tranchais. Je décidais d'aller dans une direction plutôt qu'une autre. J'agissais comme un dictateur bienveillant pour Bitcoin Core mais je pense que cela marchait.* » (*Ibid.*). Preuve encore du poids pris par la personnalité du mainteneur principal, cette situation va changer à partir de 2014, avec

---

<sup>428</sup> Wladimir J. van der Laan, Gavin Andresen, Jeff Garzik, Gregory Maxwell et Pieter Wuille.

l'arrivée de W.J. van der Laan : « *Wladimir, à qui j'ai passé la main, n'envisage pas son rôle ainsi. Il est plus conservateur, il n'ajouterait rien sans avoir le consensus* [des autres mainteneurs<sup>429</sup>]. *Les changements peuvent donc être bloqués par un simple veto et je ne pense pas que cela soit très sain.* » (*Ibid.*). W.J. van der Laan conçoit son rôle de « mainteneur principal » du répertoire « Bitcoin Core » différemment et souhaite défendre « *avec ferveur la décentralisation et l'autonomie* » de Bitcoin, d'où des actions mues par un principe simple : « *toute proposition ou amélioration survenant dans un BIP au profit de Bitcoin doit être approuvée par la grande majorité des développeurs\* et des collaborateurs avant d'être mise en œuvre dans le système* » (Bit2MeAcademy 2020). D'ailleurs, ce groupe n'est ni totalement fixe, ni totalement homogène. Au contraire, l'histoire démontre qu'il est en perpétuel recomposition et que, entre les acteurs concernés existent des différences de vues présidant à l'existence de conflits, parfois violents, comme le « Scaling Debate » en a témoigné.

### **Une technocratie soumise à consensus communautaire : entre confiance et défiance**

Malgré la décentralisation vantée de Bitcoin, ce dernier repose sur une implémentation logicielle référente et la maintenance de ces codes nécessite un groupe restreint et centralisé d'acteurs. Ce centre peut prendre un poids considérable, selon qu'il se comporte ou non comme dictateur philosophe. Et tous voient leur activité de production dépendre de la plateforme « GitHub ». Ces acteurs nécessaires disposent d'un pouvoir structurel que les *bitcoiners\** reconnaissent comme problématique. D'un côté, « *dans une perspective adverse, on ne peut pas faire confiance à GitHub* » puisque ces employés « *pourraient utiliser leurs priviléges administratifs pour injecter du code dans le dépôt sans le consentement des mainteneurs* » (Lopp 2018). D'un autre, « *la question de savoir qui contrôle la capacité à fusionner les modifications du code dans le dépôt GitHub de Bitcoin Core* » revient de manière récurrente sous la forme d'« *un "point central de contrôle" du protocole Bitcoin* » (*Ibid.*). Cette centralisation fait peser des risques importants sur Bitcoin et pourrait conduire à des « *scénarii catastrophes* » (Hasday 2020). Qu'est-ce qui empêcherait qu'un des mainteneurs décide de saboter le code du Bitcoin Core dont il a la charge ? Ou qu'un attaquant prenne le contrôle d'un compte de mainteneur afin, là encore, de saboter ces codes pour tuer Bitcoin ? D'ailleurs, les mainteneurs doivent-ils faire confiance à l'entreprise GitHub et ses employés pour ne jamais modifier arbitrairement le repo Bitcoin Core et ce qui s'y trouve ? Cette poignée de développeurs\* hautement qualifiés et d'ingénieurs informatiques ayant la charge de faire évoluer l'infrastructure Bitcoin peut apparaître comme constituant une structure de gouvernance hautement technocratique, fondée sur l'autorité d'un leader charismatique (De Filippi et Loveluck 2016, p. 15).

Lopp (2018) répond que, « *bien qu'il existe une poignée de comptes "mainteneurs" [...] il s'agit plus d'une fonction de concierge que d'une position de pouvoir* ». La position de surplomb de Bitcoin Core relève d'un point Schelling, il « *est un point central pour le développement du protocole Bitcoin plutôt qu'un point de commande et de contrôle. S'il cessait d'exister pour quelque raison que ce soit, un nouveau point focal émergerait - la plateforme de communication technique sur laquelle il est basé (actuellement le dépôt GitHub) est une question de commodité plutôt qu'une question de définition/d'intégrité du projet. En fait, nous avons déjà vu le point central du développement de Bitcoin changer de plateforme et même de nom* » (*Ibid.*). L'épisode du changement de nom a déjà permis de souligner les vues parfois opposées des « Core Devs » sur les

---

<sup>429</sup> La personne en charge allant jusqu'à influencer le seuil établi du consensus entre mineurs (en part de Hashrate du réseau) nécessaire à l'acceptation d'un Hard Fork : « *Andresen, di[s]ait que 75% des mineurs suffisent [...] tandis que les développeurs\* de Bitcoin Core aimeraient voir un "accord quasi-universel"* » (Torpey 2016, cf. section III.3.2 suivante sur ces questions).

objectifs et moyens du développement de Bitcoin. En outre, qu'un consensus émerge entre eux ou non, ces développeurs\* devront encore composer avec l'ensemble des *bitcoiners*\*, qui peuvent adhérer ou non à leurs décisions : en dernière instance, la communauté « *tranche par elle-même* » en mettant à jour ses logiciels ou non. La gouvernance *sur* le protocole de Bitcoin ne se réduit pas aux seuls développeurs\* puisqu'il existe un jeu complexe de rapports de force entre les parties en présence, relevant de l'édition de structures de gouvernance visant à réaliser des objectifs collectifs, gérer les conflits et contrôler les relations de pouvoir. C'est ce processus de gouvernance dynamique qui, en assurant la légitimité collective des actions décidées, garantit la stabilité et soutenabilité de Bitcoin.

La légitimité des modifications proposées dépend ultimement du degré de consensus qui les entoure. Au sein des communautés de CM comme Bitcoin, comme pour de nombreux protocoles Internet, cette légitimité relèverait de l'obtention d'un « *consensus approximatif* » (« *rough consensus* ») comme défini par l'« *Internet Engineering Task Force* » (IETF) (*Ibid.*, p. 18; Lopp 2018). Ce type de consensus désigne une prise de décision reposant sur « *le sentiment du groupe concernant une question particulière à l'étude* » qui « *n'exige pas que tous les participants soient d'accord, même si c'est bien sûr préférable* » (Internet Engineering Task Force 2014). Il n'est pas question d'acceptation à la majorité absolue (> 51%). L'« *absence de désaccord est bien plus importante que l'accord* », cette règle « *d'éviter les dangers de la "règle de la majorité" et de parvenir à des décisions consensuelles avec les meilleures résultats techniques* » (*Ibid.*). L'IETF précise qu'il s'agit moins de définir des processus et des procédures que de réfléchir à la façon dont sont prises les décisions (*Ibid.*).

Il nous reste à voir comment la faille Bitcoin CVE 2018 fait apparaître que ce « *consensus approximatif* » en cache différents sous-types, suivant différentes procédures communautaires pour faire évoluer les codes Bitcoin Core. Suivant le périmètre de la modification proposée, des procédures distinctes sont en place, dont les exigences asymétriques forcent à mobiliser des arènes plus ou moins locales afin de toucher tout ou partie des membres de la communauté. Que cette crise ait été déclenchée et résolue sous le sceau du secret met au jour l'existence de niveaux d'engagement variés des parties prenantes à ce consensus, au sein d'arènes de débats segmentées. Ainsi, si les acteurs précédents disposent de pouvoir sur le sous-système du répertoire GitHub « *Bitcoin Core* », les activités qu'ils y réalisent sont encadrées, et de nombreux dispositifs et arrangements visent à garantir une information et un contrôle communautaire en dernier ressort, afin de prévenir tout abus et catastrophe.

En contrepartie des pouvoirs que les mainteneurs se voient octroyer, un système de contrôle et de consignation *ad hoc* a été ajouté à celui fourni par défaut par GitHub, permettant d'assurer la traçabilité, la transparence et l'auditabilité des modifications passées : le « *système d'intégration continu basé sur des vérifications de clefs PGP de confiance* » (Lopp 2018). Il impose que toute modification des codes sources passe par un mainteneur qui doit la signer avec une clé PGP reconnue<sup>430</sup>. L'identité des mainteneurs Bitcoin Core ayant des droits d'administration est publique,

---

<sup>430</sup> Un « *pre-push hook* » existe pour garantir aux mainteneurs « *qu'ils ne poussent pas de commits non signés dans le dépôt* » et les « *commits de fusion sont optionnellement horodatés de manière sécurisée via OpenTimestamps* » (Lopp 2021). « *OpenTimestamps* » est un service de consignation et d'horodatage\* utilisant la base de données Bitcoin, permettant de certifier l'existence de données (dont l'empreinte de hash est consignée) à une date précise (celle de la publication de la transaction).

et s'y attache une clef de chiffrement PGP unique<sup>431</sup>. Toute modification des codes sources Bitcoin doit être signée par une de ces clefs PGP de confiance. Ce dispositif, en plus d'assurer que seuls les mainteneurs peuvent réaliser de telles actions, permet de retracer l'ensemble des évolutions de Bitcoin et de les lier à l'identité des mainteneurs qui y ont pris part. Ce dispositif de consignation n'assure pas en soi une sécurité parfaite : une clef PGP n'est « *pas une preuve d'identité* [, elle] pourrait être compromise et nous ne le saurions pas à moins que le propriétaire initial de la clé ne prévienne les autres mainteneurs » (Lopp 2018). Mais en tant que tel, ce dispositif rend « *plus difficile pour un attaquant d'injecter du code arbitraire* » (*Ibid.*), puisqu'il lui faudrait d'abord prendre le contrôle de ladite clef. À cela s'ajoute que lesdites évolutions de codes sont publiques et soumises à des relecteurs, pouvant être formellement reconnus, là encore afin d'assurer contrôle, traçabilité et responsabilité. En cas de constatation d'activités suspectes, les autres mainteneurs peuvent réagir et revenir aux codes initiaux grâce au système de gestion des versions.

Les dispositifs précédents ne sont pas propres aux *bitcoiners*\* : ces arrangements et pratiques existent depuis longtemps dans la production de logiciels libres. Mais, du fait de l'importance accordée à la sécurité et à l'intégrité des codes sources pour les membres de la communauté, ces derniers ont innové et offert un nouveau standard (repris par des projets comme TOR, Debian, Mozilla, etc., Wirdum 2018). Pour les *bitcoiners*\*, c'est la nature ouverte des codes sources qui permet à Bitcoin d'être sécurisé et « sans confiance » (trustless), puisque « *toute personne capable de le lire peut vérifier par elle-même s'il fait ce qu'il est censé faire* » (*Ibid.*). Les codes disponibles sur GitHub sont lisibles, car rédigés dans un langage de haut niveau. Il reste un risque fondamental, touchant tant Bitcoin que l'ensemble de la production de logiciels libres, que le « *code source ouvert n'élimine pas* (*Ibid.*) : la confiance que les utilisateurs accordent au fait que « *le logiciel qu'ils exécutent sur leur ordinateur reflète effectivement le code source ouvert* » (*Ibid.*). Comme l'explique C. Dong, Bitcoin repose sur un environnement existant (Ubuntu) qui amène « à télécharger des binaires opaques et non auditables (en d'autres termes, des "binaires de confiance") [...] ce qui nous expose à des risques de tiers », comme le fait qu'un attaquant pourrait corrompre les binaires exécutables « *de la version Bitcoin Core par une intrusion dans l'infrastructure d'Ubuntu (ou, peut-être simplement en y travaillant)* » (Costea 2019). Supprimer ce risque revient à garantir que les codes qui sont lisibles sur le répertoire Bitcoin Core sont bien ceux que l'on trouve dans les binaires du logiciel téléchargé, illisibles pour les humains. À cette problématique cruciale, la communauté des *bitcoiners*\* répond par une « *politique de sécurité rigoureuse* » : le « *Gitian Buildind* ». Ce dernier est un logiciel à code source ouvert offrant un « *environnement de construction* » (Wirdum 2018) garantissant la production et la publicisation sécurisée de logiciels : comme « *un "ordinateur dans l'ordinateur" qui fournit un espace virtuel où les binaires peuvent être compilés sans variables* » (Costea 2019). Ainsi, « *Gitian* » garantit que la compilation des binaires est exactement la même « *quel que soit l'ordinateur utilisé* » (Wirdum 2018). Ce processus garantit à tout *coiner* que le logiciel qu'il télécharge et installe sur sa machine correspond en tout point aux codes sources qu'il a audités.

---

<sup>431</sup> Sur le « repo Bitcoin Core », nous n'avons pas réussi à trouver en un seul endroit, l'ensemble des acteurs disposant de ces priviléges et leurs clefs PGP à jour, comme souligné par Awemany (2018). Sont présentes les 3 clefs PGP de confiance de W. Van Der Laan, de P. Wuille et de M. Ford (<https://github.com/bitcoin/bitcoin/blob/master/SECURITY.md>). La liste de l'ensemble des développeurs\* ayant eu des droits d'administration sur les codes sources Bitcoin put être trouvée sur un forum, voir <https://bitcoin.stackexchange.com/questions/176/is-there-a-list-of-core-bitcoin-committers> [consultation au 02/12/2021].

Mais avant qu'une modification des codes protocolaires Bitcoin n'arrive à l'étape de la production de binaires, il faut encore qu'elle ait été proposée, débattue, évaluée, voire critiquée, et amendée dans le cadre procédural en place, ce que nous étudions maintenant.

### II.2.3 Bitcoin CVE 2018 : une gouvernance de huis clos suspendue à l'absence de dissensus public

Pour un système de paiement comme Bitcoin, le fait de toucher à ses codes logiciels n'est pas un acte anodin. Nous avons vu que ses codes protocolaires dépendent de l'implémentation « Bitcoin Core », dont l'administration dépend elle-même d'une hiérarchie entre les développeurs\* de poids différents, ultimement soumis au pouvoir de la plateforme GitHub. Face aux risques posés par la présence irréductible de tiers de confiance et de priviléges hiérarchiques, des garde-fous communautaires existent. À côté des dispositifs de contrôle et consignation précédemment présentés et au gré des besoins du développement infrastructurel de Bitcoin (comme des crises rencontrées), des dispositifs, procédures et arrangements ont été institutionnalisés pour encadrer le fait de proposer, d'évaluer et de faire valider des propositions de modification des codes sources « Bitcoin Core » et ce, afin de s'assurer de leur innocuité et de construire leur légitimité. Ensemble, ces dispositifs visent à préserver la liberté individuelle des *coiners*\* quant au choix de l'implémentation logicielle qu'ils font fonctionner, incarnation matérielle et pratique des règles qu'ils considèrent comme canoniques, consensuelles et légitimes (et congruentes avec l'esprit qu'ils en attendent).

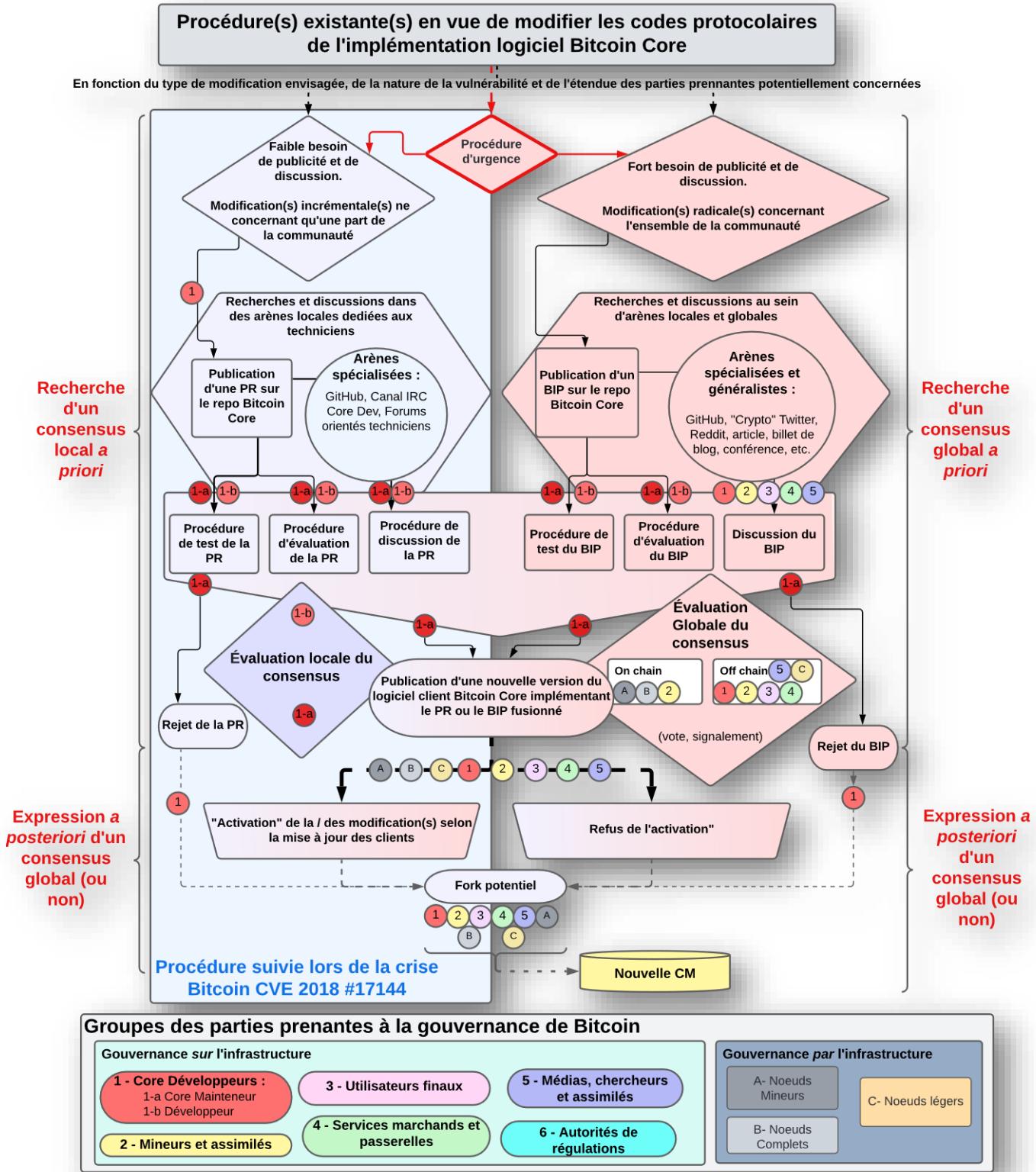
#### Maintenance ou innovation ? Deux procédures d'évolution protocolaire différencierées

Toute proposition, qu'importe sa nature, doit faire consensus en ne produisant pas de divergences d'opinions trop marquées la concernant. Néanmoins, puisque toute modification n'est pas forcément critique, et pour faciliter la maintenance des codes Bitcoin, deux types de procédures ont été mises en place qui n'ont pas les mêmes exigences : la procédure simplifiée des PR, au cœur de la crise CVE 2018, est dédiée aux évolutions considérées comme incrémentales, tandis que la procédure des Propositions d'Amélioration de Bitcoin (ou *BIP* pour « *Bitcoin Improvement Proposal* ») est réservée aux innovations plus radicales [M. Corallo, Entretien n° 15]. Ces deux procédures dessinent une frontière claire entre les modifications proposées selon qu'elles touchent ou non aux règles canoniques consensuelles et, de ce fait, qu'elles concernent tout ou partie de la communauté des utilisateurs. Toucher aux règles de consensus relève d'*« un accord très différent que, par exemple, pour une amélioration des performances de Bitcoin Core »* [Ibid.]. Du fait que chaque procédure vise à produire un consensus mettant aux prises des acteurs, des arènes (plus ou moins locales) et des modalités de publicisation hétérogènes. La Figure 12 présente synthétiquement ces procédures, leurs processus clefs, ainsi que les acteurs impliqués. On trouve les groupes de parties prenantes de la gouvernance de Bitcoin précédemment cernés, que ce soit ceux participant de la gouvernance *par* l'infrastructure (avec les nœuds\* mineurs, complets et simples), ou ceux prenant part à la gouvernance *sur* l'infrastructure (en l'espèce les développeurs\*, les mineurs et assimilés, les médias et assimilés, les utilisateurs finaux, les services de marchands et passerelles\*, et les autorités de régulation ; cf. Chap. II section II. 3.3)<sup>432</sup>.

---

<sup>432</sup> La granularité est plus faible que celle de la cartographie préliminaire (cf. Figure 7 Chap. II, section II.3.3) : seul le groupe des développeurs\* protocolaires, au centre de notre étude, est décomposé en sous-groupes. On le divise entre les « mainteneurs » ayant des priviléges d'administration sur les PR et BIP, et les « développeurs\* » qui n'en n'ont pas. Les autorités de régulation ne participent pas. Leur présence en légende ne fait que souligner qu'elles participent du cadre de la décision des acteurs de la gouvernance *sur* l'infrastructure (d'où encadré au fond du même ton).

**Figure 12 : Deux procédures différencierées permettant de modifier les codes sources Bitcoin Core**



Source : Rolland Maël

La procédure simple des « *Pull Requests* » (demandes d'extraction ou PR) encadre ce qui relèverait de la maintenance des codes protocolaires. Elle est réservée à des changements considérés comme mineurs et peu critiques, au sens où ils ne modifient pas d'éléments relevant des règles de consensus canoniques. De ce fait, ces changements ne concernent qu'une part des utilisateurs sans avoir de conséquence pour « *l'utilisateur moyen de bitcoin* » [M. Corallo, Entretien n° 15]. Le simple usager n'a aucune raison « *de se soucier de l'amélioration des performances de Bitcoin Core, ou même d'un changement d'API* [ou] dans l'interface RPC de Bitcoin Core », ces composants n'étant utilisés que par un collège restreint de super utilisateurs (les « *ingénieurs logiciels travaillant sur Bitcoin Core* » [*Ibid.*]). Tout contributeur au « *repo Bitcoin Core* » (mainteneurs ou non, 1-a et 1-b dans le schéma) peut ouvrir une PR afin de proposer des évolutions incrémentales de code. Sous réserve qu'elles en respectent les attendus formels et convainquent de leur bien-fondé les participants à la discussion, ces PR se satisfont d'un consensus local entre développeurs\*. Sans opposition, elles seront implémentées dans une nouvelle version par un « *mainteneur* ». Cette procédure est censée couvrir des modifications non ou faiblement controversées et conflictuelles : « *Vous savez, s'il y a un problème* [concernant l'un de ces composants], *nous le changeons. Qui s'en soucie ? Alors que, s'il y a un changement dans les règles de consensus [qui] affecte fondamentalement chaque utilisateur de Bitcoin [...] il est important que Bitcoin ait une sorte de processus de changement de consensus orienté vers la communauté* » [M. Corallo, Entretien n°15]. Aussi, la procédure ne prévoit pas de débat et publicisation spécifique autre que celles disponibles sur le « *repo Bitcoin Core* » GitHub et au sein d'arènes de discussion des techniciens (forums, canal IRC dédié, etc.). Une fois publiée, la nouvelle version est soumise à l'expression d'un consensus global : entre opérateurs de nœuds\* (mineurs et complets, A, 2 et B dans le schéma) qui mettent à jour (ou non) leur logiciel client et, plus globalement (et indirectement), entre les composantes communautaires (1, 3, 4 et 5) qui utilisent des nœuds\* légers (C) et délèguent donc cette mise à jour à des intermédiaires.

La deuxième procédure, celle du « *Bitcoin Improvement Proposal* », vise à encadrer l'ensemble des modifications de codes non couvertes par la procédure simplifiée précédente, c'est-à-dire les modifications protocolaires radicalement innovantes. Contrairement aux modifications incrémentales, elles sont considérées comme relativement « *critiques* », car elles touchent aux règles de consensus canoniques consensuelles : « *un utilisateur de Bitcoin [a] fondamentalement opté pour les règles de consensus de Bitcoin telles qu'elles existent* » *a priori* [M. Corallo, Entretien n°15]. Modifier ces règles est problématique. Au sein de ce type de modification, et suite à un travail de normalisation et de classification (Andresen 2012; Timón 2015; Lombrozo 2015; Lombrozo 2017), les *coiners\** distinguent (et préfèrent) les modifications étiquetée *Soft Fork\**, conçues comme rétrocompatibles avec les règles canoniques initiales qu'elles remplacent, à celles qualifiées de *Hard Fork\**, qui doivent s'imposer à l'ensemble des nœuds\* car non rétrocompatibles (cf. section III.3.3). Ces propositions de modifications protocolaires sont en elles-mêmes des crises (de plus ou moins grande intensité) où des *coiners\** proposent de remplacer « *Bitcoin* » par « *un nouveau Bitcoin* » aux caractéristiques différentes : s'y s'objectivent les attentes et désirs de tout ou partie de la communauté des *coiners\** et l'existence d'une gouvernance politique, qui réussit ou non à modifier cette gouvernance *par l'infrastructure*, *via la gouvernance sur l'infrastructure*. Car, si le WP\* décrit le consensus *par le protocole* au centre duquel Nakamoto a établi « *la preuve de travail\** [comme] *un moyen de conserver [un] consensus* », Nakamoto ne « *définit pas un moyen de transiter vers un autre consensus, c'est pas décrit cela en fait [...]* Il n'y a pas de specs d'évolution d'un consensus vers un autre [...] Et donc, pour moi l'évolution, si tu veux [...] la modification d'une blockchain, on part dans l'inconnu [,] dans des choses qui ne sont pas spécifiées » [N. Bacca ; Entretien n° 8]. Là où la procédure des PR est un dispositif que les *bitcoiners\** empruntent à la production de logiciels libres et aux forges, celle des BIP est l'institutionnalisation d'un dispositif *ad hoc* permettant de spécifier cet indéfini originel, relatif à l'évolution des règles de consensus : dès 2011,

A. Taaki (rencontré dans le Chap. I) a proposé une procédure standardisée « *permettant de proposer de nouvelles fonctionnalités, de recueillir les commentaires de la communauté sur un problème et de documenter les décisions de conception prises pour Bitcoin* »<sup>433</sup>. Puisque modifier les codes du consensus *par le protocole* que tous les *bitcoiners*\* suivent volontairement représente une révolution politique, la procédure du BIP est plus exigeante que celle encadrant les modifications incrémentales. L’acceptation communautaire renvoie à « *un seuil très très différent* » [M. Corallo, Entretien n° 15]. Comparativement à la procédure simplifiée, la production du consensus sur une évolution touchant aux règles canoniques consensuelles doit être globale, entre toutes les parties prenantes du Bitcoin : soulignée par la présence de chaque groupe aux étapes successives de la procédure - les développeurs\* (1), mais aussi les membres du groupe mineurs et assimilés (2), des utilisateurs finaux (3), des différents services marchands et de passerelles\* (4), des médias et chercheurs (5). D'où des processus impliqués par la procédure des BIP « *très différents dans le sens où, vous savez que vous avez la liste de diffusion, le processus BIP, [...] en parallèle, vous devez développer le code, le faire examiner lourdement et évidemment, cela concerne plus que vous et l'équipe Bitcoin Core, vous avez aussi besoin d'avoir un certain niveau de compréhension de si la communauté est soit en faveur, soit contre un tel changement* » [M. Corallo ; *Ibid.*]. Un BIP doit fournir une « *spécification technique concise de la fonctionnalité et une justification de cette dernière* » et sert tout à la fois à « *proposer de nouvelles fonctionnalités, [à] recueillir les commentaires de la communauté sur un problème et [à] documenter les décisions de conception prises pour Bitcoin. [...] Les BIP étant conservés sous forme de fichiers texte dans un référentiel de versions, l'historique de leurs révisions constitue la trace historique de la proposition de fonctionnalité* », et c'est son auteur qui « *est responsable de la création d'un consensus au sein de la communauté et de la documentation des opinions divergentes* » (Taaki 2011).

Les BIP sont tout à la fois un outil de proposition et d’évaluation par les pairs, un support de débats et d’amendement et, finalement, un outil de documentation et de consignation permettant d’archiver de manière transparente les différentes décisions qui ont conduit aux codes de Bitcoin reconnus par la majorité. En tant que procédure formelle, elles déplacent les problèmes sur un champ procédural ordonné et permettent de limiter la survenue de conflits personnels, voire d’attaques *ad hominem* (les développeurs\* peuvent y intervenir sous pseudonyme). Ce dispositif *off chain*\* est multifacette, relevant dans sa pratique d’une forme instituée de résolution de crises et conflits : à la formalité du BIP répond l’informalité de la « *création d'un consensus au sein de la communauté* », suivant une publicisation large au sein d’arènes de débats différenciées et de dispositifs hétérogènes permettant de mesurer l’assentiment général, *via* l’établissement de dispositifs variés à la fois *on chain* et *off chain*\*. L’étendue des changements proposés commande une publicité large. Mais si les BIP (comme les PR) sont publiés et soumis à relecture *via* le répertoire Bitcoin Core (utilisé par les techniciens), les discussions les entourant impliquent plus largement l’ensemble de la communauté. Les informations et débats, pour aller au-delà des groupes techniciens, se font par des canaux et arènes plus larges et inclusifs (« *Bitcointalk* », « *Crypto Twitter* », « *Reddit* », etc.). Les discussions « techniques » des arènes de développeurs\* sont traduites par les médias et chercheurs (5), ainsi que par chacun des membres des différents groupes et factions, à travers les débats publics, les compagnes de communication, l’organisation d’évènements, la publication d’information et de prise de position (développeurs\* (1), mineurs et assimilés (2), utilisateurs finaux (3), services marchands et de passerelles\* (4)). Quant aux dispositifs de mesure du degré d’acceptation d’une modification, ils constituent une question épineuse. Comment évaluer l’accord ou le refus des membres de la communauté alors même qu’il est impossible d’identifier ces derniers exactement ? Si le consensus *par le protocole* repose sur la PoW\*, qui permet de s’assurer de l’absence d’*attaque sybille*\*, il n’en

---

<sup>433</sup> Le BIP 0001 original décrit l’objectif et les moyens de cette procédure. Voir <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki> [consultation au 05/12/2021].

est pas de même pour ce qui touche au consensus *sur* le protocole. En dehors de la chaîne\*, rien ne permet de se prémunir contre le fait que des acteurs multiplient les comptes, pour donner à leurs propres avis l'apparence d'un consensus large (pratique dite d'« *astroturfing* » largement présente et documentée dans le champ des CM, voir Lielacher et Pickering 2020 ; Redman 2019). La mesure de l'assentiment communautaire a historiquement relevé de plusieurs dispositifs *ad hoc* s'adaptant aux situations et aux acteurs concernés : au sein de la chaîne *via* la mise en place de procédures de signalement et d'activation<sup>434</sup> accessibles aux opérateurs de nœuds\* mineurs, et aussi *via* des procédures *off chain*\* permettant de récolter l'avis des autres groupes de la communauté (cf. section III.3, dédiée à une crise « d'évolution » à gouvernance publique, qui sera l'occasion de traiter ce type de dispositifs).

Ainsi, les deux types de procédures d'évolution de Bitcoin assurent la production d'un consensus, mais leurs formes diffèrent. Là où un BIP impose de mobiliser l'ensemble des composantes communautaires de Bitcoin, la procédure simplifiée des PR, elle, déroge à ce principe de publicité large des débats et se satisfait d'un consensus essentiellement local entre spécialistes.

### **Gouvernance de huis clos : consensus local *ex ante* entre une poignée d'acteurs en réseau\***

Comme nous l'avons vu, la faille Bitcoin CVE 2018 illustre une face importante de la gouvernance de Bitcoin : sa forme de huis clos. La procédure des PR, au cœur de l'activité quotidienne de maintenance infrastructurelle de Bitcoin et ouverte aux évolutions incrémentales, se satisfait d'un consensus local. Et toutes les modifications ayant concouru à cette crise, qui ont introduit les failles ou qui ont plus tard cherché à les corriger, relevaient de cette procédure et non des BIP (cf. Figure 13). L'étude de la crise Bitcoin CVE 2018 permet de retracer les canaux de communication mobilisés dans le cadre de la procédure simplifiée. Tous reflètent la publicisation faible, cantonnée à la communauté restreinte des « super utilisateurs » (Github, canal IRC ; Tableau 8 ci-après).

---

<sup>434</sup> Ces procédures d'activation évoluent au gré des besoins et « les propositions de nouveaux mécanismes d'activation de Soft Forks sont souvent conçues pour éviter les problèmes rencontrés lors de Soft Forks précédents » (Optech 2021). Par exemple, la BIP 0009 mise en place en 2015 permet de définir un laps de temps (exprimé en nombre de blocs) après lequel une mise à jour sera enclenchée à condition qu'elle ait reçu le soutien de suffisamment de nœuds\*. La temporalité comme le quorum devant être définis dans la proposition BIP. Voir <https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki> [consultation au 06/12/2021]. D'autres procédures de ce type seront implémentées comme pour le BIP 0034, le BIP 0066 ou le BIP 0065, Optech (2021) qui fournit un aperçu des procédures d'activation historiquement notables.

**Tableau 8 : Les différents canaux d'information et de discussion mobilisés lors de la crise CVE 2018**

| Type de canal d'information mobilisé  | Canaux informationnels dégagés lors de notre enquête  | Caractéristiques   |
|---------------------------------------|---|--|
| <b>Canal de sécurité Bitcoin Core</b> | « Page contact Bitcoin Core <sup>435</sup> » : transmission du rapport de divulgation responsable à P. Wuille, G. Maxwell & W. Van der Laan, de l'équipe Bitcoin Core (Bitcoin Core 2018a; Awemany 2018)  | Canal de sécurité formel et privé indiquant les acteurs à contacter (adresse mail et clef PGP).  |
| <b>Canaux privés divers</b>           | P. Wuille transmet le rapport à C. Fields, S. Daftuar, A. Marcos et M. Corallo (Bitcoin Core 2018a). M. Corallo le trouve sur son bureau à « Chaincode labs » et en discute avec ses collègues Marcos et Daftuar [Entretien n° 20]                      | Canaux d'information informels et privés permettant la coordination des acteurs participant à la remise en ordre (importance du capital culturel des acteurs comme de leur capital social) |
|                                       | Prise de contact téléphonique entre M. Corallo et les CEO et CTO de la <i>pool</i> de minage « Slush pool » ; J. Newbery et J. O'Beirne sont informés par M. Corallo de la faille et contactent « différentes entreprises du secteur » ( <i>Ibid.</i> ) |  |
|                                       | N. Bacca reconnaît avoir connaissance d'un problème par une connaissance avant même la divulgation publique [N. Bacca, Entretien n° 8]  |  |
|                                       | Les échanges sur le canal IRC du 18 septembre 2018 démontrent que Luke Dashjr a connaissance du bogue et qu'il est en charge de signaler la vulnérabilité à l'autorité d'identification CVE (voir ci-après)   |  |
| <b>Canaux publics divers</b>          | Répertoire « Bitcoin Core » sur « Github »: échange concernant la faille et les correctifs ( <i>Ibid.</i> ; Awemany 2018)   | Canaux d'information formels et informels majoritairement publics permettant une publicisation large en direction de l'ensemble de la communauté   |
|                                       | Canal IRC #bitcoin-core-dev (freenode, 18/09) : Luke Dashjr, qui n'apparaît pas dans la divulgation complète, écrit sans plus de précision : « Pour ce que ça vaut, j'ai obtenu le CVE 2018 17144 pour cela »   |  |
|                                       | Publication de la divulgation complète par « Bitcoin Core » sur le site Bitcoin Core (Bitcoin Core 2018)  |  |
|                                       | Publication d'informations : billet de blog, podcast/vidéo, etc. (Song 2018 ; Awemany 2018 ; Bitcoin Q&A 2018 ; jnewberry-cve-2018-17144-bug ; Straw Hat 2019)  |  |

Source : Rolland Maël

La publicisation du bogue CVE 2018 ne fut ni totale, ni réalisée d'un seul coup, ni directement à l'adresse de la communauté dans son ensemble. Pendant les phases d'évaluation du problème et de développement/test de solutions correctives et jusqu'à la publication du rapport de divulgation complète par l'équipe Bitcoin Core, le bogue de « faux monnayage » est dissimulé et seule la faille DOS est publique (Bitcoin Core 2018 ; Entretien n° 15). Cette logique de rétention/libération graduelle de l'information renseigne sur les liens existant entre les acteurs impliqués. Les informations furent d'abord partielles et tournées vers des réseaux\* d'acteurs ayant la confiance des développeurs\* Bitcoin Core. Ce n'est que durant la phase de résolution, à la suite du dépôt public des correctifs sur GitHub, puis par la publication du rapport de divulgation complète, qu'un

<sup>435</sup> <https://bitcoincore.org/en/contact/> [consultation au 08/12/2021].

consensus global entre tous les *bitcoiners*\* a pu se former, via la mobilisation de canaux publics et non plus privés.

Dans le cadre de cette gouvernance de huis clos, la phase d'évaluation n'a impliqué qu'une poignée d'acteurs en réseau\* aux liens forts. Sur le « repo Bitcoin Core », l'enquête fait ressortir que le nombre de contributeurs, bien qu'en augmentation, reste relativement restreint et cantonné au même groupe d'intervenants en ce qui concerne les activités critiques (moins d'une vingtaine d'acteurs impliqués dans les PR recensées). Nos entretiens avec des acteurs aux compétences techniques reconnues sur Bitcoin, au sein de la communauté parisienne [Anon 1, 2, 3 et 4] ou plus globalement dans la communauté Bitcoin élargie [J. Song, M. Corallo, A. Le Calvez] démontrent que, bien que formellement ouvertes à tous, ces activités ne sont accessibles qu'à certains : à l'exception de Corallo et Song, tous les acteurs rencontrés se déclarant codeurs Bitcoin reconnaissent n'avoir jamais réalisé d'activité de code, voire de relecture, car ils « *ne maîtrisent pas* » suffisamment le langage de programmation\* de Bitcoin Core (cf. le C++, Chap. I) : « *je le lis comme ça, je peux comprendre ce que ça fait mais de là à review vraiment...* » [S. Roche ; Entretien n°23 ; idem pour Anon 1, 2, 3, 4 et L. Thiébaut]. Au-delà des statuts formels dégagés entre « Core Devs » (cf. Core mainteneur et développeur\* simple), d'autres plus informels existent suivant les activités et compétences impliquées. Au sommet, les plus compétents participent de la catégorie des « chercheurs », car « *des idées, par exemple Segwit, il faut bien avoir quelqu'un qui a eu l'idée et qui la vendre aux autres* » [A. Le Calvez, Entretien n° 20]. Song s'exclut de cette catégorie, car tout le monde n'est pas en capacité de « *dire "oui, nous devrions faire ceci ou cela"* [...] , d'avoir assez d'influence pour pouvoir le faire,[et] la plupart des personnes qui parlent de ces choses sont impliquées depuis plusieurs années. » Lui se voit, avoir le « *rôle [d']un éducateur [ :] je prends ce qu'ils disent et puis j'interprète pour les gens qui ne comprennent pas vraiment. [...] Je suis plus un enseignant qu'un chercheur* » [J. Song ; Entretien n° 17]. Ces chercheurs à la P. Wuille (à qui l'on doit la BIP SegWit) sont les « super codeurs » qui ont la confiance des *bitcoiners*\*<sup>436</sup>. Cette confiance n'est jamais donnée, il faut des membres, comme Song, plus nombreux à la base, pour assurer relecture, traduction et vulgarisation. D'ailleurs, ce cadre procédural ordinaire évolue et s'intentionnalise afin d'assurer qu'un travail minimum sur chaque PR soit réalisé : la relecture par les pairs est ainsi passée de l'informalité des contributions volontaires à un dispositif d'assignation formel de relecteurs (ce qui apparaît pour les PR #9049, #10195 et #10537, Figure 9 précédente ; rapporté aussi par S. Roche ; Entretien n° 23].

Corallo [Entretien n°15] fait aussi partie des chercheurs peu nombreux, comme ses collègues de bureau avec qui il partagea la découverte du rapport de divulgation responsable. Et seuls ces chercheurs arrivent, tant bien que mal, à se faire financer. Le financement des personnes en charge de la maintenance et de la sécurité de la couche protocolaire de Bitcoin est « *un problème [...] intéressant [...] à regarder* » : malgré la valeur générée, il n'y a finalement que « *très peu de gens en fait, dans les boîtes autour de l'écosystème, qui sont impliqués dans les couches protocolaires, en tout cas sur Bitcoin [ :] Ethereum c'est un peu l'exception avec Consensys [et] la fondation Ethereum [en comparaison] Blockstream [...] c'est ce qui pourrait se rapprocher le plus [...] d'un truc comme l'Ethereum Foundation dans le monde de Bitcoin* » [N. Bacca, Entretien n° 8, rejoint par Léa Thiebaut, Entretien n° 21]. Rapporté à d'autres projets à codes sources ouverts, ce problème structurel s'expliquerait par l'absence d'*« une culture qui va fonctionner un petit peu comme tu peux avoir sur Linux aujourd'hui. Les choses s'y sont extrêmement professionnalisées et au final tu as toutes les grandes distributions qui participent aussi au noyau. Tu n'as pas du tout cette équivalence en fait aujourd'hui dans les cryptomonnaies\**. Donc tu as extrêmement peu [...] de développeurs\*

---

<sup>436</sup> « In Super Coders We Trust », voir <https://twitter.com/APompliano/status/1420095187578195974?s=20> [consultation au 01/01/2022].

*Bitcoin sur le... au niveau du protocole et du consensus qui sont dans une boîte. »* [N. Bacca, Entretien n° 8]. À l'exception de l'entreprise de Corallo et ses collègues, « ChainCode labs », ou encore de « Blockstream », explicitement tournées vers la recherche et le développement de Bitcoin qui leur offrent des contrats de travail en vue de financer leurs travaux sur Bitcoin Core<sup>437</sup> (BitMEX Research 2020a), bien peu nombreux sont les développeurs\* Bitcoin à pouvoir en vivre [Stéphane Roche, Entretien n° 23].

Justement, le contact que Corallo ouvre avec Slush Pool relève de ces liens forts entre les personnes et les organisations dont elles sont membres : Slush Pool développe le protocole de minage Stratum V2 sur une idée originale de Corallo de ChainCode Labs (Wirdum 2019). De fait, de ces liens existants, « *Slush Pool est beaucoup plus facile et plus fiable à contacter, que beaucoup de... pools chinois [, à cela s'ajoute] aussi le fuseau horaire, c'était... un fuseau horaire raisonnable pour l'Europe, ce n'était pas un fuseau horaire raisonnable pour la Chine.* » [M. Corallo, Entretien n° 15]. Si les codeurs se font législateurs, l'application de la loi nécessite les mineurs, d'où ce contact privilégié avec une pool amie, où ils sont invités à participer aux débats privés en qualité d'experts de confiance.

Ainsi, c'est au cours d'une discussion confinée qu'un premier consensus *ex ante* sur la validité et la légitimité des correctifs s'est construit au sein d'un collège restreint d'acteurs et en dehors des canaux d'information publique. La production et la mesure du consensus entourant ces modifications se sont limitées à l'absence d'opposition frontale des participants, sachant que, dans le cadre de cette procédure, les conflits sont rares, voire inexistant<sup>438</sup>. D'où des PR fusionnées dans la branche principale du répertoire pour être implémentées dans une nouvelle version logicielle : ces changements sont « *rapidement considéré[s] comme bon[s] dans l'examen par les pairs, ACKed dans le langage du Core* » (Awemany 2018). Mais cela n'est pas suffisant ! Encore faut-il qu'un consensus communautaire large soit réalisé *ex post*, alors même que lesdits correctifs touchent aux règles canoniques consensuelles de Bitcoin.

### **Unanime et inaperçu : l'Audience Publique sans vague d'une crise et sa résolution**

La crise Bitcoin CVE 2018 n'est ni la plus controversée, ni la plus politique, donc - en théorie - pas la plus intéressante au sens de Callon (2006). Cet auteur a montré l'importance des controverses et conflits, comme « *épicentre* » et « *point de fusion* » où la « *technique prend forme* »,

---

<sup>437</sup> « *C'est tous des gens qui sont de leur côté, qui font des trucs, tu peux en avoir quelques-uns chez Blockstream mais c'est... et même, enfin je veux dire, Blockstream aujourd'hui je considère que c'est plus une boîte de recherche, tu vois* » [N. Bacca, Entretien n° 8]. Blockstream faisait partie des sponsors des événements « Breaking Bitcoin » (Observation participante n° 14 et 25, Annexe n° IV.2), dont l'une des organisatrices nous apprend que « Chaincode Lab » organise aussi des formations « *sur plusieurs semaines de “relecture” (“review”) autour de la proposition de modification “Taproot”* ». [...] Organisé par des core dev [...] Et en fait c'était sur 7 semaines normalement, c'était quatre fois par semaine, 40 heures par semaine. J'ai arrêté parce que c'était trop... trop chronophage, j'étais un petit peu larguée et en fait c'était une review avec toutes les semaines un sujet différent sur un petit peu de tout : “Taproot”, “Grassroot”, “Schnorr”, “MAST” [...]. On était 160 au début, je crois que ça a terminé avec beaucoup moins [...]. J'étais déjà extrêmement contente que leurs initiatives au groupe 160 personnes, j'ai trouvé que c'était vraiment génial, ils ont organisé ça mais de manière incroyable, les mails, les machins... on sentait vraiment qu'il y avait un énorme investissement de la part des organisateurs pour faire en sorte de rendre le travail fluide pour tout le monde ».

<sup>438</sup> Questionné sur l'apparition de conflits entre développeurs\* suite à de simples PR ou à des BIP, M. Corallo nous répond : « *Vraiment pas... Vous savez, en général il y a très très peu de conflits, voire aucun. Vous savez, évidemment il y a beaucoup de discussions couvrant les changements [/] il y a des demandes de Pool Request et les gens ont beaucoup à dire sur les choses mais [...] ce n'est jamais vraiment litigieux [...]. En général, relativement, très peu de conflits dans ce domaine. [...] Quand vous regardez les changements du système de consensus et que toute la communauté doit être d'accord, il y a eu des conflits, mais en termes de changements du logiciel de base de bitcoin, il n'y en a vraiment pas beaucoup.* » [M. Corallo, Entretien n° 15]

mais s'il reconnaissait que les controverses « *ne manquent pas* », pouvant « *surgir de partout* », leur choix nécessiterait une attention particulière (*Ibid.*, p. 2-3). Se libérer « *d'un monde préconstruit* » impose de trouver des controverses « *suffisamment ouverte[s] dans l'[es]quelle[s] les négociations sont multiples, la nature des choix est encore discutable, les acteurs impliqués nombreux et variés, les exclusions non définitives* » (Callon 2006, p. 4). Une « bonne » controverse se définit par quatre caractéristiques (*Ibid.*, p. 5) comme pour celles entourant les véhicules électriques légers (VEL) : la controverse portait bien « *sur un objet technique [...] non réductible à de la pure technique* », car différents types d'argumentaires (scientifique, économique, etc.) disputent continuellement les arguments techniques ; « *les solutions envisagées étaient bien multiples* » et renvoient à des problématiques différentes suivant les acteurs, « *les groupes sociaux impliqués et leurs intérêts [y étaient] aussi nombreux et variés que possible* », ce qui conduit certains acteurs à privilégier certaines problématiques au détriment d'autres. Enfin, « *les forces qui s'opposent [...] s'équilibrivent en permanence* », ce qui « *rend peu efficaces les arguments d'autorités [,] permet à la controverse de demeurer ouverte* ». Et si certains acteurs parviennent à faire triompher leur voix (et à faire taire celles des autres), celle-ci peut-être bien « *vite contesté[e] et débordé[e] de tous côtés* » (*Ibid.*, p. 5). Sur ces critères, seul le premier est activé dans notre cas. Bitcoin est un objet socio-technique et ses règles canoniques consensuelles, ainsi que les discussions entourant leurs définitions/modifications, ne se réduisent pas à de simples problématiques techniques : le monnayage, comme les règles encadrant les transactions\* – vérification et sanction des doubles dépenses – relève bien de justifications et de négociations hybrideant des argumentaires économiques, techniques, philosophiques. De ce fait, cette crise apparaît plus comme une crise « *post-technologique* » où Bitcoin est déjà « *réifié* » en bonne partie (*Ibid.*, p. 4)

Si l'absence de débats et controverses durant la crise peut s'expliquer par la confidentialité de la remise en ordre, la persistance de cette absence après la divulgation complète éclaire la question de la nécessité d'un consensus communautaire *a posteriori*. Il s'y joue la reconnaissance de la légitimité des actions secrètes et discrétionnaires, construite dans l'épreuve. Nous en voulons pour preuve le bouleversement explicite des représentations de certains *bitcoiners\** suite à cette crise : « *au début, j'étais de ce côté-là* [de l'interprétation rigoriste du « *Code is Law* » à la Szabo, NDA]. *En effet, ben si le code dit cela, il va se passer cela. J'étais encore de ce côté-là pendant la "CVE 2018 je ne sais plus quoi là" ... je me suis dit, ben finalement si quelqu'un avait exploité cela, est-ce qu'il aurait fallu accepter ou pas les changements ? Je me suis dit bon... il a fait ça, ok... Pareil avec "The DAO", avec le temps je me dis qu'il y a quand même un consensus social. "Code is law as long as people don't mind"* » [A. Le Calvez, Entretien n°20]. Cette citation montre l'évolution et la formation d'un consensus sur le fait que la lettre du code ne peut à elle seule prétendre à être « *loi* » : la déférence au code et la légitimité des interactions réalisées au sein de la chaîne renvoient d'abord à des interprétations humaines.

D'un côté, les versions logicielles vulnérables publiées (et celles implémentant les correctifs) peuvent être conçues comme des évolutions radicales de type *Fork\**, car elles touchent aux règles consensuelles canoniques pour tout *bitcoiner* (Hacker News Forum et Apo 2018, rejoint par Awemany 2018). Du côté des *bitcoiners\**, ces changements non anticipés n'ont pas été consciemment implantés, d'où la qualification en termes de vulnérabilité. En tant que crise « *de vulnérabilité* », la déviance est explicite pour les *bitcoiners\**, les codes vulnérables permettant des actions considérées *a priori* comme illégitimes. Personne, de Nakamoto aux autres *bitcoiners\**, n'a imaginé que le faux monnayage et la double dépense puissent être légitimes. Aucun doute chez les acteurs : les comportements de double dépense permis par les versions 0.15.x-0.16.x, comme le faux monnayage induit, ne relèvent ni de la lettre du code acceptée (les règles contenues et rendues exécutoires par les versions précédentes), ni de son esprit. D'où un consensus sous la forme d'une absence de dissensus, exprimée à la fois par la mise à jour rapide vers les versions corrigées par les

opérateurs de nœuds\* vulnérables et l'absence notable de débats et conflit intracommunautaire entourant cette crise et sa révélation publique finale. Au cœur de la résolution de cette crise, pas de controverse technologique, au sens de Callon (2006, p. 5) : *les solutions envisagées* ne furent pas *multiples* et la remise en ordre peu complexe. Il a suffi de réintégrer les vérifications de validité qui avaient été supprimées, car considérées à tort comme redondantes. En outre, *les groupes sociaux impliqués et leurs intérêts* n'y étaient pas *nombreux et variés*. Enfin, difficile d'y voir un *équilibre de force* en opposition permanente : ni la mise en crise, ni la remise en ordre n'ont conduit à des controverses à l'intérieur de la communauté Bitcoin. Les critiques extra-communautaires sur la gravité et la gestion irresponsable des « Core Devs » proviennent principalement de ceux qui ont subi la défaite du « Scaling Debate », les membres de la communauté « Bitcoin Cash », et apparaît une tentative de réactiver la controverse : « *600 microsecondes* », c'est « *le temps que Matt Corallo voulait rogner sur la validation\* des blocs avec sa Pull Request de 2016 sur Bitcoin Core* » alors que, à l'époque, d'autres solutions proposées par les *Big Blockers* permettaient des gains de propagation plus importants (Awemany 2018). Néanmoins, pour les *bitcoiners\**, ces questions sont closes, les critiques exprimées ne visent qu'à « *gonfler hors de [leurs] proportions* » les conséquences de cette crise afin de « *faire paraître ce bug pire pour que [Bitcoin Cash] ait l'air meilleur* » (McCormack et Song 2018). Suite à la divulgation complète, la communauté Bitcoin reconnaît sa gravité potentielle, mais ne le fait qu'en soulignant sa faible gravité réelle (Song 2018, Antonopoulos 2018) et en se félicitant des conditions dans lesquelles les « Core Devs » ont rapidement conduit la remise en ordre : « *ce qu'il faut regarder, c'est la gravité des bogues (celui-ci était grave), la rapidité avec laquelle ils sont corrigés, s'ils sont exploités avant d'être corrigés ; s'ils le sont, quelles sont les conséquences à long terme et s'ils ont un impact durable. [...] Les systèmes [de réponse] sont [déployés] lorsque les choses tournent mal, et le système continue de fonctionner. [Ce bug] n'a pas tué Bitcoin, il l'a rendu plus fort, ce qui est l'un des aspects de Bitcoin qui... continue de me surprendre, dans sa résilience* » (Antonopoulos 2018). Cette crise Bitcoin CVE 2018, en tant que crise « de vulnérabilité » à gouvernance de « huis clos », présente l'intérêt d'éclairer la « micropolitique » qui est au cœur de la maintenance des codes de Bitcoin. Elle permet de décentrer l'analyse vers les activités quotidiennes de maintenance, qui, du point de vue des acteurs, paraissent moins critiques, et relèvent d'une gouvernance routinière et normalisée.

L'absence de dimension vraiment critique, politique et conflictuelle de la crise Bitcoin CVE 2018 se mesure à l'aune de sa faible connaissance dans la communauté des *coiners\**. Cette crise est loin d'avoir donné lieu à la même quantité d'analyses et de commentaires que les « crises d'évolution », dont le « Scaling Debate » est emblématique (cf. Chap. II, section II.3.3). La crise est une affaire de visible et d'invisible, plus exactement de visibilisation et d'invisibilisation. L'histoire des crises « de vulnérabilité » *aconflictuelle* de Bitcoin (cf. Chronologie 4) est donc en général mal connue des membres de la communauté. Les *bitcoiners\** rencontrés méconnaissent aussi bien la dénomination de la faille que ses caractéristiques et enjeux, son déroulé et les conditions de sa résolution. À la question type de savoir quand et comment nos intervenants ont eu connaissance de cette faille, les réponses révèlent que ce « *CVE 2018 je ne sais plus quoi* » [A. Lecalvez, Entretien n° 20] a laissé peu de traces dans la mémoire des *bitcoiners\**. S. Gouspillou [Entretien n° 17], n'ayant aucune connaissance de cet événement, nous redirigera vers Jean-François Augusti, le CTO de son entreprise ayant à charge ce type de problématique technique. Ce dernier nous répond : « *Houla, pas du tout [...] ben écoute, non, non, non, je regarde en même temps que tu m'en parles. J'en ai peut-être entendu parler alors, mais cela ne m'a pas du tout... j'ai pas du tout percuté.* » [J.-F. Augusti, Entretien n° 18]. Même connaissance imprécise de la part de M. Phuc : « *alors attends, qu'est-ce qui s'est passé ? Rafraîchis-moi la mémoire.* » [...] « *Ça, je me souviens, c'est assez marrant parce que... [...] tu vois, tu as dû me le remémorer. Mais je me souviens que cela ne m'avait pas beaucoup marqué [...], bon même si on avait traité évidemment le sujet [dans le Journal du Coin, NDLR].* » [Entretien n° 19]. S. Roche abonde : lui aussi a « *dû vérifier lequel c'était [...]* »,

tout en reconnaissant n'avoir pas vraiment « creusé » la question bien qu'il en ait pris connaissance à l'époque : « *Ouais [...] j'ai lu l'annonce pour comprendre de quoi il s'agissait.* » [Entretien n° 23]. L. Thiébaut, elle non plus, n'est « *pas sûre de l'avoir vu passer celle-là* » et d'ajouter : « *si tu veux, j'en ai pas entendu parler de cette faille parce que j'ai l'impression qu'elle n'a pas fait trop parler d'elle...* ». En même temps, elle nous « *avoue, [que] les CVE [, elle] ne les suit pas trop, parce que [...] une fois que c'est publié, c'est trop tard pour que cela soit marrant [elle rigole un peu]* » [L. Thiébaut, Entretien n° 21].

La crise Bitcoin CVE 2018 « *n'a pas fait trop parler d'elle* » [*Ibid.*], car, par construction, les crises « de vulnérabilité » n'impliquent pas de dissensus communautaire. Dans le cas contraire, la gouvernance de huis clos dégagée se transforme en gouvernance ouverte et publique. L'histoire des crises Bitcoin présentée dans la Chronologie 4 le montre : certaines mises en crise ou remises en ordre passent par la procédure des BIP (différenciée des PR dédiées à la maintenance) et peuvent être moins consensuelles, comme l'illustre, pour Bitcoin, le « Scaling Debate » ou l'épisode du HF d'Ethereum consécutif à l'attaque de « The Dao », que nous allons étudier à présent.

### III.3 UNE GOUVERNANCE PUBLIQUE D'EXCEPTION : LE *HARD FORK* D'ETHEREUM CONSÉCUTIF À L'ATTACQUE DE « THE DAO »

Jusqu'à présent, notre enquête au cœur des crises protocolaires de Bitcoin a pointé l'existence d'une gouvernance de crise à double face, qui va avec la définition d'une nomenclature de « pathologies » mais aussi d'acteurs, de lieux, canaux, procédures et dispositifs d'interactions, de contention et de remédiation. À l'image de son développement, la gouvernance de Bitcoin et des CM est également carnavalesque. Elle se fait théâtre où se jouent des drames complexes, mêlant secrets bien gardés et débats publics enflammés. La crise Bitcoin CVE 2018 a principalement attiré l'attention sur la gouvernance de huis clos - les coulisses - que nous avons pu documenter et analyser. Cette face routinière de la gouvernance *sur* le protocole et la centralité, qui prend le groupe restreint des « Core Devs », a déjà été saisie et analysée par d'autres auteurs qui concluent à une gouvernance fondée sur « *une structure de pouvoir hautement technocratique* », sise sur une logique « *autocratique-mécanique* » avec « *des élites excessivement centralisées* » autour d'un « *dictateur philosophe* » (De Filippi et Loveluck 2016, p. 12-13 ; cf. Chap. II section I.3.3). L'analyse de la gouvernance *sur* l'infrastructure d'une CM ne peut s'arrêter à cette face. La gouvernance de huis clos est toujours suspendue à l'absence de dissensus communautaire, dont la gouvernance ouverte et publique est le contrepoint nécessaire, qu'il nous reste à analyser.

Des acteurs ont ainsi critiqué des analyses qu'ils considèrent comme partielles<sup>439</sup>, voyant dans cette vision d'une administration des codes Bitcoin comme « *point de contrôle unique [,] un faux-fuyant qui découle d'une perspective autoritaire* » (Lopp 2018). À ces critiques, les *bitcoiners*\* répondent qu'une épée de Damoclès pèse sur toute tentative d'imposition discrétionnaire de code que la communauté jugerait contraire à ses intérêts : la « *liberté de l'open source* » offre à « *quiconque est insatisfait du projet Bitcoin Core* » ou « *en désaccord avec les "mainteneurs"* », la liberté de lancer le sien en propre, en partant de zéro ou en « *Fork\*ant* » les codes existants. L'administration du répertoire « *Bitcoin Core* », en tant qu'il est un système de ressources (Hess et Ostrom 2007) essentiel de la gouvernance *sur* l'infrastructure, serait substituable par d'autres, qui

---

<sup>439</sup> Lors de notre enquête de terrain et de nos entretiens, plusieurs acteurs nous ont fait part rapidement de l'avis négatif qu'ils pouvaient avoir sur des travaux académiques traitant de Bitcoin et des CM, en citant particulièrement ces travaux. Cf. Introduction générale, section C. 1 et note 46.

pourraient assurer des fonctions similaires : le travail des développeurs\* (et les productions/unités de ressources qui en résultent, peuvent être déplacées vers « *un dépôt différent sur lequel les mainteneurs de Bitcoin Core n'auraient aucun privilège administratif* » (*Ibid.*). C'est cette possibilité toujours ouverte aux *bitcoiners*\* de s'opposer à des modifications non consensuelles par le *Fork*\*, qui leur garantirait en dernier ressort de conserver la souveraineté du choix des règles canoniques consensuelles qu'ils suivent. Si notre propre travail souligne la structure technocratique du sous-système de ressources qu'est le répertoire Bitcoin Core, impossible d'en tirer des conclusions. Encore faut-il éprouver l'affirmation que les « Core développeurs\* » disposent plus d'une « *fonction de concierge [que d']un poste de pouvoir* » (*Ibid.*), ce qui nécessite de voir en action l'ensemble des règles et dispositifs précédents qui visent à le garantir. Faire ce travail était difficile pour De Filippi et Loveluck (2016) : analysant un « Scaling Debate » encore en phase d'insémination, ils n'avaient pas accès aux matériaux de la remise en ordre sous forme de schisme de 2017. Ces matériaux ont étayé l'idée que les pouvoirs étaient concentrés dans l'espace des priviléges/faisceaux de droits que les mainteneurs ont sur le répertoire « Bitcoin Core » et que ces derniers se muent en autorité, que peuvent reconnaître ou refuser les acteurs des autres sous-systèmes imbriqués participant de la gouvernance *sur* l'infrastructure Bitcoin. Routinièrement, la reconnaissance de cette autorité se fait tacitement et sans ambages, comme avec le cas Bitcoin CVE 2018. La situation diffère avec les crises « d'évolution » qui conduisent inéluctablement à des débats, voire des conflits, eux, résolus sur une « grande scène » *via* une gouvernance publique. C'est lors de l'expression rare et intermittente de cette seconde face de gouvernance que les acteurs des autres sous-systèmes de ressources (minage, services marchands et passerelles\*, utilisateurs finaux, médias et chercheurs) se parent des costumes du contre-pouvoir, et que l'ensemble des mécanismes communautaires de contrôle visant à assurer la production de consensus (et d'expression du dissensus) est mobilisé (comme la procédure des BIP, décomposée dans la Figure 12 précédente, l'illustre).

La crise du « Scaling Debate », építome d'une controverse technologique à la Callon (2006, p. 5, cf. Encadré n°4 Chap. II, section II.3.3) est emblématique de l'ontologie politique de Bitcoin : son dénouement par schisme protocolaire et communautaire a révélé les tensions en valeurs, ainsi que des attentes monétaires hétérogènes au sein de sa communauté. Mais Bitcoin, pour une fois, ne fut pas pionnier avec cette crise à gouvernance *publique*. C'est Ethereum qui a été le premier champ de bataille de ce type de guerre communautaire et protocolaire, avec le *Hard Fork*\* consécutif à l'attaque de « The DAO ». Ces deux crises partagent le fait de revêtir les caractéristiques d'une controverse technologique et un dénouement sous forme de schisme/*Fork*\* à la suite d'un conflit entre des visions antinomiques de ce que doit être l'objet monétaire, donc concernant les modifications de code désirables. Une première section reviendra sur les conditions brutales, publiques et tapageuses de la mise en crise. Puis, nous analyserons les conditions complexes, contraintes et controversées de la remise en ordre. Outre les enjeux débattus de la crise et ses conséquences, ainsi que des voies de remédiation souhaitables, nous ferons ressortir les grands traits de la gouvernance *publique* mobilisés durant cette crise. Nous reviendrons enfin sur la remise en ordre, qui produira un schisme protocolaire et communautaire surprise démontrant que, pour ces communautés de paiement, les *Forks* sont des moyens de retrouver, par sécession monétaire, le semblant d'homogénéité en valeurs que la crise avait fait voler en éclat.

### III.3.1 Une mise en crise brutale, publique et tapageuse

Au-delà de sa proximité avec la crise du « Scaling Debate », ce sont ses différences qui nous conduisent à choisir la crise du *Hard Fork*\* d'Ethereum consécutive à l'attaque de « The DAO » comme deuxième terrain d'enquête. Tout d'abord, de 2015 à 2017, nous avions été témoin de nombreuses crises, de différentes importances, ayant touché l'écosystème des CM, dont les débats

et conflits consécutifs à ce problème de *débit*\* de Bitcoin. Nos premières réflexions sur la gouvernance de l'infrastructure Bitcoin (Rolland et Slim, 2017) puisent leur origine dans la controverse du « Scaling Debate ». Nous marchions dans les pas des travaux de De Filippi et Loveluck (2016), tout en souhaitant les actualiser et les préciser. Nous avions aussi découvert Ethereum peu après son lancement et participé aux premières ICO associées, dont celle très médiatique de « The DAO ». « The Dao » est un fonds d'investissement distribué sous forme de *smart contract*\*, dont un attaquant réussit à dérober une bonne part de la trésorerie. Cette situation conduit la communauté à se déchirer sur l'opportunité d'y remédier par un *Hard Fork*\*, une intervention discrétionnaire sur le protocole décriée chez les *coiners*\*. Ensuite, la crise d'Ethereum, en tant que pionnière, fait précédent et s'érite comme fondatrice : elle a participé à « créer l'Ethereum tel qu'il est aujourd'hui [et] une grande partie de la crypto telle que nous la connaissons aujourd'hui n'existerait pas » sans elle (Morris 2023 ; ce que souligne aussi V. Zamfir, Entretien n°9). Elle apparaît « *a posteriori* [comme] un moment historique qui aura des implications, très lointaines dans l'histoire de la création des concepts dans le numérique » [A. Roussel, Entretien n°11]. Le dénouement même du « Scaling Debate » n'est compréhensible qu'à la lueur de ce précédent dont les *bitcoiners*\* sont imprégnés (ce qui explique d'ailleurs pourquoi ils sont aussi nombreux à avoir un avis critique sur cette crise et sa gestion). La crise de « The DAO » est au cœur de la controverse entre *bitcoiners*\* et *etheristes* sur les questions de gouvernance de CM. Pour les premiers, la gouvernance d'Ethereum y apparaît frappée du sceau infamant de la centralisation et de la discréption, autour du fondateur Buterin et de la Fondation Ethereum. Notre choix d'étudier la crise « The DAO » provient aussi d'un accès au terrain facilité. À l'opposé d'un « Scaling Debate » trop vaste par le nombre de participants, ou de solutions proposées et dispersées dans sa temporalité, cette crise était plus accessible, car circonscrite, et nous y avions pris part en tant qu'usager (voir Immersions participantes, Annexe n°IV.1.). La singularité de cette crise apparaîtra dans la présentation de sa périodisation que nous allons aborder.

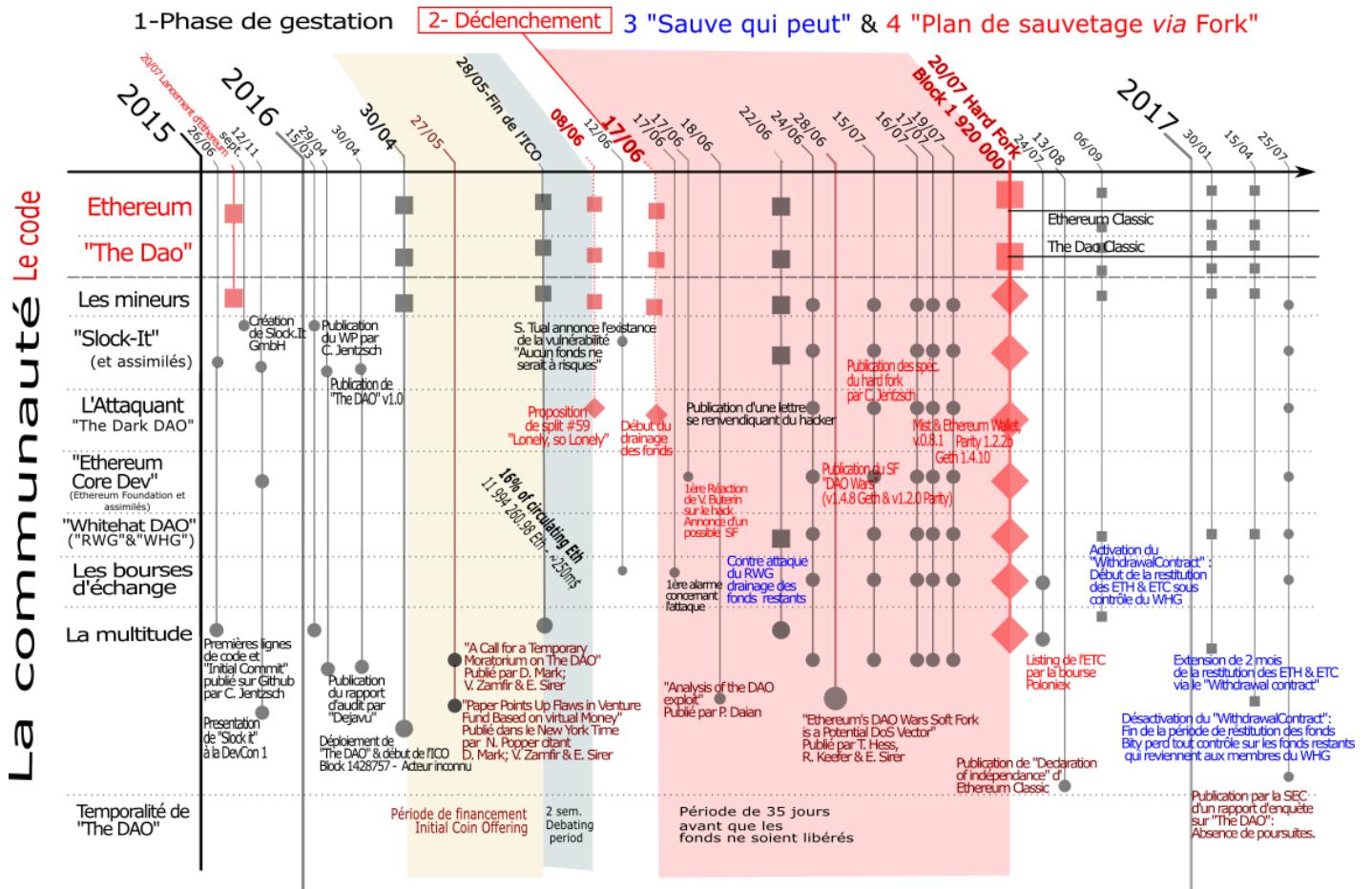
### Périodisation du *Hard Fork*\* de « The DAO »

Ce cas d'étude, comme le précédent, permet d'interroger le rapport qu'entretiennent les *coiners*\* à l'« *autorité algorithmique* » (Lustig et Nardi 2015) et leur degré de « *déférence aux codes* » (Hinkes, 2021). Mais il apparaîtra plus crûment encore que les *coiners*\* peuvent mobiliser la gouvernance sur l'infrastructure pour amender la gouvernance par l'infrastructure de leur CM, afin de la faire coïncider aux attentes monétaires et politiques mouvantes qui traversent leur communauté. Les deux cas que nous avons choisis pour cette thèse offrent de forts contrastes, tant en termes de mise en crise que de remise en ordre. La crise du *Hard Fork*\* consécutive à l'attaque de « The DAO » revêt la forme d'une double crise emboîtée. Le point de départ est une crise « de vulnérabilité » liée à l'exploitation effective d'une vulnérabilité connue, « *terrible* » et « *largement répandue* » (Vessenes 2016a) concernant un fonds d'investissement distribué déployé sur Ethereum (sous forme d'une application en *smart contract*\*): il s'agit d'une faille dite de « *réentrance* (ou « *reentrancy* »/« *re-entry* ») qui permet à un « *attaquant* » de quitter le fonds en récupérant plus de capital qu'initialement investi (Atzei, Bartoletti et Cimoli 2017, p. 172 & 177 ; DuPont 2018, p. 6). Cette faille permet de « *demandeur de l'argent plusieurs fois avant que son solde ne soit mis à jour et que l'ordinateur ne s'aperçoive qu'il n'y a plus d'argent sur son compte* » (Russo 2020, p. 185). Cette crise « de vulnérabilité » touche d'abord la couche applicative, avant de muter en une crise « d'évolution », du fait d'une proposition de remédiation sous forme de modification des règles protocolaires canoniques. Là réside l'intérêt de cette crise : la résolution d'un problème circonscrit concernant un projet lancé sur Ethereum va passer par une modification du protocole Ethereum

lui-même<sup>440</sup>. Cette évolution, nous le verrons, s'explique par la jeunesse de cette CM qui, à l'époque, est encore en phase de « preuve de concept », d'où la centralité – réelle ou perçue - de V. Buterin et des membres de la Fondation Ethereum dans sa gestion. Les *bitcoiners*\* critiques de la gouvernance des événements ne doivent pas oublier comment Nakamoto fut central dans les crises – « de vulnérabilité » et /ou « d'évolution » – qui ont touché Bitcoin lorsqu'il était le seul mainteneur principal et que la crise Bitcoin CVE 2018 traitée précédemment, elle, est arrivée en phase de maturation de son développement infrastructurel (cf. Chap. I).

L'analyse de cette crise repose, comme nous l'avons fait pour la crise Bitcoin CVE 2018, sur une périodisation documentant les acteurs (humains ou non) et la structure de leur relation, à chaque étape de la mise en crise et de la remise en ordre (Chronologie 6 suivante).

### Chronologie 6 : Périodisation de la crise consécutive à l'attaque de « The Dao »



Source : Rolland Maël

<sup>440</sup> Ce qui explique pourquoi certains acteurs filent l'analogie (péjorativement) de l'action de prêt en dernier ressort, typique des Banquiers centraux et de leur pouvoir discrétionnaire honni : « la fondation Ethereum a poussé le Hard Fork à renflouer les développeurs\* de Slockit et d'Ethereum, bien qu'il n'y ait pas de consensus du tout » (WhalePanda 2016).

Au sein de la période de mise en crise, nous conservons un découpage entre une phase d'insémination/gestation et une phase de déclenchement. Si, comme précédemment, elles correspondent à deux étapes distinctes dans leur temporalité et les actions entreprises, les frontières sont plus poreuses. La découverte du bogue sous la forme d'une attaque principale est certes « le » moment du déclenchement de la crise, et c'est elle qui va donner le « tempo » de la remise en ordre à venir. Mais elle a été précédée d'une série d'alertes publiques concernant la sécurité de « The DAO » qui ont amorcé des réflexions sur la remise en ordre. Nous démarrons la périodisation au lancement du protocole Ethereum, le 30 juillet 2015, pour souligner que le contexte de cette crise est celui des premiers temps du protocole Ethereum. Au sein de son écosystème naissant, l'entreprise qui lance « The DAO » et ses membres sont des acteurs centraux et reconnus. L'extension du périmètre de la crise, comme de son intensité, procède de l'engouement suscité au sein de la jeune communauté pour le lancement de « The DAO ». Celui-ci s'est en effet traduit par une levée de fonds record, pour l'un des premiers projets d'ampleur. En ce qui concerne la période de remise en ordre, *a contrario*, nous sortons du découpage entre phase d'évaluation et phase de résolution. Un tel découpage est pertinent pour une crise à gouvernance de « huis clos », mais il ne l'est plus pour restituer la crise présente et l'incertitude entourant sa gouvernance. Le déclenchement de la crise par la découverte d'une attaque en cours ouvre dans l'urgence, pour la communauté « The DAO » et celle d'Ethereum, une période de remise en ordre cacophonique. L'« effet laboratoire » particulièrement présent dans la crise Bitcoin CVE 2018 s'estompe : acteurs et instruments mis en action ne sont pas « *tout puissants* » d'où un « *gouvernement des crises [...] fait de bricolages* », [subissant] *des échecs [...] des imprévus tout au long du déploiement des politiques qu'il expérimente* » (Aguiton, Cabane et Cornilleau 2019, p. 16).

Du fait d'un attaquant actif *et* réactif, mise en crise et remise en ordre vont survenir *on chain*\*, de façon publique et obliger à réagir en temps réel, produisant incertitude (stratégique, organisationnelle et juridique) et complexité. On est loin du « confort » offert par le secret et la confidentialité d'une gouvernance de « huis clos », déterminant *une* remise en ordre unitaire, cohérente et coordonnée par une poignée d'acteurs de confiance. Ici, l'incertitude et les contraintes (particulièrement temporelles) prédominent et des questions de gouvernance se posent explicitement : des fenêtres d'action sont définies dans les codes de « The DAO » (renseignées en bas de la chronologie et par des aires de couleurs). Elles forcent à des actions rapides et précipitées dans un contexte d'absence de réponse claire aux questions du « qui » est en charge de la remise en ordre et de « comment » et « pourquoi » le faire. Cette crise fait place à *des* remises en ordre, hétérogènes en termes d'acteurs (d'où le grand nombre de groupes d'acteurs y participant, cf. marge de gauche), d'objectifs et de moyens. La cacophonie débouchera finalement sur une résolution sous forme d'une action collective et concertée.

Pour comprendre qu'un bogue touchant au domaine protocolaire conduise à réaliser un *Hard Fork*\* contentieux de la couche protocolaire, il faut saisir le contexte du développement infrastructurel d'Ethereum qui était encore en phase « de preuve de concept ».

### Phase d'insémination : démesure d'un fonds d'investissement distribué sur Ethereum

Comme pour la crise Bitcoin CVE 2018, l'origine de la crise réside dans la présence d'une faille dans des codes informatiques. À la différence du cas précédent, cette crise « de vulnérabilité » ne relève pas du domaine protocolaire, mais du domaine applicatif (cf. section I.2.1 précédente) : les codes d'Ethereum sont hors de cause, la faille étant logée dans ceux d'un *Smart Contract*\* établissant l'une des premières Organisations Autonomes Distribuées (ou DAO) « *de l'histoire de l'humanité* », sous la forme d'un fonds d'investissement en capital-risque décentralisé « *régi par la philosophie "code is law", par opposition aux mécanismes de contrôle centralisés* » (Bitmex Research 2017b). Cet organisme doit permettre « *aux investisseurs du monde entier de mettre en*

*commun leurs fonds, puis de voter sur la manière de les déployer* » (David Z. Morris 2023). L'idée et le développement du projet « The DAO » a émergé avant même le lancement d'Ethereum : la création du répertoire Github hébergeant le développement des codes logiciels et le premier *commit* datent de juin 2015<sup>441</sup>, soit un mois avant le lancement du « *mainnet* » (la version « *frontier* », cf. Chap. I section I.3.2). Ce projet s'inscrit dans la stratégie de financement d'une start-up : « *Slock It* ». L'entreprise allemande est fondée en septembre 2015<sup>442</sup> par trois associés, les frères Christoph et Simon Jentzsch et Stephane Tual, qui recrutent deux collaborateurs, Griff Green et Lefteris Karapetsas. L'équipe de développement est ainsi constituée de cinq membres, dont trois participent déjà de l'écosystème d'Ethereum : Tual est à l'époque chargé de la communication d'Ethereum pour la Fondation, C. Jentzsch a travaillé pour elle au développement du langage Solidity<sup>443</sup> (avec Christian Reitwiessner et Gavin Wood) et du client C++, au sein de l'équipe de V. Buterin à laquelle participe Karaptesas (Slockit GmbH et Jentzsch 2015, cf. Tableau 9 suivant).

**Tableau 9 : L'équipe Slock It**

| Nom<br>Prénom                  | Statut(s) et rôle(s) chez « Slock It »  | Statut(s) et rôle(s) dans l'écosystème   |
|--------------------------------|---|--|
| <b>Jentzsch<br/>Christoph</b>  | Co-fondateur et directeur de la technologie (« <i>Chief Technology Officer</i> ») | Équipe C++, responsable des tests (« <i>Lead Tester</i> »), « ETH Dev Berlin » & Ethereum            |
| <b>Jentzsch<br/>Simon</b>      | Co-fondateur et directeur général (« <i>Chief Executive Officer</i> »)            | /  |
| <b>Tual<br/>Stephan</b>        | Co-fondateur et directeur des opérations (« <i>Chief Operating Officer</i> »)     | Directeur de la communication (« <i>Chief Communication Officer</i> »), Ethereum                     |
| <b>Karapetsas<br/>Lefteris</b> | Responsable ingénieur technique (« <i>Lead Technical Engineer</i> »)              | Équipe C++, « ETH Dev Berlin » ; « Robin Hood Group » et « White Hat Group » au cours des événements |
| <b>Green<br/>Griff</b>         | Organisateur de la communauté (« <i>Community Organizer</i> »)                    | « Robin Hood Group » et « White Hat Group » au cours des événements                                  |

Source : Rolland Maël

« Slock it » ambitionne de « *décentraliser l'économie de partage* » en contestant le monopole des plateformes « *Airbnb* » ou « *Uber* » et leurs « *frais extraordinaires* » : pour ce faire, « *pas besoin de faire fonctionner des serveurs ou de gérer des transactions*\* [,] de transférer de l'argent ou de gérer la remise des clés. Tout cela sera géré par la blockchain Ethereum » et des *smart contracts*\* permettant aux usagers de contracter via une plateforme décentralisée et des serrures et

<sup>441</sup>

Voir

[https://github.com/blockchain\\*llc/DAO/commits/develop?after=e50d3bc008cf0bbe4285de9dda54d3a541cb0b4+944&branch=develop](https://github.com/blockchain*llc/DAO/commits/develop?after=e50d3bc008cf0bbe4285de9dda54d3a541cb0b4+944&branch=develop) [consultation au 14/02/2021].

<sup>442</sup> Voir <https://www.crunchbase.com/organization/slock-it> [consultation au 14/02/2021].

<sup>443</sup> C. Jentzsch, actif de 2014 à courant 2016, est le quatrième contributeur au répertoire Github de « *Solidity* », voir <https://github.com/ethereum/solidity/graphs/contributors> [consultation au 19/05/2022].

verrous qui y seront connectés<sup>444</sup> (slock.it 2016). Le projet est ambitieux. En plus de développer « *la plateforme en déployant le contrat intelligent\* sur la blockchain Ethereum et en vendant le matériel qui l'utilise* », il vise aussi à fournir différents services : un explorateur *ad hoc*, l'intégration de méthodes de paiement traditionnelles, des solutions personnalisées, etc. (*Ibid.*). L'entreprise doit être financée et, au commencement, le projet n'est pas encore « The DAO », mais une simple ICO qui ne s'« *appelait [même] pas ICO à l'époque [...] On ne savait pas encore... les mots on ne les avait pas encore* » [et] « *la conscience que ça crée une nouvelle forme d'entité s'est construite au fur et à mesure [...] au début c'était, on fait un crowdfunding... [...] puis [ :] ah oui, mais si on faisait un token et puis on peut voter et puis machin et puis [...] on se pose de nouvelles questions.* » [A. Roussel, Entretien n°11]. C'est au fil des questions rencontrées par l'équipe « *Slock It* » pour se financer que se construit l'idée d'établir un fonds de capital-risque indépendant et autonome, sans conseil d'experts ou de managers, dédié au financement des entreprises de l'écosystème naissant d'Ethereum.

C. Jentszsch, qui fait partie des premiers à avoir travaillé pour la Fondation Ethereum, sait que « *l'organisation à but non lucratif qui supervise le développement de la blockchain [Ethereum], manqu[e] de fonds* », d'où le fait que « *beaucoup de ses contributeurs sont rapidement partis pour poursuivre des projets connexes* » (David Z. Morris 2023). Le fait qu'une partie des membres de l'équipe soit déjà intégrée au développement d'Ethereum et aux ambitions du projet concourt à leur présence à la « *DEVCON 1* » (conférence annuelle des développeurs\*, organisée par l'*Ethereum Fondation*, nous y reviendrons dans une section suivante). En novembre 2014 à Berlin, la DEVCON 0 avait donné lieu à la présentation de recherches entourant la conception du design d'Ethereum. Très suivie de la communauté naissante, la DEVCON 1 de novembre 2015 à Londres est la première édition depuis le lancement d'Ethereum et l'évènement fait la part belle aux recherches appliquées et aux projets ambitionnant d'utiliser Ethereum (environ 400 personnes y participent, Gerring 2016). Le projet de serrure connectée est accueilli avec intérêt. Plus encore, l'annonce d'un financement innovant<sup>445</sup>, ne s'arrêtant pas aux canaux de la finance traditionnelle. En effet, les organisateurs revendentiquent disposer « *maintenant de la blockchain Ethereum et [pensent pouvoir] faire beaucoup mieux* »<sup>446</sup> : en plus de droits de vote, des avantages pécuniaires seront à « *retirer si vous participez* », « *vous pourrez voter sur les décisions importantes et, surtout, vous contrôlerez les fonds ! [Le] but est d'être une DAO rentable. Il s'agit d'une DAO à but lucratif.* » (Slockit GmbH et Jentszsch 2015) Puisque ce qu'ils « *faisaient était suffisamment intéressant pour intéresser une communauté [choix fut fait de] donner une dimension complètement différente* » au financement de Slock It via la constitution de l'entité « The DAO » : leur entreprise ne serait financée qu'en tant que] service provider de cette entité, c'était ça leur but [...]. Ils disaient : « *on développe un truc, on le donne à la communauté et en échange on devient service provider de ce truc-là.* » [A. Roussel, Entretien n°11]. « *Slock It* » développe cette entité comme un véhicule de financement, espérant

<sup>444</sup> La serrure, dénommée « *Slock* », sera « *connectée au contrat intelligent\* Slock de la blockchain\* Ethereum et contrôlée [et] le propriétaire [pourra] fixer un montant de dépôt et un prix pour la location [...] et l'utilisateur paiera ce dépôt par le biais d'une transaction [pour obtenir] la permission d'ouvrir et de fermer ce verrou intelligent [avec] son téléphone.* » (slock.it 2016)

<sup>445</sup> Chaque panel et présentation est diffusé en ligne et en temps réel, puis archivé. Pour la présentation de « *Slock It* », voir <https://archive.devcon.org/archive/watch/1/slockit/?playlist=Devcon%201&tab=YouTube> [consultation au 22/05/2022].

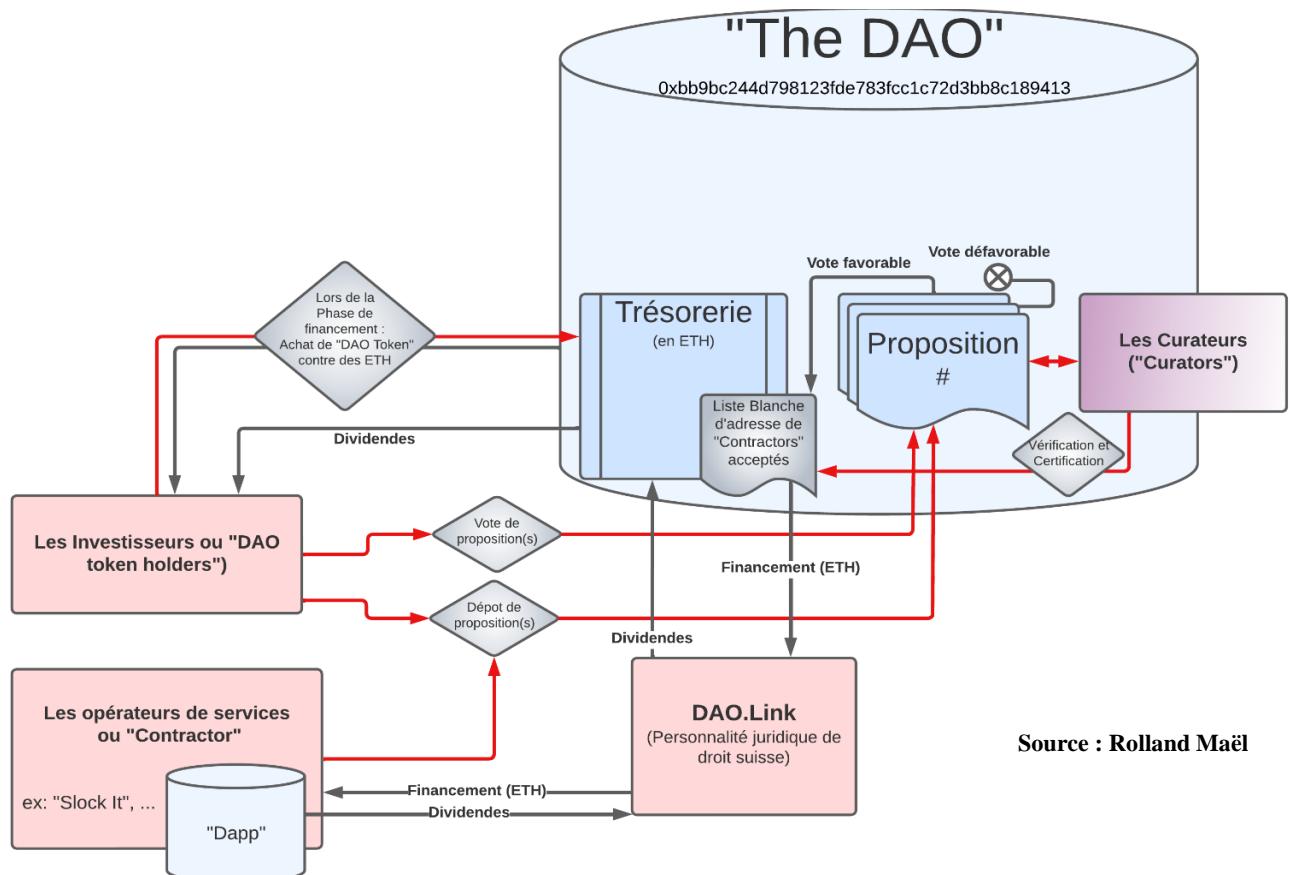
<sup>446</sup> Jentszsch témoigne de l'intérêt des investisseurs pour « The DAO »: « *Nous discutons avec des investisseurs et certains d'entre eux veulent nous donner de l'argent. Comment pouvons-nous gagner de l'argent ? [...] Nous n'avons pas besoin de le faire à l'ancienne. [...] Bien sûr, il faut que ce soit une DAO ! [...] Quelles sont les tâches de la DAO ? Tout d'abord, elle finance le développement. Nous ferons une prévente, une collecte de fonds, un crowdfunding. C'est là que nous avons besoin de votre aide* » (Slockit GmbH et Jentszsch 2015). Notre entretien avec A. Roussel [Entretien n°11] confirme cet engouement.

être « *au début [ce] fournisseur de services, mais en fait [la DAO et ses membres seront] libres de choisir le fournisseur de services qu'ils veulent* » (*Ibid.*). « Slock It » ne sera à terme qu'un de ses prestataires ou « *contractor* », acteurs humains que la DAO doit engager afin d'« *exécuter des actions dans le monde réel* », car la DAO en tant que « *logiciel pur* » (Teruzzi 2016a), « *ne peut pas construire un produit, écrire un code ou développer du matériel.* » (Jentzsch 2016b)

À partir de l'introduction publique de la *Devcon*, les projets de « Slock It » et de DAO d'investissement ne cesseront de croître, comme l'intérêt qu'il suscite au sein de la communauté Ethereum. « Slock It » continue d'assurer la promotion du projet *via* la publication d'informations sur son blog : en mars, S. Tual (2016a) publie un billet se voulant être « *une introduction de haut niveau au cadre standard DAO et à son White Paper\** ». La communauté se structure d'abord *via* le forum « *Slack* », créé par « *Slock It* » et conçu comme le canal de discussion principal. En février, on compte une multiplicité de canaux linguistiques différents (communauté polonaise en tête), fin mars le « *canal général de The DAO comport[e] près de trois mille membres* » (Shin 2022, p. 125) et culminera à près de 5 000 (Jentzsch 2016c). En mars 2016, le *White Paper\** est rendu public, suscitant un engouement renouvelé (Falkon 2017) : revenant d'abord sur le concept de DAO, il décrit et propose la version standardisée d'une « *première implémentation* » d'« *un code de contrat intelligent\* standard [permettant de] former une organisation autonome décentralisée (DAO) sur la blockchain Ethereum.* » (Jentzsch 2016b) Ce code est un « *modèle même de simplicité, avec à peine 900 lignes de code source* » (DuPont 2018, p. 2). Il annonce « *automatiser la gouvernance et la prise de décision au sein d'une organisation [...] en utilisant des contrats intelligents écrits en Solidity* » (Jentzsch 2016b). Le *Smart Contrac\*t TheDAO v.1* constitue un ensemble de règles et de dispositifs organisationnels formalisant le fonds et son administration, établissant un ensemble de statuts, rôles et actions légitimes en son sein (cf. Figure 13).

« The DAO » représente un fonds de trésorerie abondé lors d'une phase préliminaire dite « *de création* » durant laquelle seront émis les tokens « The DAO » contre des Ether. Tout détenteur d'ETH pourra devenir investisseur dans « The DAO » et dans les projets, qui demanderait à être « *Contractor* » via un processus de proposition cadré. La gestion du fonds relève directement de ses investisseurs, membres formels en tant que porteurs du jeton « The DAO » (ticker – DAO), qui sont les seuls à décider quel projet sera financé avec leurs fonds et selon quelles modalités, car ils bénéficient des droits suivants : proposer des projets à financer, voter pour ou contre des projets demandant des financements et recevoir des dividendes des projets financés, qui versent des revenus au fonds « The DAO » en contrepartie de leur financement, ensuite réparti aux porteurs en proportion de leur possession dudit Token (*Ibid.* ; Chohan 2017 ; DuPont 2018). Quatre statuts différents existent : les porteurs de jeton DAO (« DAO Token Holders ») ; les prestataires (ou

**Figure 13 : Statuts, rôles et fonctionnements clefs de « The Dao »**



L'intérêt communautaire large pour la structure proposée se traduit par la publication d'informations excédant l'équipe de développement : S. Polrot, pour la communauté Ethereum France présentera, par exemple, les *promesses* du projet (Polrot 2016b). Le choix innovant de « Slock It » de n'être qu'un prestataire parmi d'autres du fonds « The DAO » s'inscrit dans l'éthos de décentralisation, et offre aussi une protection juridique à l'équipe. Il impose de structurer la communauté au-delà de la start-up. Des membres actifs du *Slack* existant, « *Felix Albert et Auryn Macmillan* [...] rejoint par une équipe Core de six autres membres »<sup>447</sup> (DuPont 2018, p. 2) créent un forum indépendant, « *DaoHUB.org* » (Auryn 2016). « Slock It », via Tual, est « très satisfait » : « *les forums de Daohub.org sont un excellent* » outil, servant à fournir des informations et conseils

<sup>447</sup> Les membres sont : Felix Albert, Auryn Macmillan, Boyan Balinov, Arno Gaboury, Michal Brazewicz, Taylor Van Orden-Monahan, Des Donnelly, Daniel McClure (Auryn 2016 ; Bitmex Research 2017b).

aux nouveaux usagers, ainsi qu'à proposer et débattre des propositions (lucratives ou non) à soumettre à « The DAO » (Tual 2016b). Début avril sont dévoilés les résultats de l'audit des codes de la V1.0 de « The DAO », réalisé par l'entreprise « *déjàvu* » (celle qui avait audité les codes du protocole Ethereum pour la Fondation Ethereum) (Tual 2016a) : pas de problème notable. Mais la sécurité ne tient pas qu'au code. Puisque l'entité « The DAO » est indépendante vis-à-vis de « Slock It », « *le fournisseur de services par défaut de la DAO devrait être remplacé par un ensemble de curateurs indépendants* » (Jentzsch 2016c), garantissant une sécurité minimum, en assurant la sélection des équipes et projets demandant des financements au fonds (Teruzzi 2016a). Ce statut de « *Curators* » s'incarne dans une liste d'adresses à fonction particulière, liée à des acteurs humains reconnus et de confiance devant vérifier l'authenticité de l'identité des personnes (physiques ou morales) qui souhaitent réaliser des transactions\* avec l'entité « The DAO » : c'était « *une sorte de contrôle KYC* », un « *contrôle humain, pour s'assurer que les adresses mises sur liste blanche, qui pourraient recevoir beaucoup d'argent, [appartiennent bien aux] personnes [déclarées]* », et le rôle attendu des personnalités choisies est « *de... whitelister des adresses, si la DAO veut financer un projet quelconque, c'est nous qui devrions dire, cette adresse appartient à ce projet et maintenant les électeurs de la DAO peuvent voter. Nous ne votons pas, nous ne décidons pas, nous ne faisons rien d'autre que de mettre ou non des adresses sur liste blanche* » [Fabian Vogelsteller, Entretien n°12]. Leur rôle est conçu comme « *trivial et purement technique* », pouvant « *être remplacé à tout moment* » au bon vouloir des possesseurs de DAO token (Wood 2016). Le 25 avril est annoncée la liste des « *experts bien connus de la communauté Ethereum [...] portés volontaires pour faire ce travail* » (Jentzsch 2016c) : « *en partenariat avec Daohub.org, [« Slock It » obtient] un ensemble de signataires du curateur de la DAO qui ressemble au Who's Who de la cryptographie\** [avec] 11 membres [...] tous des membres actuels ou anciens du projet Ethereum » (Tual 2016d), dont le fondateur d'Ethereum lui-même<sup>448</sup>, « *ce qui a donné au projet une traction supplémentaire* » (Jentzsch 2016c). Les codes sources de « The DAO » sont ouverts au public le 29 avril. Publié sous licence libre, ces codes, bien que majoritairement écrits par C. Jentzsch et L. Karapetsas, ont vu près de 18 contributeurs participer à leur rédaction sur le répertoire Github<sup>449</sup>. Pour définitivement asseoir le caractère décentralisé de l'entité « The DAO » et son autonomie vis-à-vis de « Slock It », le déploiement des codes, par réalisation de transactions\* dédiées, est laissé à l'initiative d'anonymes de la communauté. Le 30 avril, 8 instances des codes ont été déployées selon les consignes préalablement données sur le forum DAOhub et celle choisie par « DAOhub.org » pour devenir

---

<sup>448</sup> Les 11 « *Curators* » sont : V. Buterin, Inventeur et fondateur d'Ethereum, Ethereum Foundation ; G. Wood, Fondateur d'Ethereum et d'Ethcore ; C. Reitwießner, Chef d'équipe Solidity & C++, Ethereum Foundation. ; A. Van de Sande, Designer en chef, Mist, Ethereum Foundation ; V. Tron, Développeur principal client Go, Ethereum Foundation ; A. Buchanan, Responsable de la recherche et du développement, Ethcore et EthDev, Berlin ; T. Gerring, Directeur de la technologie, Ethereum Foundation ; M. Becze, Développeur client JS et la R&D sur l'EVM, Ethereum Foundation ; G. Simonsson, Développeur principal, Ethereum Foundation ; V. Zamfir Recherche PoS (Casper), Ethereum Foundation ; F. Vogelsteller, développeur principal Mist et l'API web3.js, Ethereum Foundation (Tual 2016d).

<sup>449</sup> Par ordre décroissant en quantité de commits : C. Jentzsch, Letteris Karapetsas, Yoichi Hirai (aka *pirapira*) ; Griff Green ; Hayden Colm (aka « *CryptoColm* ») ; Simon Jentzsch ; Zhangyaning (aka « *u2* »), J. Baylina, Pawel Bylica (aka « *chfast* »), Stephan Tual, Paul Schmitzer (aka « *LiteBit* ») ; Jeffrey Anthony ; Christian Reitwiessner aka « *Chriseth* »), Pierre-Elouan Réthoré (aka « *rethore* »), Anthony Akentiev , Isidoro Ghezzi (aka « *isghe* »), Eric Fish (aka « *mrefish* ») et Gustav Simonsson. Voir <https://github.com/blockchainsllc/DAO/graphs/contributors> [consultation au 14/02/2021].

canonique est tirée « à pile ou face » entre deux adresses sélectionnées pour leurs conditions de pseudonymat renforcées<sup>450</sup> (Tual 2016a).

Ce même jour, « *The DAO* [entre] en ligne et [...] dans sa phase de création à l'adresse 0xbb9bc244d798123fde783fcc1c72d3bb8c189413 » (*Ibid.*), qui est programmatiquement ouverte pour 28 jours : la « crowdsales » est lancée jusqu'au 28 mai, il devient possible de créer des DAO tokens en envoyant des ETH à « *The DAO* »<sup>451</sup>. Les premiers *DAO Token Holders* agissent moins par confiance que par foi, envoyant, sans diligence raisonnable (contenue dans l'injonction DYOR) aucune, « plus de 1 537 000 ethers [...] au contrat intelligent\* de la *DAO*, [alors même que personne ne sait] si le code source du contrat est correct » : heureusement, l'instance choisie est conforme aux codes publiés, en particulier les adresses de curateurs qui y sont stipulées coïncident avec celles publiquement annoncées (DAOhub 2016). Là où les membres « *Slock It* » avaient conçu « *The DAO* » « comme un mécanisme de collecte de fonds » pour eux seuls et s'attendaient à lever « quelque chose comme 5 à 10 millions de dollars », « les choses ont rapidement dérapé alors que le buzz autour de *The DAO* s'accélérerait [ :] l'objectif est rapidement et « largement dépassé, [et c'est après] avoir récolté 20 ou 30 millions de dollars [, qu'] on est passé du financement de *Slock.it* au financement de toutes les applications sur Ethereum » (Jentzsch cité par David Z. Morris 2023). Si J.R. Willet avait inventé l'ICO pour financer Omni/MasterCoin (cf. Chap I), « *The DAO* », en « établissant le record de la plus grande campagne de crowdfunding de l'histoire à l'époque » (Insider 2021, voir Annexe n°I.4), fait gagner ces lettres de noblesse à ce type de financement. Son attaque va permettre d'identifier de bonnes et mauvaises pratiques. Nombreuses sont les personnes que le projet va intéresser et même exciter<sup>452</sup>. En témoigne A. Roussel, qui va avec son associé Gian Botshler : « [s'] intéress[er] à *Slock It*. C'était un projet qui était en vue, il était intéressant [...] on a fait partie de cette communauté de gens qui était absolument hallucinés par ce qui était en train de se passer [...] On a voulu participer » [A. Roussel, Entretien n° 11]. Cette volonté d'investissement va se muer en un partenariat entre la plateforme d'échange Suisse Bity et « *Slock It* » (Roussel 2016c), permettant d'ouvrir une passerelle\* simplifiée pour les novices, leur

---

<sup>450</sup> Déployer une instance de *Smart Contract*\* via une transaction nécessite des UCN ETH pour les frais de transaction afférents à l'opération. Les conditions d'approvisionnement en ETH du compte sont déterminantes dans la préservation de l'anonymat de la/des personne(s) impliquée(s) ; elles pourraient être attachées à des données *off chain*\* (adresse IP, adresse mail, ID, etc.). Un tutoriel de la procédure de déploiement de « *The DAO* », couvrant cette anonymisation, est publié sur le forum DAOHub (voir <https://forum.daohub.org/t/the-dao-official-bytocode-deployment-and-pushing-the-big-red-button-thread/519> [consultation au 14/02/2021] et sur le Slack (le 29 avril) : « Hey tout le monde. Si vous voulez déployer le *DAO*, regardez ce fil de discussion. Nous allons en choisir un au hasard dans ce fil pour être la *DAO* officielle très bientôt. Procurez-vous des pièces intraçables / sans historique (ShapeShift, btc mixer, etc.) et déployez. » (T. Monahan cité par Shin, 2022, p. 131).

<sup>451</sup> La levée de fonds se déroule en trois phases : les 15 premiers jours, le ratio était de 1 ETH/ 100 DAO Tokens, ensuite le nombre de tokens reçus diminue progressivement chaque jour avant la dernière phase des 4 derniers jours, où 100 Dao Tokens valaient 1,5 ether. L'excédent des investisseurs contribuant à plus de 1 ETH pour 100 DAO Tokens est alloué à un compte spécial appelé extraBalance (Jentzsch 2016b).

<sup>452</sup> Tous les acteurs rencontrés soulignent cette excitation. *Idem* du côté des académiques : pour nous, c'était la première participation à une ICO sur Ethereum ; même excitation de notre collègue A. Slim, nous racontant s'être procuré des DAO Tokens via Kraken. Dupont (2018) aussi y participera et va même proposer la création d'une « organisation caritative environnementale [...] "The DAO of Whales" [visant à prendre soin] de baleines oranges dans le nord-ouest du Pacifique » (DuPont 2018, p. 5).

permettant d'accéder à l'ICO, *on chain\** mais en fiat monnaie<sup>453</sup>. Un autre partenariat crucial s'est noué entre eux à quelques jours de l'ICO, prenant la forme d'une entreprise, « DAO.Link », « SARL » créée comme « *un Join Venture 50/50* », elle permet de résoudre le dernier « *blocage* [que l'équipe] avait »<sup>454</sup> [A. Roussel, Entretien n° 11] : « *Slock It* » et tout « *Contractor* » passeront via cette entité *Ad Hoc* de droit suisse pour contracter légalement avec « *The DAO* », car « *les factures et les bons de commande des entreprises ont besoin d'une adresse physique et - soyons réalistes - "The DAO, Ethereum blockchain smart contract address 0x93139adb39alf...dd031" ne fera pas l'affaire de votre bureau local des impôts* » (Tual 2016e). À l'accès facilité pour les investisseurs à l'ICO s'ajoute celui à des marchés secondaires. Dès le 27 mai, la bourse Kraken annonce ouvrir des marchés secondaires pour le DAO token dès qu'il deviendra transférable, le 28, devenant « *l'une des premières grandes bourses internationales à échanger des tokens DAO* [et ce, relativement à] *cinq monnaies fiduciaires différentes* » (Kraken et Southurst 2016). D'autres bourses suivent, comme « *Gatecoin, Bity, ShapeShift et Bittrex* » (De Tychy 2016). Dans le même temps, le traitement médiatique est large, la curiosité pour cette « *entreprise automatisée [levant] l'équivalent de 120 millions de dollars en monnaie numérique* » (Waters 2016) excède les cénacles *coiners\** et leurs publications spécialisées : à cet article de Waters du *Financial Time* le 06 mai s'ajoute celui de Popper (2016) pour le *New York Times* du 22 mai. Tout concourt à une participation massive qui n'a pas été anticipée : au montant minimum programmé pour que la levée de fonds soit valide (Jentzsch 2016b) ne répond aucune limite maximale (Buterin 2016e), d'où une ICO de tous les records : près de 11 994 260 ETH, équivalents à près de 16% de la masse monétaire en circulation, ont été mis en commun pour une valeur de près de 150 millions de dollars à l'époque par environ 6 700 adresses uniques (Castillo 2016 ; Waters 2016 ; Quentson 2016). Ce succès bénéficie aussi à Ethereum et à son UCN\* l'Ether, dont le cours passe « *d'environ 7,50 dollars lors du lancement de la DAO [à près] de 12 dollars à la clôture de la DAO le 28 mai, soit un bond de 60%* » (Shin 2022, p. 134). À mesure que « *The DAO* » sucite « *beaucoup d'enthousiasme dans l'écosystème crypto* » (Bitmex Research 2017b), les inquiétudes grandissent ; en témoigne, le 13 mai, la défection de G. Wood au poste de « *Curator* », qui justifie son choix par des craintes de réputation liées à « *l'utilisation du terme "curateur"* », pour lui « *trompeuse, suggérant une certaine autorité pour un jugement indépendant* », donc des responsabilités, là où « *les deux propriétés essentielles d'une DAO sont qu'elle est décentralisée et qu'elle est autonome* » (Wood 2016)...

### **Le déclenchement : des alertes variées précédant l'attaque de « *The DAO* »**

En cette fin du mois de mai 2016, les derniers jours de l'ICO, pour autant qu'ils ne sont pas « le » moment du déclenchement de la crise à venir, s'y lient inextricablement. Certains

<sup>453</sup> Cet arrangement permet « *de payer en euro, en dollars ou en francs suisse [...] On faisait vraiment les choses bien, [...] tout on chain\*, la personne nous déclarait une adresse ether [...]. Tu envoyais tes euros. À ce moment-là, on te quotes un prix en Ether et [...] on fait deux transactions [...] une transaction du montant d'Ether, de 100 balles [...] on envoie 99 euros équivalent Ether vers la DAO mais avec transfert, en ajoutant cette fonction particulière [...] create by proxy donc on attribuait les tokens au wallet de la personne. Et [...] on envoyait l'équivalent de 1 euro d'Ether à la personne [...] qu'il ait un petit peu d'Ether pour faire bouger son token, parce que du coup... Il y a eu beaucoup de gens c'était la première [, ils] voulaient participer à la DAO sans avoir d'Ether, ils ne savaient pas. [...] Je crois qu'il n'y avait que deux boîtes qui ont fait cela.* » [A. Roussel, Entretien n°11].

<sup>454</sup> Ils « *voulaient tout bien organiser hein, ils ont vraiment fait ça de manière professionnelle, c'est des ingénieurs et tout, ils ont tout bien fait. Et à moment donné, quelqu'un leur a dit [...] Mais la DAO, est-ce qu'elle a un numéro de TVA ? Puis ils ont dit ben non ! Et là on leur a répondu, bien alors vous ne pouvez pas faire du business avec vous, puisque vous, en tant que société allemande, vous devez avoir comme contrepartie une société qui a un numéro de TVA. Et ça les a complètement bloqués. [...] Il y avait tout le code [...] en préparation, ils corrigeaient les derniers bugs, enfin bon, il y a eu des bugs mais, heu... ils faisaient les derniers ajouts, la communauté était prête, tout le monde était prêt. Le business model était prêt, l'ICO était prête, [pour ne pas pouvoir] finalement faire ce qu'on veut, parce que il y a pas de numéro de TVA* » [A. Roussel, Entretien n°11].

« aficionados [...] craignent que le code de l'organisation n'ait été élaboré relativement hâtivement [,] les jeunes machines complexes ont tendance à avoir des failles et des vulnérabilités que l'on ne peut pas anticiper » (J. Lubin, cité par Popper 2016b). Les premières alertent n'attendent pas la fin de l'ICO pour éclater publiquement. Pour « Slock It », « The DAO » et les membres de leur communauté, la crise commence...

Le succès de la levée de fonds conduit le contrat de « The DAO » à devenir involontairement un « *pot de miel*<sup>455</sup> » : autant d'argent au même endroit attire l'attention, et pas seulement de personnes bien intentionnées. Des personnes bien intentionnées d'abord. De l'aveu de Zamfir [Entretien n° 9], chercheur pour la Fondation Ethereum et membre des « *Curators* » de « The DAO », la diligence raisonnable fut trop tardive, pour lui comme pour d'autres, et « malheureusement [...] on a regardé une fois seulement après qu'il y ait eu beaucoup d'argent » : « j'ai commencé à m'inquiéter parce que je ne savais pas comment fonctionnait la DAO, qui était vraiment impliqué, ce qui se passait, rien du tout. » [V. Zamfir, Entretien n° 9]. Zamfir fait partie du groupe de chercheurs en sciences informatiques qui publie le 26 mai un billet de blog relevant des problèmes de design (Sirer, Mark et Zamfir 2016). L'analyse ne regarde pas le code, mais les incitations structurelles en termes de théorie des jeux. Le design et les mécanismes de vote sont problématiques. Ces derniers induisent différents vecteurs d'attaques<sup>456</sup> pouvant « conduire à des manipulations financières, voire à des pertes », et, puisque « l'étude a identifié des solutions potentielles pour atténuer ces biais et vulnérabilités », les auteurs proposent un « moratoire temporaire » sur toutes les propositions qui seraient soumises à « The DAO », jusqu'à ce qu'une nouvelle version corrigée soit développée, acceptée et implantée (*Ibid.*). Cette alerte ne reste pas confinée et, le même jour, un article du *New York Times* revient sur les vulnérabilités qui viennent d'être publiées (Popper 2016a). Les conditions de cette divulgation posent question. Pour certains, il est « bizarre » que « Gun Sirer et Vlad Zamfir [aient] publié cette vulnérabilité d'abord dans le New York Times, avant de parler à Christoph et aux parties impliquées ? [...] C'est la pire chose à faire parce que cela a immédiatement attiré l'attention de tous les pirates et escrocs du monde sur The DAO parce que c'est le oh wow » [Entretien SuperAnon]. D'après Zamfir, la divulgation est responsable, « tous les curateurs et la team » ont été informés au « plus vite qu'on pouvait », avant la publication : différents canaux sont mobilisés (Skype, mais aussi email) pendant « deux jours [pour] essayer d'obtenir un accord politique, [...] entre Slock It et les curateurs pour avoir un moratorium » [V. Zamfir, Entretien n° 9]. La « team Slock It n'a pas vraiment apprécié la sortie du document, [...] ils pensaient que c'était quelque chose qu'[il aurait fallu] faire plus tôt » [*Ibid.*]. Le timing de cette publication n'est pas idéal, puisqu'elle intervient un jour avant la fin de la période de création ouvrant sur celle de proposition et de vote [*Ibid.*, F. Vogelsteller, Entretien n° 12 ; Jordi Baylina, Entretien n° 7]. Impossible d'intervenir maintenant. Le moratoire temporaire est acquis chez les curateurs, et le mieux aurait été de gagner du temps afin de « réfléchir à une stratégie de mise à niveau » en taisant cette publicité [Entretien SuperAnon].

Ce papier du « *Moratorium n'a pas parlé de la réentrance, la réentrance est une question très technique* [...] cela n'a rien à voir avec... ce social... c'était une chose très différente » [Jordi

---

<sup>455</sup> Un « *pot de miel* », en sécurité informatique, est unurre conçu pour attirer les attaques informatiques. Dans ce cas, les 150 millions de dollars d'ETH du contrat agissent non intentionnellement comme tel, attirant les attaquants potentiels.

<sup>456</sup> Différentes versions du papier existent (Sirer, Mark et Zamfir 2016 ; Mark, Zamfir et Sirer 2016) et malgré des divergences marginales, les vecteurs d'attaque identifiés sont : « *Le biais affirmatif et la désincitation au vote non* » ; « *L'attaque par harcèlement* » ; « *L'attaque par embuscade* » ; « *Le raid sur les jetons* » ; « *L'attaque par déséquilibre* » ; « *L'attaque par fractionnement de la majorité* » ; « *L'attaque simultanée par ligotage* » ; « *L'hypothèse d'indépendance* » ; « *La dilution des récompenses* » ; « *Le vote sans risque* » ; « *Le piège de la proposition simultanée* ».

Baylina, Entretien n° 7]. Mais début juin, ce sont les codes qui commencent à être éprouvés, indirectement d'abord. Le 5, l'architecte principal du langage de programmation\* d'Ethereum, Solidity, annonce y avoir « *découvert un anti-modèle [...] qui pourrait conduire à des attaques sur les contrats intelligents* » (Jentzsch 2016c). Sa découverte, il l'explique par la jeunesse d'Ethereum dont le développement infrastructurel n'est encore qu'en phase de « *Preuve de concept* » : « *lancé en octobre 2014, alors que ni le réseau\* Ethereum, ni la machine virtuelle n'avaient fait l'objet de tests en conditions réelles [...], certaines des premières décisions de conception [de Solidity, NDA] étaient initialement considérées comme les meilleures pratiques [, mais] confrontées à la réalité [,] certaines d'entre elles se sont révélées être des anti-modèles* » (Reitwiessner 2016). Soulignant le manque relatif de relais médiatique à l'époque (cf. « *comme la plupart des gens ne suivent probablement pas le flux des commits github sur ce dépôt* »), Reitwiessner vise à « *mettre en évidence certaines des conclusions ici* » : dans l'exemple de code qu'il donne, « *pendant que la fonction d'envoi est toujours en cours, le destinataire peut rappeler withdrawRefund [...] et il recevra donc à nouveau le montant, et ainsi de suite* » (*Ibid.*). Le 9 juin, le chercheur « Peter Vessenes [...] écrit un blog sur la découverte de Christian » (Jentzsch 2016c) où l'immaturité du développement infrastructurel d'Ethereum apparaît cuisamment. Le billet de blog commence en précisant que « *Chriseth, sur github, a attiré l'attention sur une terrible attaque contre les contrats de portefeuille* » et que s'« *il existait une voie de divulgation responsable pour les développeurs\* de contrats Ethereum* », l'auteur l'utilisera, mais pour l'heure, « *il ne semble pas y en avoir* » (Vessenes 2016b). L'annonce de Vessenes a de quoi inquiéter. La vulnérabilité de la « *course au vide* » (« *Race-To-Empty* »), ou « *bogue de réantrace* », est une « *véritable menace* », malheureusement « *très répandue* » : « *votre contrat intelligent\* est probablement vulnérable au vidage si vous gardez une trace des soldes des utilisateurs et que vous n'avez pas été très, très prudent* » (*Ibid.*). Le problème réside dans « *une fonction par défaut* » présente dans les « *codes de portefeuilles\** » et induisant une mauvaise comptabilisation des retraits : plusieurs retraits peuvent être déclenchés sans que la balance de l'usager n'en soit affectée et, quand « *le code est résolu, le solde de l'utilisateur est fixé à 0, quel que soit le nombre de fois que le contrat a été appelé* » (*Ibid.*). À « *ce stade, l'ensemble de la communauté des développeurs\* d'Ethereum [est mise] au courant de ce problème* » (Jentzsch 2016c) et les développeurs\* de différents projets s'y intéressent. Le 11 juin, l'équipe de développement de « *MakerDAO* » (sur lequel repose l'émission du stablecoin DAI, cf. Chap. II section II.2.3) découvre qu'un de leurs *Smart contracts\** y est exposé, permettant « *à n'importe qui de le drainer* » : en guise de remédiation, ils drainent eux-mêmes les fonds à risques pour les sécuriser (i3nikolai 2016) et gratifient P. Vessenes d'une récompense (« *Bug Bountie* ») en plus de remerciement (i3nikolai 2016b). C'est le 12 juin que le diagnostic est finalement posé pour « *The DAO* » : l'utilisateur « *Eththrowa* », membre du forum DAOHUB, a « *trouvé ce même antipattern dans la DAO, dans la section récompense du code* » (Jentzsch 2016c). L'annonce publique du diagnostic est faite par « *Slock It* » le même jour et se veut rassurante : « *Aucun fonds de la DAO n'est menacé suite à la découverte du bug du contrat intelligent\* Ethereum "recursive call"* » (Tual 2016f). Pour l'équipe, « *ce qu'il faut en retenir [, c'est qu'] il n'y a pas d'éther dans le compte de récompenses de la DAO, ce problème ne met PAS les fonds de la DAO en danger aujourd'hui [, mais] cela pourrait cependant nécessiter une reconsideration du Proposal Framework 1.0 avant le déploiement d'un DAO Framework 1.1.* » (*Ibid.*). Le diagnostic n'a mis au jour un problème de réentrance que pour « *le mécanisme de récompense [pour lequel] une solution de contournement était disponible[, d'où le désormais] fameux message "no-funds-at-risk"* » (Jentzsch 2016c). Si « *le cadre [de la mise à jour v1.1, NDA] a été rapidement corrigé en quelques heures* », reste que « *la base de code déployée n'a évidemment pas pu être modifiée aussi rapidement* », car c'était « *un processus lourd qui nécessitait un délai de vote de 2 semaines et une majorité des détenteurs de jetons pour voter* » (*Ibid.*).

Jusqu’alors, comme pour la crise Bitcoin CVE 2018, cette faille, bien que « de vulnérabilité », n’est pas activée, et l’équipe et la communauté pensent encore avoir du temps. Mais, c’est sans compter qu’un attaquant lui, ne manque pas, comme eux, d’identifier un « *exploit similaire dans la fonction splitDAO* » (*Ibid.*). Au petit matin du 17 juin, une attaque est lancée impliquant cette fonction, qui est un dispositif innovant conçu par « Slock It » pour protéger les investisseurs du problème de « *dictature de la majorité* » auquel fait face « *chaque DAO [ :] la possibilité pour la majorité de voler la minorité en changeant les règles de gouvernance et de propriété [...]. Par exemple, un attaquant possédant 51% des jetons [DAO] pourrait proposer de s’attribuer tous les fonds [et, détenant] la majorité des jetons, il serait toujours en mesure de faire passer ses propositions* » (Jentzsch 2016b, p. 2). Comme le statut de « *Curators* », cette « fonction split » est pensée pour réguler un comportement considéré comme illégitime en assurant à « *la minorité* » la pleine capacité « *de récupérer sa part des fonds* » : « *si un individu ou un groupe de détenteurs de jetons n'est pas d'accord avec une proposition et veut récupérer sa part d'Ether avant que la proposition ne soit exécutée, ils peuvent soumettre et approuver un type particulier de proposition pour former une nouvelle DAO [dite « Child DAO » et ceux] qui ont voté pour cette proposition peuvent alors diviser la DAO en transférant leur part d'Ether vers cette nouvelle DAO* » (*Ibid.*). La DAO enfant ainsi déployée suivant le cadre prédéfini est alors autonome, mais reprend la structure de la DAO mère : l’ensemble des mécanismes sont les mêmes sauf qu’il faut définir de nouveaux « *Curators* ». Réaliser une proposition de split était la première étape de l’attaque. Elle fut réalisée le 08 juin via « *la proposition DAO #59, avec le titre "Lonely, so Lonely"* », comme révélée par la première analyse de l’attaque de Daian<sup>457</sup> publiée le 18 juin (2016). L’attaque suit ce déroulement : « *1. Proposer un split et attendre que la période de vote expire [...] 2. Exécuter la scission. [...] 3. Laisser la DAO envoyer à votre nouvelle DAO sa part de tokens [...] 4. S'assurer que la DAO essaie de vous envoyer une récompense avant qu'elle mette à jour votre solde mais après avoir fait (3). [...] 5. Pendant que le DAO fait (4), exécuter à nouveau splitDAO avec les mêmes paramètres qu'en (2) [...] 6. La DAO va maintenant vous envoyer plus de child tokens, et aller retirer votre récompense avant de mettre à jour votre solde. [...] 7. Retour à (5) ! 8. Laissez la DAO mettre à jour votre solde. Parce que (7) retourne à (5), il ne le fera jamais :-)* » (*Ibid.*).

Le 17 juin, à « *T 7 ou 8 heures, heure de Berlin, Griff s'est réveillé et a vérifié son téléphone [ :] un membre de la communauté Slack nommé Mo [lui apprenait] que quelque chose d'étrange se passait avec la DAO [,] les fonds étaient en train d'être drainés. Griff a vérifié : un flux de transactions\* de 258 ETH (5 600 \$) quittait la DAO.[...] Il a appelé les autres membres de Slock.it. Mo a réussi à joindre le frère de Christoph, Simon, et Griff l'a imploré de prévenir Christoph au plus vite* » (Shin 2022, p. 141). Simon Jentzsch préviendra son frère Christoph qui, sans arriver à « *comprendre immédiatement ce qui se passait* » avec ce split de la DAO principale, était certain « *que quelque chose n'allait pas du tout* » (*Ibid.*). À 9h10, heure de Paris, l’utilisateur « ledgerwatch » annonce la même découverte sur le forum Reddit : « *Je pense que TheDAO est en train de se vider en ce moment [...] je ne peux pas enquêter, mais il semble qu'il s'agisse d'une sorte d'exploit d'appel récursif* »<sup>458</sup>. La crise vient de se muer en crise « de vulnérabilité » et la remise en

<sup>457</sup> Voir la transaction ici : <https://etherscan.io/tx/0x5798fbc45e3b63832abc4984b0f3574a13545f415dd672cd8540cd71f735db56> [consultation au 12/05/2024]. L’investigation de Shin (2022, p. 148-151) démontre que cette proposition de split émanait d’un investisseur chinois honnête et, le « *mercredi 15 juin, à 6h26 (heure de Berlin), l'attaquant, utilisant deux contrats différents, a voté en faveur de la DAO enfant 59 [...] qui était actuellement vide [et] plus d'une heure plus tard, la période de vote de sept jours sur la Child DAO 59 s'est terminée [et] personne d'autre ne pouvait y entrer. Étant donné que le détenteur chinois de jetons DAO n'avait jamais voté en faveur de sa propre proposition, l'attaquant DAO était la seule personne à pouvoir se séparer de cette DAO.* »

<sup>458</sup> Voir [https://www.reddit.com/r/ethereum/comments/4oi2ta/i\\_think\\_thedao\\_is\\_getting\\_drained\\_right\\_now/](https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/) [consultation au 12/05/2024].

ordre commence, dans la panique. En ce vendredi matin de juin 2016, nombreux sont ceux (comme nous) à se réveiller à la manière de Griff Green et à découvrir en temps réel l'attaque, le krach du cours DAO Token et surtout celui de l'Ether qui s'en suivent<sup>459</sup>. Au-delà d'Ethereum, l'ensemble des communautés *coineuses* est en émoi à la découverte des informations qui commencent à se répandre sur les réseaux\* sociaux. Finalement, les délais programmés au sein du *Smart Contract* laissent « *35 jours avant que le pirate ne puisse accéder aux fonds [laissant] le temps [...] à la communauté de réagir... et de se déchirer* » (Polrot 2016c).

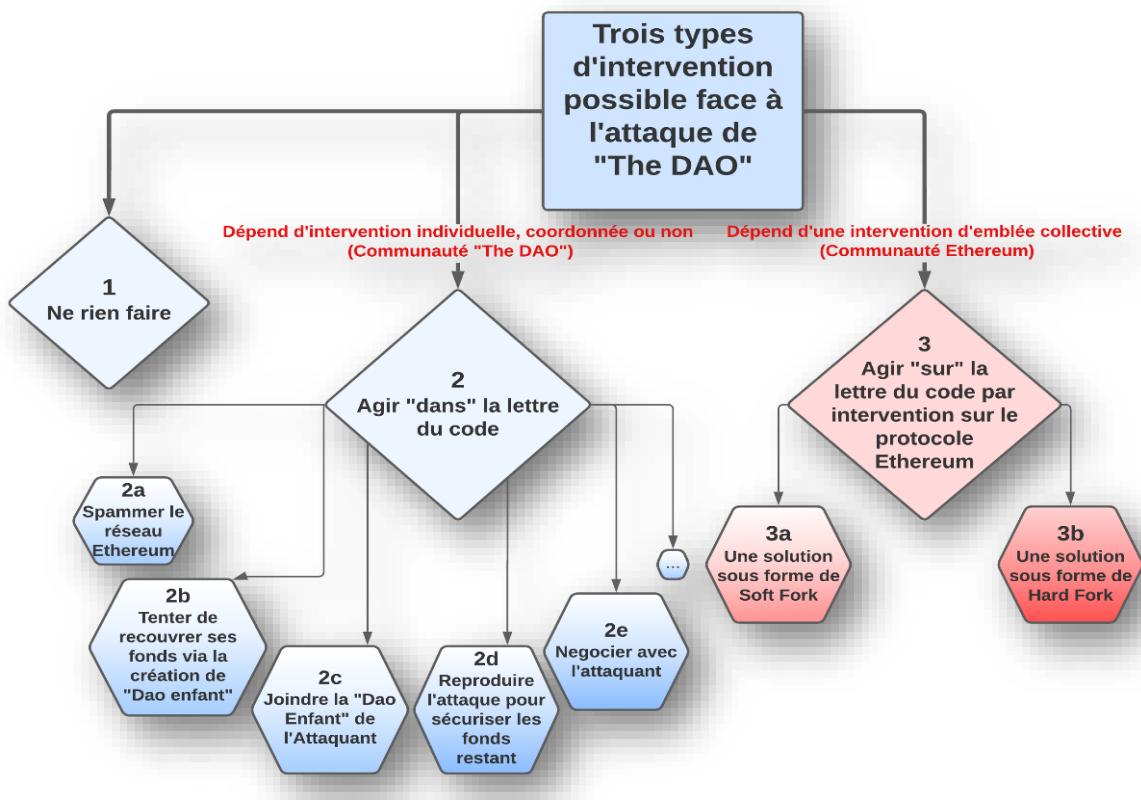
---

<sup>459</sup> A. Roussel [Entretien n°11] « *organisai[t] une séance avec une dizaine de personnes pour leur montrer ce que c'était la DAO et puis le hack s'est passé en même temps ça c'était genre fantastique. [...] je leur montre, ha regardez [,] c'est quand même bizarre, le nombre d'Ether il descend. [On rigole] Et puis là, un de mes collègues qui commence à regarder les news* ».

### III.3.2 Une remise en ordre complexe, contrainte et controversée : moyens et enjeux d'un consensus multi-acteur

En ce vendredi 17 juin au matin, à la surprise répond l'urgence. Bloc d'enregistrement après bloc d'enregistrement, l'attaquant s'empare « de 258,056565<sup>460</sup> ETH à la fois [, représentant] entre 3 500 et 5 550 dollars [, et ce] à peu près toutes les secondes, soit [...] entre 210 000 et 330 000 dollars par minute, ou entre 12,6 millions et 19,8 millions de dollars par heure » (Shin 2022, p. 149). La première alerte sur le Slack de « The DAO » permet à l'équipe de commencer à évaluer la situation, de relayer les premières informations et, surtout, de créer une cellule de crise avec les personnes clefs de l'écosystème. Car, dès le déclenchement, différentes stratégies de remédiation paraissent possibles, nécessitant des experts aux compétences différencierées. Outre l'option de ne rien faire (1), il est possible d'intervenir à la fois via le domaine applicatif et le domaine protocolaire : soit agir au sein de la lettre du code de « The DAO v.1 » (2, en Bleu, cf. section « Sauve-qui-peut » suivante) ; soit agir sur celle du protocole Ethereum lui-même, plus ou moins radicalement, par la publication d'une nouvelle version de l'implémentation protocolaire incluant un patch correctif soit de type *Soft Fork*\*, soit de type *Hard Fork*\* (3, en rouge, cf. section III.3.3 qui explicitera les deux formes), hiérarchiquement supérieur puisqu'il en contient les données endogènes\* (Annexes n°V.6).

Figure 14: : Trois types de stratégies de remédiation



Source : Rolland Maël

<sup>460</sup> L'attaquant a accumulé « 25 805,61 Tokens DAO (environ 4 650 \$) » dans l'adresse servant à l'attaque et la fonction split lui permet de réclamer des ETH au rapport de 100:1, d'où le drainage par transaction de 258,06 ETH (Shin 2022, p. 152).

## **Une cellule de crise à l'image des stratégies de remédiation : diversifiée**

En premier lieu, Christoph avertit « *la Fondation Ethereum[, ] Stephan et Griff [sont choisis pour servir de] porte-voix [et] Simon, Lefteris et lui [tentent] de comprendre comment l'attaque [a] fonctionné et ce qui [peut] être fait* » (*Ibid.*, p. 143). À Shangaï, V. Buterin, informé *via Skype*, pense d'abord à « *spammer le réseau\* pour ralentir l'attaque, pendant que lui et d'autres développeurs\* essayaient de déterminer exactement ce qui se pass[e]* » (Russo 2020, p. 188). Une cellule de crise (ou plutôt des cellules) excédant « *Slock It* » et regroupant des experts aux compétences différentes est rapidement constituée avec « *Christoph, Simon, Vitalik et les autres [via la création de] groupes Skype [mais aussi Slack, etc. NDA] avec tous les anciens visages - Lefteris, Vitalik, Gav, Jeff, Aeron Buchanan, Péter Szilágyi, Christian Reitwießner, Avsa [Alex Van de Sande, NDA], Taylor Gerring, Fabian Vogelsteller, etc.* » (Shin 2022, p. 144). V. Zamfir [Entretien n°9] prend part à cette cellule de « *peut-être 10 à 20 [...] personnes dans ces canaux de discussion* ». À « *l'époque [...] tout le monde était dans un état très réactif, [la] The Dao était drainé, et tout le monde regardait la page etherscan sans savoir ce qui se passait, [...] jusqu'à ce que nous découvrions [que] quelqu'un a trouvé le bug [...] et ensuite ce qui s'est passé en interne c'est que les gens ont dit hooo, que devrions-nous faire ?* » [Fabian Vogelsteller, Entretien n°12].

La crise « de vulnérabilité » concerne les codes de « The DAO v.1 » qu'exploite à son avantage un attaquant. La priorité est de cerner les mécanismes de l'attaques et le fonctionnement de « The DAO ». La compréhension des codes de « The DAO v.1 » est cruciale en ce qu'elle détermine les actions correctives possibles dans le cadre de « la lettre du code » de « The DAO ». Ces codes régissent toutes les procédures et délais d'intervention pour tous les participants, y compris l'attaquant. Cependant, les connaissances les entourant sont pour le moins asymétriques. L'attaquant est l'un des mieux informés. L'attaque « *n'est clairement pas triviale* » et la vulnérabilité était « *non seulement connue, mais corrigée par les créateurs [...] dans une mise à jour planifiée* » [(la « The DAO v.1.1 ») : mais] alors qu'ils rédigeaient leurs articles de blog et croyaient victoire, [voilà que] le pirate préparait et déployait un exploit ciblant [...] la fonction 'splitDAO' [dont il est le seul à avoir remarqué qu'elle] était vulnérable au modèle d'envoi récursif» (Daian 2016). À l'opposé, les membres de la cellule de crise « avaient différentes informations » et beaucoup de « *questions* » : qu'est « *ce qu'il était possible de faire dans le software [, ] comment fonctionne The DAO ? [...] Quels étaient les temps d'arrivée à différentes échéances ? Qu'est-ce qui pouvait se passer ? Qu'est-ce que pouvait faire le DAO Hacker ? À quel moment ?* » [V. Zamfir, Entretien n° 9]. La programmation complexe du fonds établit « *un jeu d'attente très compliqué. [...] Donc, il fallait arrêter [l'intervention de type Fork\*] avant les échéances inscrites dans The DAO. Et il y avait beaucoup de controverses autour [des questions de] Fork\*. Qu'est-ce que fait The DAO ? Où sont les différentes DAO ? Comment est-ce qu'on peut s'assurer qu'on les trouve et qu'on peut récupérer les fonds ? Et que le DAO Hacker n'obtienne pas de l'argent des DAO avant ça* » [V. Zamfir, Entretien n° 9]. Pour tout ce qui touchait à la programmation de « The DAO v.1 », « *seuls Christophe et Lefteris pouvaient répondre à ces questions* » [*Ibid.*] et « *ils ont essayé de discerner la méthode d'attaque pour pouvoir contre-attaquer et récupérer les pièces* » (Shin 2022, p. 144). La compréhension des codes de « The DAO » contraint la capacité des acteurs à mener des actions correctives au sein de la lettre des codes : les différentes échéances à tenir (le délai pour que les Ethers volés par l'attaquant deviennent transférables) s'imposant aux acteurs de la cellule pour que d'éventuelles actions correctives protocolaires soient décidées, mises en place et finalisées. Temps pour le moins restreint, que ce soit pour implémenter un patch correctif sous forme de *Fork\** (*Soft ou Hard*), mais surtout pour le faire accepter par l'ensemble de la communauté alors qu'il est par nature plus controversé. Pour ce qui concerne le domaine protocolaire, « *seuls Gavin, Jeff et Vitalik pouvaient vraiment [agir] ... Moi et tout le monde on pouvait voir ce qui était possible sur le côté* »

*blockchain. Mais Gavin et Jeff devaient le faire. Leur équipe devait le faire.* » [V. Zamfir, Entretien n° 9].

Le temps est au brainstorming, toutes les options de remédiation possibles doivent être proposées et évaluées. Dans « *un groupe Skype avec des opérateurs d'échange* », Buterin et d'autres discutent des « *stratégies de mitigation* » et celles auxquelles les opérateurs de bourses pourraient prendre part : « *saisir les fonds volés qui passeraient par des bourses d'échange* », comme ils le font généralement si d'aventure l'attaquant réussissait à les sortir de « *The DAO* » (*Ibid.*). À l'extrême et dans la panique, Buterin et George Hallam demandent la suspension des cotations ainsi que des dépôts et retraits d'Ether et de DAO Token : « *"TOUTES LES BOURSES : veuillez interrompre les échanges d'Ether dès que possible* » (George Hallam, porte-parole de la Fondation Ethereum cité par Russo 2020, p. 189). Présent, Dino Mark, co-auteur avec Sirer et Zamfir du « *Moratorium* », va jusqu'à aborder l'hypothèse d'un *Hard Fork*\* avec « *rollback* » : correspondant à un changement des règles protocolaires permettant un retour en arrière dans l'historique des enregistrements, cette éventualité est perçue comme violant le sacro-saint principe d'immutabilité (Shin 2022, p. 144). Les opérateurs de Bourse réagissent vivement à ce qu'ils considèrent comme des mesures radicales risquées : « *Tristan D'Agosta de Poloniex* » est critique, selon lui ce type de HF ne manquera « *de provoquer une panique sur le marché si la blockchain est considérée comme non fiable* », puisque soumise au désir de censure de certains. En outre, si certaines bourses acceptent d'arrêter le trading, d'autres se demandent « *si la mesure [est] absolument nécessaire* » car, pour autant que cela « *empêcherait l'attaquant de liquider des fonds, [cela] pénaliserait également les traders légitimes* » (Bill Shihara, CEO de Bittrex cité par Russo 2020, p. 189). Leurs clients traders, potentiellement investisseurs dans « *The DAO* », seraient pénalisés deux fois, par l'attaque et par cette mesure, les empêchant de quitter le marché au plus vite alors qu'ils anticipent, à raison, que le prix décrochera... Pour le coup, c'est un *vendredi noir* et le « *le jour de l'exploit, les détenteurs d'ETH et de DAO ont connu un véritable chaos [durant lequel] le prix de l'Ethereum a chuté de 21 dollars avant l'attaque à seulement 14 dollars après* » (Shin 2022, p. 153). Crack qu'on soupçonne d'avoir été exploité financièrement par l'attaquant, via une position vendeuse (*short*) puisqu'il en définissait la temporalité<sup>461</sup>.

En quelques heures, par petits groupes et en secret, les membres des cellules ont entrevu différentes stratégies de remédiation possibles. Elles n'impliquent pas toutes ni les mêmes actions, ni les mêmes acteurs, ni les mêmes domaines d'intervention. Et il apparaît d'emblée que les actions sur le protocole de type *Fork*\* suscitent la controverse. Il est aussi temps d'informer le public des avancées en cours, de l'impliquer et d'évaluer sa réception des différentes solutions, dont les plus radicales nécessiteront l'implication de toutes les franges. Dans les deux heures de la découverte de l'attaque, Green informe la communauté « *The DAO* » via le « *Slack* » et « *DAOhub* » : « *@channel ALERTE D'URGENCE ! SI VOUS AVEZ UN SPLIT OUVERT, Veuillez ENVOYER UN MESSAGE À UN MEMBRE DE SLOCK.IT DÈS QUE POSSIBLE!!!* » (*Ibid.*, p. 143). Message repris et amplifié par Buterin répondant au billet de « *ledgerwatch* » sur Reddit par le même type d'appel : « *Il serait très utile que la personne dont le split se terminera dans 2 heures (#69) nous contacte.* » (Buterin 2016d). Ces premières réactions traduisent que des stratégies de contention sont à l'œuvre, marquant une nouvelle étape dans la remise en ordre. À 13 heures, Buterin (2016b)

---

<sup>461</sup> Des « *allégations [...] ont fait état d'un short Ethereum de 3 millions de dollars qui s'est produit sur Bitfinex quelques instants avant l'attaque, [...] clôturé avec un bénéfice de près de 1 million de dollars. [...] Tout attaquant motivé par des considérations financières [...] serait incité à s'assurer des profits, indépendamment d'un éventuel rollback ou fork, en vendant à découvert le jeton sous-jacent [car] la chute vertigineuse [du cours de l'Ether] qui s'est produite dans les minutes qui ont suivi le split malveillant offrait une excellente opportunité de profit [qu'] il aurait été stupide de ne pas saisir.* » (Daian 2016)

publie, via le Blog de la Fondation Ethereum, une « *mise à jour critique* » à l'adresse de la communauté Ethereum dans son ensemble. Le post est succinct et optimiste : l'annonce de l'attaque en cours précise déjà qu'il « *s'agit d'un problème qui affecte spécifiquement la DAO [et qu'] Ethereum lui-même est parfaitement sûr* », mais ajoute que, en tout état de cause, un « *Fork\* logiciel a été proposé (sans ROLLBACK ; aucune transaction\* ou bloc ne sera "inversé") qui [empêchera l'attaquant] de retirer l'Ether au-delà de la fenêtre de 27 jours.* » (*Ibid.*). Buterin tire même des événements des leçons pour le développement infrastructurel d'Ethereum, sous forme de conseils aux développeurs\* : ils sont enjoins à prêter une grande attention aux « *bugs d'appels récursifs* », à se tenir informés « *des conseils de la communauté de programmation [et d'] éviter de créer des contrats qui contiennent plus de ~\$10m de valeur* »), tout en rappelant que des financements sont ouverts (« *DevGrants* », « *Blockchain Labs grants* » et « *String autonomous finance grants* ») à ceux travaillant sur « *les outils [...] qui facilitent l'écriture de contrats intelligents sûrs sur Ethereum* » (*Ibid.*). Voilà que vers « *13 heures, heure de Berlin, peu après la publication [de ce] billet de Vitalik, l'attaque de The DAO s'est arrêtée* », sans que l'on sache si le *smart contract\** utilisé pour l'attaque a cessé de fonctionner (hypothèse de G. Green), ou si l'attaquant a pris peur des menaces brandies (hypothèse des autres membres de « *Slock It* » ; Shin 2022, p. 153).

## 50 nuances de « Code is Law » : un diagnostic et des stratégies de remédiation controversés

Nous l'avons vu, il n'y a pas de crise en soi et l'établissement d'un diagnostic de crise est un acte politique essentiel qui détermine, outre la « nature » de la pathologie (et sa gravité), le prescripteur, le malade, les traitements et le parcours de soin. Tout diagnostic de crise renvoie à une lecture imposée dans laquelle « *les problèmes publics résultent d'erreurs, de dysfonctionnements ou de mauvaise gestion* » servant non seulement à identifier les problèmes, mais aussi à légitimer les actions de différents acteurs en produisant du sens ou en contestant l'état du monde, et créant ainsi des fractures matérielles, idéelles et temporelles (Aguiton, Cabane et Cornilleau 2019, p. 10). Puisque « *mettre en crise, c'est [...] fabriquer un cadrage politique [permettant] soit de tracer des voies de "sortie de crise" [...], soit de construire des infrastructures de prévention en amont* » (Aguiton, Cabane et Cornilleau 2019, p. 15), c'est par définition une manière d'imputer et d'exonérer des responsabilités : « Quoi faire » sous-tend un « pourquoi », un « par qui » et un « à l'avantage / au désavantage de qui » ? Dans le cas de la crise Bitcoin CVE 2018, le bogue affecte les codes d'une implémentation logicielle protocolaire dont la maintenance est formellement à la charge d'une équipe. Le diagnostic du « bogue » et la voie de remédiation proposée font consensus entre tous, comme l'indique l'absence de controverse tant *a priori* entre les techniciens (au sein de l'arène locale du repo GitHub Bitcoin Core) qu'*a posteriori*, entre les autres composantes communautaires (après la publication du *post mortem*). C'est que la solution corrective (revenir à des codes antérieurs non vulnérables) est simple et n'ouvre aucun débat. Dans le cas de « The DAO », en ce vendredi 17 juin 2016, le concert des commentateurs s'étend sur la qualification d'« attaque », reconnaissant dans ce qui se passe l'existence d'un hiatus entre le résultat anticipé et celui effectivement obtenu du code de « The DAO v.1 » qui serait abusé par un acteur mal intentionné. Mais cette unanimité première va vite s'éroder, car la situation entourant la crise de « The DAO » est très différente.

Bien que le diagnostic considérant les faits comme une attaque liée à l'exploitation d'un bogue soit majoritairement partagé, une minorité va le contester. En second lieu, même en considérant la chose comme une attaque, les voies de remédiation sont multiples selon l'évaluation et les cadrages retenus de ces enjeux : « *Soft Fork\*, Hard Fork\*, contre-attaque, ne rien faire et de multiples combinaisons de ces options sont autant de voies possibles* » (Karapetsas 2016a). Les débats et dissensus entre spécialistes, apparus au sein de l'arène locale qu'est la cellule de crise, sont annonciateurs des débats publics. La présence de ces controverses conduit à mobiliser une

gouvernance publique dans la gestion de cette crise. Aucune solution n'est simple. Au-delà de questionner ce qui dysfonctionne, les diagnostics contradictoires réalisés et stratégies de remédiation proposées (cf. Figure 14 précédente) renvoient à l'hétérogénéité des risques perçus (pour la communauté « The DAO » ou pour Ethereum dans son entier), à des coûts et bénéfices associés à chacune des stratégies offertes (coûts économiques auxquels s'en ajoutent d'autres, en termes d'image et de motivation communautaire) enfin, à l'assignation de responsabilités *via* la définition de statuts et rôles pour chacun des acteurs dans cette remise en ordre. Pour chaque voie de remédiation, la question de sa légitimité communautaire fait débat : se dessinent, concernant la « bonne » gouvernance d'Ethereum, des positions oscillant entre les deux pôles idéal-typiques déjà posés (cf. Chap. II section II.3.3). Certains réduisent cette légitimité à une simple question de conformité des actions aux principes du "Code is Law" dans sa version la plus rigoriste et hypostasiée (cf. l'idéal-type de la « loi de Szabo ») : tout résultat de code est par définition légitime, la déférence au code (Hinkes 2021) et à l'« autorité algorithmique » (Lustig et Nardi 2015), même fautive, doit être totale. Face à ces représentations de *coiners*\*, d'autres positions existent et vont s'imposer (plus proches du pôle idéal-typique opposé de la « Loi Crypto » de Zamfir 2019). Ce cas démontre l'hétérogénéité de vues monétaires structurant ces communautés, leur évolutivité\*, donc le fait qu'« autorité algorithmique » et « déférence au code » sont complétées d'une gouvernance humaine et sociale essentielle. On retrouve les conclusions du chapitre II : pour nous, la qualité et la viabilité d'une CM, comme la confiance/défiance qui en sous-tendent les usages, s'apprécient à l'aune de sa capacité à se reproduire légitimement aux yeux des acteurs. D'où l'intérêt d'étudier une crise à gouvernance *publique* qui, contrairement au cas du huis clos, voit s'exprimer un dissensus éclairant plus crûment les rapports, attentes et désirs pluriels qu'ont les *coiners*\* envers leur système de paiement et l'« autorité algorithmique » (Lustig et Nardi 2015) qu'ils lui accordent.

La figure précédente (Figure 14) distingue trois types de stratégies de remédiation suivant le rapport qu'entretiennent leur justification à l'interprétation rigoriste du « *Code is Law* » et à l'« *autorité algorithmique* » pleine qui devrait en découler. Elles ne relèvent ni du même cadrage politique, ni des mêmes domaines d'intervention, ni des même acteurs. Et leur efficacité est incertaine. D'un côté, les actions agissant, comme l'attaquant, *au sein* de la lettre des codes (1 et 2, en Bleu, présentés dans la section « *Sauve-qui-peut* » suivante) : ces interventions sont par nature limitées à contenir et minimiser les pertes financières auxquelles les membres de « The DAO » font face. Le second type est théoriquement plus efficace, permettant une remise en ordre globale en agissant directement « sur » la lettre du code protocolaire d'Ethereum (et donc sur les données endogènes\* hiérarchiquement inférieures, cf. Annexe n°V.6). Mais, à son efficacité théorique répond son caractère incertain, lent et politiquement complexe. Ce type d'intervention suppose des modifications protocolaires radicales (3, en rouge, cf. section III.3.3), qui dépendent « *de la communauté Ethereum au sens large pour [leur] mise en œuvre* » (Karapetsas 2016b). À travers la présentation des enjeux de ces familles d'intervention (plus individuels ou collectifs), de leurs cadrages et des débats qu'ils vont susciter, il est permis de comprendre les ressorts de cette crise ouverte à gouvernance publique. La légitimité, accordée ou non à chaque famille d'intervention, renverra aux questionnements communautaires sur les propriétés désirées de leur CM et de la « bonne » gouvernance qui y est associée.

### « *Ne rien faire* » (1)

Partant de l'interprétation rigoriste du « *Code Is Law* », certains arguent que l'attaquant n'est qu'un usager agissant dans les limites définies par le code. Dans ce cadre, il n'y a pas d'attaque et il est légitime de ne rien faire. Pour les tenants de cette vision, impossible d'être *coiners*\* sans se revendiquer du camp de la règle radicalisée, où la seule « bonne » gouvernance préservant les propriétés qu'ils attendent d'Ethereum est que les équipes de développement, tant de « Slock It »

que d'Ethereum, n'agissent pas. La controverse se structure autour de ce qui est conçu au sein de l'interprétation rigoriste du « *Code Is Law* » comme deux paradoxes (Xiangfu Zhao et al. 2017, p. 3) déjà en partie soulignés (cf. section III.2.1) : à considérer la « lettre du code » comme toujours légitime, les actions de l'attaquant sont « légales » au sens de « *The DAOv.1* » ; dans ces conditions, pourquoi les qualifier d'attaques ? Le second paradoxe touche au principe d'immutabilité au cœur de ces représentations libérales-technicistes : les modifications protocolaires annoncées contreviendraient à cette propriété hypostasiée, donc à l'*« esprit du code »*, au même titre que les actions de l'attaquant. Des arguments de ce type sont mobilisés par certains pour s'opposer vocalement à tout type d'intervention, comme le 18 juin, où un de ces opposants, travesti en un attaquant auto-proclamé (dont la « *signature fantaisiste* » échoue à prouver cette identité, Buterin 2016) publie une « *lettre ouverte* » adressée à « *The DAO et à la communauté Ethereum* » où des arguments similaires assoient des menaces d'actions juridiques (Attaquant auto-proclamé 2016).

Cette « *lettre ouverte* » pointe que « *Slock It* » devrait s'en tenir aux conditions d'utilisation encadrant l'ICO stipulant leur absence de responsabilité<sup>462</sup>. Et ce, en cohérence avec l'inscription du projet dans ce type d'interprétation rigoriste du « *Code is Law* », qui a alimenté la perception d'un projet radicalement innovant et l'euphorie entourant son ICO. Des représentations libérales-technicistes sont revendiquées, tant par le projet « *Slock It* » que par ses membres, et se trouvent au fondement du design des mécanismes de gouvernance de « *The DAO* ». Dès l'origine, les références à la « *loi de Szabo* » (et au travaux de Nick Szabo) sont explicites (Jentzsch 2016b, p. 1). Les principes de conception déjà entrevus renvoient à « *un modèle de comportement humain [...] basé sur des idéologies libérales, où les humains agissent comme des agents rationnels, intéressés et sans confiance* » (DuPont 2018, p. 12). De ces fondements est née l'idée d'un fonds d'investissement vendu comme devant forcément être plus efficace car « *dirigé par un code informatique immuable, par opposition [aux] règlements fragiles et complexes* » entre entités centralisées (Tual 2016e). L'équipe de conception<sup>463</sup> et la communauté en formation y font extensivement référence. Pour beaucoup, l'intérêt fut suscité parce qu'avec « *The DAO* », « *non seulement [il] avait le code is law en pratique mais aussi dans le contrat, dans le contrat il y avait un élément qui disait[ :] si jamais il y a une différence entre la description du système [l'esprit du code pour nous, NDA] et son fonctionnement effectif [la lettre du code, NDA] c'est le smart contract\** [donc la lettre défaillante du code] qui prime. » [C. Lesage, Entretien n°22]. En conséquence, le fait que l'entité numérique attaquée soit immuable et indépendante est à l'origine une propriété, non un bogue. Des choix idéologiques ont conduit à ce qu'aucun garde-fou sécuritaire (coupe-circuit, privilège, mise à jour, etc.) ne soit implémenté, autre qu'un processus de migration, long et à quorum de participation élevé, permettant si nécessaire aux investisseurs de migrer d'une instance de *smart contract*\* à une autre contenant des mises à jour<sup>464</sup>. C'est cette même procédure

<sup>462</sup> L'*« Avis de non-responsabilité »* (*« Disclaimer »*) stipule que, sans pouvoir « *spéculer sur le statut juridique des DAO dans le monde* », reste que « *toute personne qui utilise le cadre générique de la DAO, y compris la DAO appelée "La DAO" ou toute autre DAO, le fait à ses propres risques [et] les auteurs ne sont pas un cabinet d'avocats, [ils] n'ont pas vocation à offrir des conseils juridiques [aussi, si] vous créez une DAO, ce sera votre DAO et vous serez responsable de son fonctionnement* ». Voir <https://github.com/blockchainsllc/DAO/blob/develop/README.md> [consultation au 12/06/2021].

<sup>463</sup> Certains membres de l'équipe, comme G. Green, ne cachent pas leur libertarianisme : à l'époque de sa découverte de Bitcoin, il était « *très opposé à la Réserve fédérale, au système bancaire, j'étais un mordu de l'or, vous savez, le type de gars libertarien classique et euh. Je mettais tout mon argent dans l'or et l'argent et j'ai entendu parler de cette histoire de Bitcoin* » (THE FILTER 2016). Souhaitant « *jouer le marché libre sans les gouvernements et les banques* » (*Ibid.*), il se retrouve dans la vision portée par « *The DAO* » : « *c'est le rêve du Réseau de partage universel [...] un réseau ouvert sans permission qui va permettre une véritable économie de partage* » (Griff Green and the DAO | Layer Zero 2021).

<sup>464</sup> L'existence de ce processus de mise à jour est un gage contre toute forme d'action discrétionnaire, permettant tout à la fois à « *The DAO de maintenir un code statique immuable sur la blockchain\* Ethereum, tout en étant capable d'être mis à jour si le besoin s'en fait sentir* », voir Jentzsch 2016b.

que devait emprunter la nouvelle version corrigée (« The DAO v.1.1 »), qui en l'état ne sert à rien. Puisque « ce contrat fera toujours exactement ce pour quoi il est programmé et ne pourra pas être abusé » (Jentzsch 2016b), il faudra faire avec les codes fautifs : « The DAO » est sans commandement, ni moyen de se défendre, puisqu'aucun individu ou groupe, pas même l'équipe de développement, ne dispose de priviléges exorbitants en son sein. Tous ces arguments sont mobilisés par l'attaquant auto-proclamé (2016). Il dit avoir participé à l'ICO après avoir « examiné attentivement le code de la DAO [et] découvert la fonction qui permet de récompenser le split par de l'éther supplémentaire [, fonction qu'il a utilisée afin de] réclam[er] à juste titre 3 641 694 ethers. [Il est] déçu par ceux qui qualifient de "vol" l'utilisation de cette fonctionnalité intentionnelle [car il] utilise cette fonctionnalité explicitement codée selon les termes du contrat intelligent\* [et son] cabinet d'avocats [confirmerait que son usage est] entièrement conforme au droit pénal et délictuel des États-Unis. À titre de référence, veuillez consulter les conditions de la DAO : "Les conditions de la création de la DAO sont énoncées dans le code du contrat intelligent\* existant sur la blockchain Ethereum à 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Rien dans cette explication des termes ou dans tout autre document ou communication ne peut modifier ou ajouter des obligations ou des garanties supplémentaires au-delà de celles énoncées dans le code de la DAO. Tous les termes ou descriptions explicatifs sont simplement offerts à des fins éducatives et ne remplacent ni ne modifient les termes explicites du code de la DAO énoncés sur la blockchain ; dans la mesure où vous pensez qu'il y a un conflit ou une divergence entre les descriptions offertes ici et la fonctionnalité du code de la DAO à 0xbb9bc244d798123fde783fcc1c72d3bb8c1894, le code de la DAO contrôle et définit tous les termes de la création de la DAO. » (Attaquant auto-proclamé 2016)

Quant à intervenir sur les codes d'Ethereum, la situation est claire : Ethereum n'est pour rien dans l'attaque, il « a fonctionné exactement comme prévu » (@IAMnotA\_Cylon cité par Shin 2022, p. 156). Aussi, de prime abord, au sein du « canal interne à la Fondation [Ethereum, NDA] [...] il y avait beaucoup d'opinions différentes [et selon] la plupart des gens [...] nous ne devrions rien faire, ce n'[était] pas notre problème... » [Fabian Vogelsteller, Entretien n°12]. Puisqu'il s'agit « simplement d'une exploitation du code logiciel que chaque investisseur de la DAO avait accepté » (Walch 2017b, p. 17), et qu'Ethereum - ses codes protocolaires et finalement ses équipes de développement - ne sont pas responsables (comme le précise d'emblée l'annonce de Buterin), pourquoi agir ? En outre, compte tenu de la responsabilité individuelle souveraine des investisseurs qui n'ont pas fait leur propre recherche et qui n'auraient pas dû faire confiance (cf. « Do Your Own Research » / « Don't trust, verify »), il était justifié de « laisser brûler The DAO ». Cela servirait de leçon coûteuse dans la « vie réelle » (« G. T. Blossom », 2016, cité par DuPont, 2008, p. 11). Il fallait choisir ce que la crise « The DAO » allait incarner : « Un Soft ou Hard Fork\* équivaudrait à la saisie de[s] éthers légitimes [de l'attaquant], réclamés légalement selon les termes d'un contrat intelligent\* [et] ruinerait de façon permanente et irrévocable toute confiance non seulement dans Ethereum mais aussi dans le domaine des contrats intelligents et de la technologie blockchain. De nombreux grands détenteurs d'Ethereum se débarrasseront de leur argent, et les développeurs\*, les chercheurs et les entreprises quitteront Ethereum [car] toute fourche, qu'elle soit douce ou dure, nuira [...] à Ethereum et détruira sa réputation et son attrait. [L'attaquant conclut qu'il se] réserve le droit d'intenter toute action en justice contre les complices du vol, du gel ou de la saisie illégitime de mon éther légitime, et je travaille activement avec mon cabinet d'avocats. [...] J'espère que cet événement sera une expérience enrichissante pour la communauté Ethereum et je vous souhaite bonne chance. Je vous prie d'agrérer, Madame, Monsieur, l'expression de mes salutations distinguées » (Attaquant auto-proclamé 2016).

Au sein de la Fondation Ethereum une majorité est ballotée entre l'inaction ou l'absence d'opinions claires, mais pour une petite minorité l'inaction n'est pas envisageable.

## « Sauve-qui-peut » au sein de « la lettre du code »

Certains ne peuvent se rallier aux arguments du camp précédent. De leur point de vue, cette crise et ses conséquences excèdent largement « The DAO » et sa communauté du fait du contexte : Ethereum n'en est qu'à ces balbutiements et cette crise pourrait se révéler coûteuse, voire mortelle, pour un jeune écosystème qui commence sa phase de « preuve de concept ». La petite taille de la communauté est une contrainte, et la part importante d'Ether volée par l'attaquant pose des questions économiques, réputationnelles, mais aussi juridiques. En contexte de grande incertitude réglementaire, cela pouvait conduire à ce que « *les codeurs d'Ethereum et de la DAO [soient l'objet de] poursuites judiciaires* » et, plus généralement, à créer un « *œil noir pour la technologie* » Ethereum (Walch 2017b, p. 17) : la somme « *volée représentait plus de trois pour cent de tout l'éther, ce qui aurait eu un impact négatif sur l'ensemble de l'espace et [sur] la motivation des développeurs\* qui construisent sur Ethereum [car] en même temps, tout était plus petit. [...] Si nous laissons maintenant cette chose, c'est foutu, [...] nous devons faire quelque chose, [...] imaginez que vous ayez une maison en feu et qu'il y a cent personnes debout devant... et qu'une seule décide d'entrer et d'aider le bébé ou les gens à l'intérieur...* » [Fabian Vogelsteller, Entretien n°12]. La petitesse d'Ethereum qui le met en péril devient alors une ressource en termes de coordination : « *C'était un très petit écosystème [,] tout le monde était sur le subreddit de Reddit [,] tous les développeurs\* et presque tous les projets [déployés sur Ethereum, NdA], il n'y en avait que 50 ou 100 [et] vous pouviez essentiellement connaître tout le monde [,] 200 personnes ou quelque chose comme ça [...]. Vous pouvez juste parler directement à tout le monde de tout parce que c'était juste minuscule* » [B. Summerwill, Entretien n° 26].

Ces arguments convainquent certaines figures de la communauté qu'il faut « *agir, ce n'est qu'un MVP<sup>465</sup> tout ceci n'est qu'un début, la communauté est suffisamment petite, nous pouvons résoudre le problème, pourquoi [ne] pas le faire ?* » [Fabian Vogelsteller, Entretien n°12].

## « Se sauver soi-même au détriment des autres » (2-b)

Contrairement aux arguments précédents, retenir la version la plus rigoriste du « *Code is Law* » n'impose pas l'inaction. Si ce qu'a fait l'attaquant est légitime, tout usager peut faire de même vis-à-vis de « The DAO » ou de la DAO enfant de l'attaquant. Les tenants de cette interprétation s'opposent à ceux qui voient en l'inaction la seule fin désirable justifiant qu'il est possible de ne pas remettre en cause la propriété d'immutabilité tout en intervenant (comme l'attaquant) dans le cadre strict de « la lettre des codes ». Au sein des stratégies de « sauve-qui-peut », certaines relèvent de simples stratégies palliatives et visent à atténuer individuellement les conséquences de l'attaque (2-b). Ces actions correctives impliquent une mise en œuvre brouillonne, non coordonnée et non coopérative.

Spammer le réseau\* Ethereum (2-a) permet de gagner du temps, mais en même temps que cela ralentit l'attaque, cela complique pour tout le monde les interactions *on chain\**. Bien que l'attaque ait pris fin, elle apparaît comme une « *divulgation non responsable* », qui risque d'entraîner des imitations (cf. Figure 9 ci-dessus), d'autant que des publications explicitent les mécanismes de l'attaque (Daian 2016 ; Gün Sirer 2016) : la survenue d'*« attaques par imitation »* devient *« la principale inquiétude »*, car il devient facile de « *s'inspirer de cette attaque et la reproduire à l'identique* » (Gün Sirer 2016). Ces attaques d'imitation ne manqueront pas d'avvenir d'ailleurs les jours suivants (Campbell 2016). Face à l'urgence, il est temps d'agir et la première stratégie au sein

---

<sup>465</sup> Pour « Produit minimum viable » (« *Minimal Viable Product* ») qui, dans le cadre de la conception produit, renvoie à une des premières versions mises en production afin de récolter les premiers retours utilisateurs.

des codes accessibles aux acteurs individuellement est non coopérative et sous-optimale. Elle correspond, pour les porteurs de DAO Tokens, à utiliser la fonction Split pour créer une DAO enfant en vue de récupérer les fonds investis au taux défini initialement. Chaque porteur peut initier la procédure de création d'une DAO enfant via la fonction Split qu'a utilisée l'attaquant, s'il est suffisamment compétent pour suivre la procédure explicitée sur Reddit. L'équipe du portefeuille non intermédiaire « MyEtherWallet » a en effet développé un outil simplifiant le split pour baisser les barrières à l'entrée technique (Monahan 2016 ; FelixA 2016b) Clément Lesaege [Entretien n°22] est de ces techniciens compétents (cf. biographie Annexe n°IV.4) : « *Pour moi, à l'époque, le premier impératif, c'était surtout d'essayer de récupérer les Ethers que j'avais mis dedans. [...] J'avais compris [...] qu'il y avait deux solutions [:] récupérer notre stake [ou] attaquer l'attaquant* ». Il opte « *pour Fork\*er une DAO enfant [, il a fait [s]on proposal de Fork\*ing [, et lorsqu'il] est arrivé à expiration [il] étais maintenant à un point où [il] pouvait [...] transformer les DAO tokens en Ether au bon taux* » [Ibid.]. Cependant, c'est une stratégie non coopérative à somme nulle. La récupération des fonds par ceux qui l'entreprennent accroît des pertes pour les autres restant dans l'entité originelle « The DAO » : « *au bout d'un moment, le DAO aurait été insolvable. Si tout le monde fait ça, ça ne marchait pas* » [Ibid.]. C. Lesaege finira par « *décid[er] de ne pas utiliser ces Fork\*ing proposals* » : déjà, car il « *avait peur de ce qui risquerait de se passer au sein de la DAO enfant* », ensuite, il voulait « *éviter de splitter les communautés* », enfin et surtout, il était devenu clair qu'*« Ethereum allait bien être Fork\*é »* [Ibid.].

Une deuxième solution qui consiste à attaquer l'attaquant suppose une intervention coordonnée selon une logique collective, visant à rendre difficile, voire impossible, à l'attaquant de bénéficier des fonds volés (2-c et d). Cette action devait permettre l'ouverture éventuelle de négociations en vue de la restitution totale ou partielle des fonds (2- e): « *pour ça, on aurait eu besoin de faire un vote du DAO [,] on ne pouvait pas juste le faire tout seul. Donc, l'idée, c'était de s'organiser et de créer une sorte d'équipe pour faire ça, que j'ai d'abord essayé de faire. Mais rapidement, j'ai trouvé des personnes [proches de] The DAO, le White Hat Group [à cette époque il s'agit encore du « Robin Hood Group », NdA], qui étaient déjà un peu plus avancées. On en a parlé un peu.* » [Clément Lesaege, Entretien n°22]

« *Contre-attaquer : action collective et coordonnée en vue d'un intérêt commun* » (2 – c, d, e)

À l'origine, la plupart des acteurs se revendiquent du camp de la moindre intervention, mais face à la crise, des premiers désistements de « *Curators* » arrivent, comme celui de « *Gavin* [, qui] a été le premier [suivi par] de plus en plus de gens [abandonnant] parce qu'ils pensaient que c'était trop risqué, [certains ont] ressenti [que] quelqu'un devait faire quelque chose sinon, rien ne se serait passé. » [Fabian Vogelsteller, Entretien n°12] Des membres de la cellule de crise se constituent en un groupe de *Pirates* à « *Chapeau Blanc* » (*« White Hat Group » ou WHG* ; Campbell 2016 ; Karapetsas 2016b ; Bitmex Research 2017b ; Muratov et Vogelsteller 2016). Ce premier groupe, qui se recomposera au gré des évènements à venir, est nommé le « *Robin Hood Group* » [:] « *ce n'était pas seulement* [Fabian Vogelsteller], *c'était Alex* [Van de Sande, qui propose le nom comme une plaisanterie, Entretien n°13], *c'était Jordy* [Baylina], *c'était Griff* [Green] » (pour ceux publiquement identifiés RHG ci-après, cf. Tableau 10 suivant) et ils se sont « *dit ok faisons quelque chose* » [Fabian Vogelsteller, Entretien n°12]. Ces acteurs (identifiés ou non) précisent que cette intervention « *n'est pas officielle [,] il s'agit d'une action collective menée par des individus qui ne représentent aucun de leurs employeurs* » (Van de Sande 2016a). La contre-attaque est constituée de deux volets distincts jouant sur le fait que « *l'attaque [...] fonctionnait dans les deux sens* » : l'exploitation de la même vulnérabilité de réentrance doit permettre, d'un côté, de « *sécuriser* » les fonds restants encore susceptibles d'être volés et, d'un autre côté, de « *hacker en retour* » la DAO enfant de l'attaquant [V. Zamfir, Entretien n° 9] afin de l'empêcher de récupérer les gains

escomptés, avec en ligne de mire : la poursuite de « *négociations* [...] avec l'attaquant ou [la survenue d'un] Fork\* » (2-e; Karapetsas 2016d).

Ces opérations opèrent dans le cadre du « *Code is Law* », prenant l'attaquant à son propre jeu. On trouve les justifications de cette riposte dans l'annonce faite par « *Slock it* » (*Ibid.*). Le premier volet de l'intervention s'adresse aux « *détenteurs de jetons DAO* » qui voudraient agir « *au cas où le Soft Fork\* ne serait pas mis en œuvre* » (*Ibid.*) : dans l'éventualité où il ne serait « *pas implémenté, la communauté* [The DAO reste en capacité d']*empêcher l'attaquant de retirer ses ETH, même après l'expiration de la période de 27 jours, en [rejoignant sa DAO enfant]*. *Cette solution n'est pas complète et n'aboutira probablement jamais à la restitution de l'ether volé aux DTH d'origine, mais elle empêchera au moins l'attaquant de percevoir des bénéfices.* » (*Ibid.*). L'annonce précise que cette intervention a peu chance d'aboutir, « *le timing est essentiel* », la communauté *The DAO* n'a que « *25 jours avant que la phase de création de la DAO enfant de l'attaquant ne se termine* » (*Ibid.*) et, d'ici là, un ensemble d'actions devra être réalisé (*Ibid.*). C'est encore par exploitation de la vulnérabilité de réentrance qu'est entrepris le deuxième volet, qui correspond à un sauvetage des fonds encore vulnérables : la contre-attaque du RHG, lancée dans le secret le 20 juin, sera rendue publique le 21 juin (Karapetsas 2016b ; FelixA 2016a ; Muratov et Vogelsteller 2016 ; Campbell 2016) : « *THE DAO EST EN TRAIN D'ÊTRE DRAINÉ EN TOUTE SÉCURITÉ. NE PANIQUEZ PAS.* » (Van de Sande 2016<sup>466</sup>) Cette opération prend la forme de « *deux siphonnages [...] effectués sur la DAO [permettant qu'] un total de 7 630 479 ETH [soit] placé dans des DAOs enfants [...] actuellement sous contrôle (principalement) ami* » (Karapetsas 2016b ; Buterin 2016a ; Shin 2022, p. 143). Le RHG promet : « *dès que cette DAO aura atteint sa maturité, nous essaierons de transférer tous les fonds dans un contrat de remboursement* » (A. Van de Sande, cité par Campbell 2016) permettant à leur propriétaire légitime (les porteurs de DAO Tokens) de les réclamer. La situation est stabilisée pour un temps seulement. Si les ETH sont « *en sécurité pour le moment* », « *un Soft Fork\* ou un Hard Fork\* est nécessaire pour les sécuriser pleinement* » (Karapetsas 2016b). La vulnérabilité reste présente dans tous les codes des DAO enfants créés, « *les fonds [sont] en danger indéfiniment [:] la répétabilité de l'attaque par réentrance dans les deux sens* » fait craindre à l'équipe une « *guerre de DAO* » : que l'attaquant riposte, imposant encore d'agir et que « *la situation [dure] éternellement* » (C. Jentzsch, cité par David Z. Morris 2023). L'attaquant leur donne raison. Le 22 est annoncé qu'il a donné « *de l'éther à la DAO et [rejoint ainsi] l'un des splits whitehat* », mais la communauté est enjointe à ne pas « *paniquer* », « *tout autre mouvement que l'attaquant essaierait de faire se produirait après 24 jours* », « *cela [...] donne plus de temps qu'il n'en faut pour mettre en place un Fork\** » (Karapetsas 2016c).

---

<sup>466</sup> Voir <https://x.com/avsa/status/745313647514226688>, un usager lui répond : « RIEN NE DIT MIEUX "NE PAS PANIQUER" QUE LES MAJUSCULES » (voir <https://x.com/KyleRiecker/status/745343956528037888>, repris par (Russo 2020, p. 200)).

**Tableau 10 : Les différents acteurs de la contre-attaque**

| Organisations   | Action(s) entreprise(s)   | Nom et prénom  |
|---|---|--|
| « Robin Hood Group »<br>ou RHG<br>(1 <sup>er</sup> groupe)                        | Mise en œuvre d'une stratégie de sécurisation des fonds et de contre-attaques   | Baylina Jordi<br>Green Griff<br>Karaptetsas Lefteris<br>Alex Van de Sande<br>Vogelsteller Fabian |
| « White Hat Group »<br>ou WHG<br>(2 <sup>ème</sup> groupe, cf. section suivante.) | Mise en œuvre de la restitution des fonds sauvegardés   | Baylina Jordi<br>Green Griff<br>Karaptetsas Lefteris   |
| Entreprise « Bity »   | Facilitation des opérations des deux groupes :<br>- Représentation et conseil juridique<br>- Aide à la sécurisation et à la conversion des fonds sous contrôle (Vente <i>via</i> les comptes de Bity) | Bochsler Gian<br>Roussel Alexis  |

Source : Rolland Maël

Le drainage des fonds de « The DAO », deuxième volet de la contre-attaque, marque la fin de ce qui n'est que la première phase du sauvetage, celle du « Robin Hood Group ». À ce point, tous les acteurs attendent la survenue d'un *Fork*\* (et certains y travaillent) pour régler définitivement la crise. Et tous postulent (et soutiennent l'idée) qu'un *Soft Fork*\* suffira. Ils se trompent, un *Hard Fork*\* sera finalement nécessaire, d'où un piratage blanc décomposé en deux temps : « *avant et après le Fork*\* ». Ainsi, le WHG ne réapparaîtra que tardivement, après le HF et le maintien-surprise de l'ancienne chaîne.

### III.3.3 Gouvernance ouverte et publique pour des *Forks* controversés

Les voies de remédiation précédentes sont difficilement critiquables du point de vue rigoriste du « *Code is Law* » car, que l'on reconnaissse ou non les faits comme relevant d'une attaque illégitime, elles sont effectuées légitimement dans le cadre de la « lettre » des codes. Mais, de ce fait, leur efficacité est relativement faible : partielles, elles se limitent à réduire les pertes et non à recouvrer les fonds volés. Sur les deux volets de la contre-attaque, seul le second est un succès : près de 70% des ETH dans « The DAO.v1 » sont contrôlés. Parallèlement et dès le déclenchement de l'attaque, les acteurs savent (Zamfir l'avait même anticipé<sup>467</sup>) qu'une remédiation totale est à portée *via* la dernière famille de stratégies : « Fork\*er », c'est-à-dire faire évoluer radicalement les règles protocolaires, hiérarchiquement supérieures aux règles de « The DAO.v1 » contenues dans sa couche base de données (cf. Annexe n° V.6) pour régler la situation. À l'efficacité de ces modifications répond un encadrement et des contraintes de coordination communautaire élevées, du fait d'attendus renforcés en termes de discussion, de publicité, de quorum.

#### « *To Fork or not to Fork* »<sup>468</sup> : enjeux et controverses théoriques autour des *Forks*

Les stratégies consistant à intervenir directement sur la lettre du code d'Ethereum sont considérées comme radicales et, de ce fait, sont controversées. Pour toute communauté *coineuse*, ce type de modification est considéré comme « critique » en ce qu'elles touchent aux règles consensuellement acceptées librement par l'ensemble des usagers (ici les *etheristes*). Le cas de crise précédent à mis au jour, pour Bitcoin, l'institutionnalisation de la procédure particulière des « *Bitcoin Improvement Proposal* » (BIP) encadrant ces modifications (cf. section III.2.1). La plupart des communautés de CM reprennent à Bitcoin cette procédure formelle en l'adaptant ; Ethereum n'y dérogera pas avec la procédure des « *Ethereum Improvement Proposal* » (ou EIP). Mais, en ce début de phase de « preuve de concept », cette dernière manque encore. Dans le jargon des *coiners*\*, ces évolutions sont aussi qualifiées de *Fork*\*, car elles impliquent de « *copier un programme [logiciel] existant et d'en distribuer une version modifiée* » (Nyman2015, p. 1 ; cité par Walch, Kuo et Deng 2017, p. 14) selon la pratique de bifurcation de code au sein des répertoires des forges logicielles, qui permet de créer une nouvelle version ou un nouveau logiciel indépendant (si les droits accordés le permettent). À la faveur d'un processus de normalisation commencé par les *bitcoiners*\* (autour de la classification et de l'encadrement des BIP justement, voir Andresen 2012 ; Timón 2015 ; Lombrozo 2015 ; Lombrozo 2017) et poursuivi par des *etheristes* (Buterin 2017c), ces *Forks*\* se répartissent en deux grands types : les *Soft Forks*\* et les *Hard Forks*\*.

Un *Soft Fork*\* correspond à toute modification qui réduit strictement le nombre de transactions\* valides au sein de l'ancien protocole, là où un *Hard Fork*\* rend valides des transactions\* et des enregistrements qui ne l'étaient pas dans l'ancien protocole (Buterin 2017c). En conséquence, dans le cadre d'un *Soft Fork*\*, les nœuds\* qui suivent les anciennes règles restent compatibles avec le protocole de registre\* distribué, « *de sorte que tous ceux qui ont déjà le même logiciel peuvent en principe le valider dans la mesure où ils le peuvent, [...] personne n'est lésé, les règles sont essentiellement les mêmes* » [J. Song, Entretien n°14]. Bien qu'une majorité de nœuds\*

---

<sup>467</sup> Vlad Zamfir, dans son opposition théorique à la loi de Szabo et en affirmation de sa « loi crypto », a toujours milité pour que les modifications protocolaire soient de type *Hard Fork*, car elles objectivent la dimension socio-politique de la gouvernance des CM. Depuis ce positionnement, il poste sur Twitter/X dès le 14 mai 2016 le message mi-sérieux, mi-provocateur suivant : « *la communauté ferait-elle un Hard Fork d'Ethereum s'il y avait un bug critique dans le DAO ? :p* » (Zamfir 2016) ; à quoi on lui répond : « *Je me demandais la même chose. Ça ne va pas être joli. :(* » (de la Rouvière 2016)

<sup>468</sup> Titre d'un billet de blog de Polrot (2016a) du 27 juin 2016, pour Ethereum France ; et de Jeffrey Wilcke publié pour la Fondation Ethereum, le 15 juillet 2016.

doit se mettre à jour pour rendre exécutoires les nouvelles règles, leur qualité de rétrocompatibilité font que les contraintes de coordination et de coercition sont faibles : « *les Soft Fork\* sont plus pratiques pour les utilisateurs, car [ils] n'ont pas besoin d'effectuer une mise à jour pour rester sur la chaîne* [, ils] sont moins susceptibles de conduire à une scission de la chaîne [et] ne requièrent réellement que le consentement des mineurs/validateurs » (Buterin 2017c). À l'inverse, bien que les *Hard Forks\** « *offrent aux développeurs\* beaucoup plus de souplesse dans la mise à jour du protocole, car ils n'ont pas à veiller à ce que les nouvelles règles “s'intègrent” dans les anciennes règles* », les contraintes de coordination et de coercition sont fortes : ils « *requièrent le consentement des utilisateurs (opt-in)* » et tous sont dans l'obligation de se mettre à jour, sans quoi ceux opérant des nœuds\* obsolètes, dorénavant non compatibles, participeront d'un protocole de registre\* distribué et d'une CM distincts suivant des règles de consensus différentes de la majorité (Buterin 2017c). Cette coercition, les *bitcoiners\** disent la rejeter. Ce type d'évolution n'est rien que « *le lancement d'une nouvelle pièce, parce que cela n'est pas rétrocompatible, vous commencez quelque chose de nouveau* [...] *on peut ajouter de nouvelles pièces, on peut en éliminer d'autres, on peut modifier le calendrier d'approvisionnement, on peut faire n'importe quoi.* [...] *Quand vous avez quelque chose comme Ethereum qui HF de temps en temps, ils peuvent changer les règles* [...] *cela signifie que s'ils le veulent, ils ne le feront sûrement pas, mais s'ils le veulent, ils pourraient dire, ok, le gouvernement de la Russie peut obtenir cent millions d'Ethereum et ainsi de suite* » [J. Song, Entretien n°14]. Ceci explique chez eux une préférence pour les *Soft Forks\** rétrocompatibles, gages d'une souveraineté hors coercition : tout *bitcoiner* conservait tout à la fois la possibilité de ne pas accepter les mises à jour et la possibilité de participer au consensus de son nœud. Cependant, cette affirmation participe davantage d'une mise en récit. Bien qu'on « *entend souvent dire que l'on peut utiliser la toute première version du logiciel Bitcoin et qu'elle sera compatible avec le réseau\** actuel [...] *la véritable réponse est beaucoup plus compliquée et nuancée* » ; certaines modifications délicates seront nécessaires et le résultat incertain (Lopp 2022). En outre, l'histoire de Bitcoin permet de questionner la rétrocompatibilité effective de certains *Soft Forks\**<sup>469</sup> comme de reconnaître que Bitcoin aussi a connu des *Hard Forks\**, des *rollbacks* même considérant que des historiques longs de dizaines de blocs ont été rendus orphelins. Ce fut le cas de la crise « *Bitcoin bug Value Overflow* », administrée centralement par Nakamoto et dont la mise à jour, n'en déplaise à Song, forçait les opérateurs de nœuds\* (mineurs ou complets) à remplacer leurs versions locales du registre\* pour revenir à une version précédente choisie à sa discrédition (cf. section III.I.2). Ou celle dite « *CVE 2013 #3220* » (crises n° 4 et n°19 de notre Chronologie n°3), que Dino Mark mobilise contre les critiques des *Hard Forks\** de Tristan d'Agusta de Poloniex : « *c'est ce qui s'est passé avec le bitcoin en 2013. Les bourses ont annulé les transactions\** » conséutivement à la scission de chaîne (Shin 2022, p. 144).

Ce cadre qui fait des *Soft Forks\** l'outil privilégié de la gouvernance des codes protocolaires d'une CM est celui qui accueille les controverses suscitées par la question d'un *Fork\** pour remédier à la crise en cours. Le premier chapitre a montré comment Ethereum, influencé par la culture des *bitcoiners\** de 2014, se distingue de manière critique de Bitcoin. Cela ne doit pas faire oublier des continuités. Au commencement, Ethereum et sa communauté empruntent pour partie aux *bitcoiners\** le fond libéral-techniciste présenté. L'inscription du projet « *The DAO* » dans l'ethos du « *Code Is Law* » et son succès l'illustrent de manière exemplaire. C'est la survenue d'imprévus qui va imposer la solution d'un *Hard Fork\**, que bien peu d'*etheristes* soutiennent de prime abord. Pour le comprendre, rappelons-nous que, dès la conception d'Ethereum, l'évolution du protocole par *Fork\** (potentiellement *Hard*) est théorisée et même souhaitée (cf. « *difficulty bomb* », Chap. I section I.3.3) : cela s'inscrit dans un principe d'agilité visant à être moins rigide au niveau infrastructurel que Bitcoin. Pour autant, un *Fork\**, et tout particulièrement un « *hard Fork\** est [...]

---

<sup>469</sup> Certains *coiners* pointent en particulier SEgwit.

*un sujet très controversé et, pour de bonnes raisons, [il ne doit] être qu'une solution de dernier recours* » (Jentzsch 2016c). D'autres principes doivent guider la prise de décision : simplicité, universalité, modularité et, bien sûr, la réaffirmation d'un principe de non-discrimination et de résistance à la censure\*... assurant que les évolutions d'Ethereum ne servent pas à restreindre ou empêcher des catégories spécifiques d'usages et d'usagers, ou à s'opposer à des applications considérées par certains comme indésirables. Pour ceux qui considèrent que ce vol ne pose de problème qu'à « The DAO » et à sa communauté, les *Forks\** entrevus, *Soft* ou *Hard*, semblent contrevenir à ces principes. Cette situation éclaire l'embarras provoqué dans la communauté Ethereum et les critiques émanant de l'extérieur, particulièrement des *bitcoiners\**. Pour nombre de *coiners\**, le HF n'est légitime ni dans son fond, ni dans sa forme. Dans le fond, « *le hack de DAO [est singulièrement] différent* », [car avec ce] *hard Fork\**, *ce n'est pas la compatibilité avec la version précédente qui est en cause, c'[est] essentiellement un renflouement pour les gens qui ont fait un investissement dans DAO, qui s'est avéré avoir une faille [afin de] s'assurer que 16% de tout l'Ether qui était dans le DAO Hack ne soit pas drainé.* » [J. Song, Entretien n°14]. Leur conclusion sur la forme est tout aussi définitive. Corallo affirme qu'avec « *le DAO Hack [...] c'est un cercle étroit de développeurs\* qui [aurait] décidé qu'il y avait une sorte de communauté [, mais] la priorité absolue n'était pas la communauté décide [, c']était prenons une décision et espérons que nous pourrons impliquer la communauté partout où nous le pourrons* » [Entretien n°15]. Phuc de généraliser : pour lui, « *sur Ethereum, quand tu as besoin d'un correctif d'urgence [...] ben les développeurs\*, ils prennent l'initiative ils développent le truc [...] ils vont appeler les différents clients quoi et puis cela sera appliqué le lendemain il n'y aura pas de discussion en général. [...] On leur pose moins de questions que chez Bitcoin* », ce qui démontrerait leur « *pouvoir [...] d'influencer le code dans une direction ou dans une autre.* » [M. Phuc, Entretien n° 19]. Les *bitcoiners\** considèrent ainsi que la gouvernance de cette crise relève de l'imposition par le haut de modifications protocolaires à tous les utilisateurs, par un pouvoir centralisé et technocratique gisant dans la main des « Core Devs » d'Ethereum.

Pourtant, cette crise d'« évolution » implique, à la manière de celle rencontrée par Bitcoin, une gouvernance ouverte polycéphale, mobilisant des acteurs de nos différents domaines infrastructurels (cf. Chap. I section I.2). Aux enjeux de légitimité des modifications s'ajoutent des contraintes de coordination élevées. Ces mêmes groupes devront participer aux prochaines étapes de la production d'un consensus, qui s'avère de fait complexe et problématique, car, quoiqu'en disent les *bitcoiners\**, Ethereum repose sur une multiplicité d'implémentations clients, donc autant d'équipes de « Core Devs » indépendantes, qui doivent dès lors s'entendre et coopérer, dans la production d'un Fork\* que la communauté devra valider.

### **La production d'un Fork : processus incertain, multi-acteur et multiniveau**

Intervenir sur la lettre des codes protocolaires n'est pas du même ordre qu'agir au sein des codes. Toute la communauté Ethereum est de fait impliquée dans la résolution, pas seulement la partie (même importante) des participants à « The DAO ». L'implémentation d'un *Fork\** - *Soft* ou *Hard*, est un processus hors de portée de la communauté « The Dao » et de l'équipe « Slock It », justifiant en parallèle les attaques en « Chapeau Blanc » au cas où il n'aboutirait pas. La création d'un correctif repose sur les équipes de développement des implémentations logicielles d'Ethereum, et s'appuie sur le même type de maintenance que celle évoquée pour Bitcoin. Cette maintenance, avec quelques différences, repose sur les mêmes types d'acteurs (les « Core Devs »), de dispositifs socio-techniques (des « *repo Github* ») et de procédures d'encadrement. Les *Forks\** de « The DAO » n'ont pas suivi la procédure des IEP censée encadrer les modifications protocolaires radicales, puisqu'elle n'était pas encore institutionnalisée. C'est cette résolution qui en posera les bases, à partir des dispositifs et procédures *ad hoc* mis en place afin d'assurer au *Fork\** une

légitimité communautaire maximale. Cette famille d'interventions nous place dans une crise d'« évolution » à gouvernance publique (donc dans un cadre proche de la procédure des BIP synthétisée en Figure 13). La controverse ouverte immédiatement au déclenchement de la crise montre que la reconnaissance d'une transgression de la lettre des codes d'Ethereum à leur esprit n'est pas évidente pour la communauté. Diagnostics et solutions ne sont pas confinés aux « Core Devs » d'Ethereum, mais relèvent d'un problème public et de négociations communautaires ouvertes en urgence. La production d'information, les arènes de débats et la formation d'évaluations partagées (en débats) excèdent, dès le début, le cercle des développeurs\* et vont même au-delà de la cellule de crise. Cette dimension globale se reflète aussi dans les profils des participants aux discussions préliminaires desdites cellules de crise, qui couvrent l'ensemble des groupes de parties prenantes de la gouvernance d'une CM, que nous avons déjà cernés : médias et chercheurs, développeurs\* (couches applicative et protocolaire), utilisateurs finaux, mineurs et assimilés, services marchands et passerelles\*. Contrairement à la gouvernance de « huis clos » et sans être à l'époque formellement encadré, il apparaît d'emblée que le consensus se doit d'être global et non local. Les équipes de « Core Devs » sont d'abord réticentes, considérant qu'il n'est pas de leur ressort d'influencer un tel choix communautaire : le *Soft Fork*\* et le *Hard Fork*\* discutés par la communauté seront produits en parallèle, les *etheristes* trancheront. La participation des composantes communautaires dans les débats et décisions s'est réalisée au travers d'une variété de médias et d'arènes de discussion, ainsi que d'une pluralité de dispositifs de mesure du consentement (*on chain*\* et *off chain*\*) pour impliquer au-delà du cercle des opérateurs du traitement des transactions\*.

Dans les débats initiaux, un *Soft Fork*\* est privilégié par les protagonistes. Si un *Hard Fork*\* représente pour Tual, comme pour d'autres, « *la voie la plus simple, la plus rapide et la plus sûre* », pour la majorité il est « *l'option nucléaire* ». Le risque est trop grand « *de diviser la communauté* » alors que le *Soft Fork*\* annoncé suffit à limiter la perte à « 30% [ce qui apparaît] parfaitement acceptable » (Shin 2022, p. 165). Ce *Soft Fork*\*, annoncé par V. Buterin (2016) le 17 juin, doit encore être spécifié, implémenté dans des codes protocolaires et publié avant de passer l'épreuve de la légitimité communautaire. Dans le cas d'Ethereum, ces activités vont mobiliser, non quelques membres d'une équipe unique de développement, mais différents types de contributeurs plus ou moins intégrés dans des équipes de développement différenciées. La « *spécification initiale a été réalisée [...] par Christophe Jentsz* [, qui] avait le plus grand intérêt à faire disparaître ce problème [qui entachait] sa réputation personnelle et son travail [: il] demandait à tout le monde [de] faire quelque chose [...] et il [fut] celui qui a [coordonné l']équipe sur la spécification » [Fabian Vogelsteller, Entretien n°12]. La spécification du *Soft Fork*\* seul ne suffit pas, il faut encore la traduire en code protocolaire. Mais voilà, si Bitcoin est structuré autour de l'implémentation hégémonique « *Bitcoin Core* », vendue comme garante d'une meilleure stabilité du protocole, les *etheristes* y voient une centralisation risquée : « *le problème que vous avez [, c'] est que le Core client de Bitcoin, c'est le standard. [...] C'est comme si Bitcoin est décentralisé, mais il ne l'est pas* » puisque vous n'avez qu'un « *groupe de développeurs*\* principaux [qui] vont décider de ce qui se passe. » [B. Summer Hill, Entretien n°26]. Ethereum a choisi *a contrario* d'« *avoir des clients multiples* » et donc différentes équipes avec différents intérêts et points de vue [B. Summerwill, Entretien n°26, cf. Tableau 11 suivant]. Avant même le lancement d'Ethereum coexistait une diversité d'implémentations protocolaires indépendantes, avec « *Vitalik qui faisait un client Python, Gav qui faisait un client C++, Jeff qui faisait un client en Go, tout en parallèle* » [B. Summerwill, Entretien n° 26]<sup>470</sup>. Cette diversité s'explique parce qu'il est « *plus facile de faire un client Ethereum qu'un client Bitcoin* », car Ethereum, lui, « *est complètement spécifié. On a le Yellow Paper qui*

---

<sup>470</sup> Quatre clients sont développés avant la *presale* : « *l'intention était de n'avoir que trois implémentations [, et] un membre de la communauté [...] a indépendamment proposé un client Java.* » (Buterin 2014c; Buterin 2014g)

*explique toutes les spécifications* » [S. Polrot, Entretien n°16]. À partir de ces spécifications, tout développeur\* peut rédiger une implémentation logicielle dans le langage de programmation\* de son choix : là où « *Bitcoin Core c'est [...] nul n'entre ici s'il ne fait du C++ [,] le positionnement d'Ethereum est plus universaliste. [...] Le Yellow Paper [...] décrit spécifiquement comment chaque fonction doit être implémentée, comment elles doivent se comporter et ce qu'elles doivent donner. Et donc, si on suit le Yellow Paper pour créer un logiciel, bah normalement, il est rétrocompatible avec le reste. [...] Ce qui [...] invite beaucoup de gens à s'intéresser au cœur du truc* » [de Tychet, Entretien n° 4].

**Tableau 11 : Ethereum, un réseau constitué d'implémentations diversifiées**

| Implémentation client  | Part du réseau*           | Implémentation client  | Part du réseau* |
|--|---------------------------|--|-----------------|
| <b>Geth</b><br>(+ Gexp)  | 97,44%<br>(94,89% +2,55%) | <b>Geth</b>  | 79,52%          |
| <b>Parity</b>  | 1,45%                     | <b>Openethereum.</b> (ex Parity) <sup>471</sup>  | 5,76%           |
| <b>Autres (&lt;1%)</b><br>(CPP Ethereum/Aleth ; Gshif )  | 1,09%<br>(0,11%+0.98%)    | <i>Implémentations dépréciées</i><br>(CPP/Aleth le 06/10/2021 ;  |                 |
| Sources : Rolland Maël, Données<br><a href="https://web.archive.org/web/20160718202836/http://ethernodes.org/network/1">https://web.archive.org/web/20160718202836/http://ethernodes.org/network/1</a> [consultation au 09/06/2022], traitement de l'auteur. |                           | <b>Erigon</b>  | 9.34%           |
|  |                           | <b>Hyperledger / Besu</b>  | 2.92%           |
|  |                           | <b>Nethermind</b>  | 2.05%           |
|  |                           | <b>Autres (&lt;0.2%)</b><br>(trippynode; coregeth; teth; akula; bor; ethlightnode; merp-client; bitcoind ) | < 1 %           |

Pour les *etheristes*, il est « très positif » qu'Ethereum dispose d'« énormément de clients » écrits dans une pluralité de langages de programmation<sup>472</sup> [S. Polrot, Entretien n°16] : en plus de permettre une meilleure résilience du réseau\* (en cas de faille dans une implémentation, les autres restent disponibles), cela accroît le nombre et la diversité des profils participant de la gouvernance des codes protocolaires. Et ces développeurs\* trouvent plus facilement que sur Bitcoin à être financés. Dès l'origine, ils peuvent compter sur la Fondation Ethereum, qui doit amorcer le

<sup>471</sup> Le cas *Parity* est symptomatique du phénomène de turn-over : il est développé par les équipes d'*EthCore*, l'entreprise de Gavin Wood, qui l'abandonne le 02/06/2020 pour se consacrer au développement d'un protocole concurrent d'Ethereum, *PolkaDot*. *Ethcore* a « transféré la base de code *Parity Ethereum* vers une DAO composée de développeurs\* et d'organisations » (*Parity Technologies* 2019). *Parity* devient alors « *OpenEthereum* », définitivement abandonnée en juillet 2021. (<https://ethereum.org/ka/deprecated-software/> [consultation au 09/06/2022]).

<sup>472</sup> Outre « *Parity, qui est écrit en Rust et Geth qui est écrit en Go, il y a CPP Ethereum qui est un client C++, il y a Trinity, qui est un client en Python, il y a PyEthereum qui est écrit en Python aussi, Panthéon/Pegasys que je citais tout à l'heure qui est écrit en Java, donc il y en a une multitude quoi. Il y a même un Ethereum H en Haskell.* » [J. De Tychet, Entretien n°4]

développement du protocole et, plus généralement, de son écosystème (Buterin 2014c ; Buterin 2014j). C'est la Fondation Ethereum qui, par ses statuts, doit favoriser cette diversité (Ethereum Foundation 2021)<sup>473</sup>. À l'époque, disposant des ressources tirées de la *presale*, elle finance en propre des développeurs\* et chercheurs (en freelance, comme V. Zamfir, Entretien n°9), mais aussi des équipes indépendantes, reposant sur des entités juridiques hétérogènes : « *vous avez la Fondation Ethereum [...] mais l'équipe de développement réelle était sous une entité légale différente, appelée EthDev [...] à Berlin, l'entité juridique était différente de celle de Londres, et [aussi] de celle en Hollande. L'équipe Gav se trouvait à Amsterdam [et aussi] à Berlin [où] elle s'occupait du client C++, mais aussi des tests.* [B. Summerwill, Entretien n°26]. En outre, toutes les implémentations Ethereum n'ont pas la même importance dans la structuration du réseau\*, surtout à l'époque de « *The DAO* ». Comme pour Bitcoin, une implémentation jouit d'un statut de référent : « *Geth* » écrit en GO, choisie par près de 97,5% des opérateurs de noeuds\*. Là encore, le statut d'implémentation « *focale* » relève moins d'une assignation formelle que d'une convention d'acteurs<sup>474</sup> : *Geth* est le client officiel de l'EF, sa maintenance n'a jamais été remise en cause, contrastant avec le turn-over des implémentations indépendantes (turn-over dénoté en grisé, cf. Tableau 11, ci-dessus<sup>475</sup>) et a *de facto* tenu le rôle de « *client de référence, [car il est] écrit normalement de la façon la plus lisible possible* » [S. Polrot, Entretien n°16]. À ces avantages répond un inconvénient : il est nécessaire de maintenir une parfaite compatibilité protocolaire entre des logiciels indépendants reposant sur « *des piles technologiques presque entièrement différentes entre l'équipe C++ et l'équipe GO* », par exemple [B. Summerwill, Entretien n° 26]. Alors, « *évidemment, il va y avoir des petits trucs, des petits machins, il va falloir aller regarder comment* » chaque équipe code les spécifications, « *par exemple, le python et le C++* » [J De Tychet, Entretien n° 4]. Cette « *triangulation entre la spécification et les implémentations de la spécification* » fait de l'interopérabilité un enjeu central de la sécurité d'Ethereum : « *est-ce que les clients peuvent se parler entre eux ?* » [B. Summerwill, Entretien n° 26] Cette capacité des implémentations à communiquer entre elles dépend de la capacité de coordination et de coopération des équipes, qui sont elles-mêmes soumises à des aléas personnels, mais aussi organisationnels<sup>476</sup>.

<sup>473</sup> Pour une présentation exhaustive des actions menées par l'EF, voir <https://ethereum.org/en/foundation/> [consultation au 13/06/2022] ou le premier rapport financier (Ethereum Foundation 2022).

<sup>474</sup> Cette position peut changer, « *maintenant je crois que le client de référence, c'est considéré comme étant le client Python. Parce que c'est plus lisible. Et il est aussi maintenu par la Fondation le client Python [.] Les personnes qui souhaitent développer leurs clients se basent plutôt sur la version Python de la Fondation.* » [S. Polrot, Entretien n°16] Ce statut implique des efforts particuliers pour les équipes de maintenance qui en ont la charge, en termes de clarté d'écriture payée au prix d'une moindre efficience : « *La référence, ça a été Go très longtemps, aujourd'hui Python et du coup Go a plutôt switché sur une implémentation d'exécution. Et c'était devenu nécessaire parce que, comme Parity a depuis le début été une implémentation focus performance, il commençait à y avoir une différence de performance assez forte entre les deux. Et donc Geth avait du mal à suivre Parity* » [S. Polrot Entretien n°16].

<sup>475</sup> Pour Geth, voir <https://geth.ethereum.org/>; concernant les clients dépréciés, voir <https://ethereum.org/ka/deprecated-software/> [consultation au 09/06/2022].

<sup>476</sup> B. Summerwill [Entretien n° 26] décrit comment la question de la coordination recouvre différents problèmes imbriqués : « *On m'a dit des choses sur, tu sais, sur Charles [Hoskinson, l'un des co-fondateurs exclus, cf. Chap. I section I.3.2] qui est un mauvais gars et [...] et ho Gav est égoïste et [...] vous savez, vous héritez [...] des préjugés du groupe dans lequel vous êtes [et d'un autre côté] il y avait beaucoup de vitriol et de haine ou quoi que ce soit envers la fondation [.] Entre l'équipe C++ et l'équipe GO [...] c'est comme si [elles] ne pouvaient même pas se parler. Vous avez aussi "Mist" le navigateur [dont l'équipe et celle] de Gav travaillent bien ensemble, mais vous avez comme Forteresse qui encombre la zone de Gav et vous avez cette compétition bizarre entre la Fondation et Ethdev, comme si la Fondation gardait l'argent, comme si c'était la volonté de Vitalik. Ensuite vous avez l'équipe de développement qui construit les clients. Mais il s'agissait en fait d'entités juridiques à but lucratif. EthDev UG, qui se trouve à Berlin et qui existe toujours, était [...] la société à but lucratif de Gav, [...] il y avait aussi une entité juridique à Londres. C'était un vrai bazar avec tout ce tas d'entités juridiques et il y avait à l'origine une séparation entre la Fondation, qui fournissait l'argent, et les sociétés qui s'occupaient du développement. La concurrence s'est accrue au fil du temps.* »

Les développeurs\* de l'implémentation GO Ethereum s'emparent des spécifications de Jentsch pour les traduire en un *Soft Fork*\* : « *Peter Szilagyi, [...] le bras droit de Jeff Wilcke dans l'équipe Go Ethereum, dirigeait les efforts pour [...] le client Geth* » (Russo 2020, p. 203 ; Entretien n°12). Les correctifs sont publiés le 24 juin, pour Geth (v. 1.4.8) et Parity (v 1.2.0), accompagnés d'un billet de blog de Szilàgyi (2016) intitulé « DAO Wars : Votre voix sur le dilemme du soft-Fork\* ». À partir du constat selon lequel il « *n'y a pas de ligne de conduite claire et optimale qui satisferait tous les membres de la communauté de manière égale*, [il a été décidé] de donner le pouvoir aux personnes qui gèrent Ethereum de décider s'ils soutiennent cette décision ou non ». Les versions patchées bloquent au niveau protocolaire le compte de l'attaquant, ainsi « *la communauté [pourra décider] de geler les fonds* » via l'établissement d'une « *liste blanche* » dont est exclue l'adresse de l'attaquant (*Ibid.*) : sera ignoré « *tout bloc contenant une transaction\* qui aide l'attaquant à déplacer les fonds de la Dark DAO [...,] fonds [dès lors] éliminés du système, et [seuls ceux] du White Hat Group pourront être restitués aux investisseurs de la DAO, à raison de 0,70 ether pour chaque ether investi* » (Gün Sirer, Keefer et Hess 2016). Chaque utilisateur doit décider s'il soutient l'activation du *Fork*\*. Télécharger le logiciel patché ne suffit pas, il faut exprimer son accord *via* une procédure de vote par signalement qui conduira, ou non, à son activation : ceux qui s'y opposent peuvent, au choix, ne pas se mettre à jour ou lancer les nouvelles versions en mode par défaut sans signalement<sup>477</sup>.

Malgré un soutien important, notamment des mineurs, publicisé sur les forums et via des billets de blogs (au sein des *pools* importantes, qui ont mis en place des outils de suivi de la « *distribution des votes* », comme Dwarfpool, Ethermine, Ethpool, le consensus est favorable au *Soft Fork*\* à près de 80%, FelixA 2016a), cette procédure ne parviendra jamais à son terme. Le 28 juin, Gun Sirer et d'autres annoncent publiquement que le remède est pire que le mal : le correctif introduit « *un vecteur d'attaque par déni de service* » au sein d'Ethereum<sup>478</sup>.

### **Arènes et dispositifs d'expression du désaccord : le camp du *Hard Fork*\* rallié par la majorité**

Avec l'abandon forcé du *Soft Fork*\*, la possibilité d'une intervention peu invasive s'effondre alors que la fenêtre d'opportunités, elle, se réduit. L'attaquant sera bientôt en capacité d'accéder aux fonds volés. Le *Hard Fork*\*, bien qu'impopulaire, s'érige en solution de dernier ressort, et les débats houleux reprennent de plus belle. En outre, par précaution, le développement du *Hard Fork*\* a été réalisé en parallèle de celui du *Soft Fork*\*, avec les mêmes acteurs à la manœuvre (Wilcke 2016 ; V. Zamfir, Entretien n° 9) : « *Christophe ne savait pas quoi faire [...] il est allé voir la seule personne qui aurait pu les aider à faire quelque chose à propos du Hard Fork\*. Et il a demandé à Jeffrey Wilcke [, qui de prime abord] ne voulait pas du tout faire partie de ça, il s'en fichait. Mais en même temps, il était le seul qui pouvait construire un Hard Fork\* dans ce court laps de temps* » [Fabian Vogelsteller, Entretien n°12]. Reste un double défi dans le temps imparti : convaincre

<sup>477</sup> « *Les mineurs supportant le DAO Soft Fork peuvent le faire en démarrant Geth 1.4.8 avec --dao-soft-fork. Cela aura pour effet d'abaisser les limites de gaz des blocs vers Pi million jusqu'à ce que le bloc décisif 1800000 (environ 6 jours à partir de maintenant) soit atteint. Si la limite de gaz de ce bloc est inférieure ou égale à 4M, le Soft Fork entre en vigueur et (toutes les mises à jour) les mineurs commenceront à bloquer les transactions DAO qui libèrent des fonds. Les mineurs qui ne supportent pas le Soft Fork DAO peuvent exécuter Geth normalement sans avoir besoin d'arguments supplémentaires. Ils essaieront de maintenir les limites de gaz des blocs à leur niveau actuel de 4,7 millions. Si la limite de gaz du bloc décisif est supérieure à 4 millions, le Soft Fork est refusé et les mineurs (tous ceux qui se mettent à jour) acceptent les transactions DAO qui libèrent des fonds.* » (Szilàgyi 2016)

<sup>478</sup> Avec les nouvelles règles implémentées, « *un attaquant peut alimenter le réseau avec des transactions qui exécutent des calculs complexes et se terminent par une opération sur le contrat DAO. Les mineurs utilisant le Soft Fork se verraien contraints d'exécuter, puis d'abandonner, de tels contrats sans percevoir aucune rémunération.* » (Gün Sirer, Keefer et Hess, 2016)

l'autre camp du bien-fondé de sa position et mesurer les avis communautaires exprimés. Dans les débats, très majoritairement publics, le camp de l'intervention s'affermi. Pour lui, « *la Blockchain est immuable jusqu'à ce qu'on décide qu'elle ne le soit plus* », tout le « *problème, [...] c'est qui ce "on" et comment on prend la décision ? [...] Si on veut bouger les choses, ben il faut un peu faire la démonstration qu'on a la population derrière, en tout cas l'opinion publique.* » [S.Polrot, Entretien n°16]. L'évaluation de l'assentiment communautaire est constitutif des débats autour des Forks\*. Là où, sur Bitcoin, les procédures de type vote/signalement ont été privilégiées, ne donnant la voix qu'aux seuls mineurs (et à leurs intérêts potentiellement opposés à ceux des autres composantes communautaires), la communauté Ethereum vise à définir exhaustivement ses parties prenantes pour leur donner la parole : « *ça a été tout l'objet du débat, les signaux, la recherche de signaux pour essayer de comprendre, ce que la Communauté voulait en fait. Je me souviens des heures passées à essayer de comprendre [...] quelle était la qualité, la valeur des différents signaux : il y avait les posts sur « Reddit », [...] Crypto- Twitter [...]. Il y avait par contre les votes des mineurs déjà, des pools de minage.[...] Et puis le fameux « Coin Vote », enfin « Carbon vote ». Après, il y avait tous les signaux de gens d'autorité, on va dire.* » [S. Polrot, Entretien n°16]. Aucune solution unique n'apparaît satisfaisante. D'où l'émergence d'une pluralité de dispositifs, à l'initiative de la Fondation Ethereum ou d'*etheristes* plus anonymes.

Afin de saisir la communauté dans toutes ses composantes, ces solutions se répartissent entre des dispositifs de type *on chain\**, considérés comme plus « objectifs » et d'autres *off chain\**, plus « subjectifs », dont la complémentarité apparaît essentielle pour une gouvernance équilibrée. Il est tout d'abord nécessaire de donner la parole aux opérateurs du traitement des transactions\* : ce sont eux qui, en dernière instance, rendent exécutoires les règles protocolaires, anciennes ou nouvelles. Leur voix est facile à récolter et objectivement vérifiable : la PoW\* protège des attaques sybillines, et les parts relatives de puissance de calcul pointant en faveur ou contre la mise à jour ne peuvent être truquées : « *chaque personne qui participait à la pool de minage pouvait signaler s'il était pour ou contre le Fork\*, et donc il y avait des tableaux mis à jour en temps réel, par des gens de la communauté, c'était assez bien fait. Qui là penchait plus vers le Fork\** » [S. Polrot, Entretien n° 16]. Mais le périmètre de la communauté Ethereum ne se réduit pas à ces opérateurs qualifiés. Si tous ne souhaitent pas gérer les contraintes d'une mise à jour de noeuds\* dans un écosystème balbutiant (la démarche n'était pas si ardue, nous l'avons nous-même effectuée), cela ne veut pas dire qu'ils revendiquent le silence. Tout porteur d'Ether est par définition membre de la communauté de paiement. Des dispositifs *on chain\** peuvent permettre une mesure « objective » avec des dispositifs de « *coinvote* », permettant de voter dans un sens ou dans l'autre avec ses ETH. La Fondation, qui développait un dispositif de ce type, fut coiffée sur le poteau par une solution alternative, « *Carbon Vote [...] un site Web mis en place par des Chinois, où vous pouviez voter avec la quantité d'ether* » [Fabian Vogelsteller, Entretien n°12]. Pour y prendre part, « *il fallait aller chercher son cold wallet, faire une transaction\* et dire je vote [...], le coup d'opportunité pour voter [était] assez énorme, il [fallait] se déplacer avec des clés qui sont [...] critiques pour voter et plus tu as un solde important d'Ether, plus tu vas avoir un poids important dans le carbon vote. Plus tu as un solde important d'Ether, plus tu as intérêt d'avoir un cold wallet et de les y mettre.* » [J. de Tychet, Entretien n° 4]. Ces contraintes expliquent que nous n'ayons pas voté nous-même alors que le résultat, qui n'allait pas changer substantiellement, nous convenait [cf. Annexes n°IV.1]. Bien que considérés comme plus objectifs, ces dispositifs de « *gouvernance on chain\** » apparaissaient incapables de représenter l'ensemble des intérêts présents dans la communauté, et il fut considéré que se limiter à eux serait vecteur d'affaiblissement, dessinant un système « *ploutocratique* » au profit des seuls mineurs et gros porteurs (Zamfir 2017). Pour donner la parole à des franges communautaires silencierées par ces dispositifs, les *etheristes*, de manière plus ou moins coordonnée, ont innové et mis en place un éventail de solutions *off chain\** : ouvertes à tous et plus faciles d'accès, elles sont cependant sujettes à caution, puisque non protégées des attaques sybillines et tentatives de fraude. En l'espèce, des

dispositifs de sondage sur des plateformes dédiées (comme sur change.org dès le 20 juin, réunissant 1 061 signataires), mais aussi les réseaux\* sociaux comme Reddit et Twitter, les forums de Slock It, de The DAO, etc. ont été mis en œuvre.

Ces différents dispositifs de mesure ont fait ressortir rapidement qu'une majorité importante de la communauté se rallie à l'idée du *Hard Fork*\*, qui était condamnée de prime abord. En première ligne, les « Core Devs » qui ne voulaient pas apparaître comme ceux imposant par le haut un tel changement : le Carbon Vote est déterminant, quand « *50% de tous les ethers ont voté à 80% en faveur du Hard Fork*\* [,] ça a été un signal clair pour Jeffrey : "OK, il y a une demande et je dois faire quelque chose, parce que je suis le seul à faire quelque chose". » [Fabian Vogelsteller, Entretien n°12]. Nombreux sont ceux dont les positions ont évolué au gré des débats : « *Ma première réaction a été non, bien sûr, vous ne devriez pas bifurquer. Et puis il y a eu ce mois de débat le plus intense, sur ce qu'on va faire ? [...] Je suppose que je suis venu pour les voir, vous savez, la valeur des deux côtés. [...] Il y avait des mérites des deux côtés. Et c'était en gros comme, écoutez, vous savez, la majorité des gens sont pour le Hard Fork*\*. » [B. Summerwill, Entretien n° 26]. Les figures d'influence, « *rapidement [Vitalik, Gavin, etc.] se sont mis d'accord, autour du fait de faire le Fork*\*. Et d'autant plus après l'arrêt du Soft Fork\* [...], sur tous les canaux, tous les gens que je considérais, [...] comme des gens d'autorité étaient pour le Hard Fork\* aussi. » [S. Polrot, Entretien n° 16]. Les conditions d'activation renvoient à des choix d'arrangements socio-techniques différents, selon les équipes de développement. Pour Geth, ce sont les résultats de « *l'outil communautaire carbon vote [qui seront] utilisés pour définir l'option de Fork*\* par défaut » (*Ibid.*). Du côté du client Mist, les développeurs\* décident, pour plus de neutralité, de ne « *donner aucun choix prédéfini, [mais une] fenêtre [demande explicitement] aux gens d'appuyer sur "Yes Fork"*\* ou "*No Fork*"[ : sur] environ 8 000 nœuds\*, [...] 7 900 étaient le navigateur Mist, donc les gens ont choisi [Il rigole]. C'était très clairement extrêmement démocratique... [À l'inverse de] ces théories du complot comme quoi la Fondation était impliquée dans The DAO et essayait de s'aider elle-même et tout ça, c'est des conneries. » [Fabian Vogelsteller, Entretien n° 12 ; nous-mêmes, utilisateur de ce client, avons dû effectuer ce choix].

### III.3.4 « Fork You ?! » : une scission surprise fondatrice et ses enseignements

Des résultats des débats et dispositifs d'expression du consensus / des désaccords variés mis en œuvre, il semble à tous que le *Hard Fork*\* est acquis et à une écrasante majorité. Les voix anti-*Forks*\*, en plus d'être largement minoritaires, semblent « *bizarres* », « *la moitié des gens qui postaient on les avait jamais vus avant [...] c'était assez louche, ce qui se passait sur Reddit* » contre le *Fork*\* [S. Polrot, Entretien n°16]. À tous niveaux, « *on avait une assez écrasante majorité, il me semble 98% et quelques, qui votait pour la Fork*\* [au niveau des nœuds\* mineurs se signalant, NDA]. Et ensuite les échanges se sont prononcés en disant ben nous on suivra la chaîne principale... et le jour de la Fork\*, il y avait 97% du hash\*rate qui pointait vers la chaîne Fork\*ée et 3% vers Ethereum non Fork\*ée et très rapidement on est tombé à 100% » [J. de Tychet, Entretien n° 4]. Dans ces conditions, tous attendent une simple mise à jour qui conduirait à ce que l'ensemble des nœuds\* rejoigne les nouvelles règles protocolaires. Aucun n'anticipe encore que certains acteurs continueront d'appliquer les anciennes règles, revendiquant de maintenir une chaîne minoritaire en vie et, à travers elle, la vision originale d'Ethereum.

#### Un *Hard Fork* et ses attendus théoriques

Le 20 juillet, l'heure est à la célébration : « *quel accomplissement !* » pour Jentzsch (2016a), quand Buterin (2016a) félicite « *la communauté Ethereum pour la réussite du hard Fork*\* ». Après un signalement majoritaire, l'activation du *Hard Fork*\* s'est déroulée comme programmé. Par jeux d'écritures, il doit permettre de renvoyer à un passé qui n'a jamais eu de réalité au sein de la chaîne

Ethereum, toutes les interactions réalisées avec le contrat « The DAO v.1 » depuis la conclusion de l'ICO (donc celles liées à l'attaque) et de recouvrer ses fonds dans des contrats de réclamation : « *The DAO [...], son extraBalance [...], tous les enfants [...] et l'extraBalance de chaque enfant sont encodés dans une liste L au bloc 1880000 [et au] début du bloc [...] 1920000 [...] tout l'ether de tous les comptes de la liste L sera transféré vers le compte de contrat* » (Wilcke 2016). Avec son activation est exécuté le « *changement d'état irrégulier qui [transfert] ~12 millions d'ETH des contrats "Dark DAO" et "Whitehat DAO" vers le contrat de récupération WithdrawDAO* », duquel « *les détenteurs de jetons DAO peuvent [réclamer leur] ETH à un taux de 1 ETH = 100 DAO* » (*Ibid.*). Le Hard Fork\* ne touche qu'au smart contract\* de « The DAO ». « *Ce n'est pas la même chose que si vous faites un hard Fork\* sur Bitcoin, [car] si vous voulez changer une transaction\* passée, vous devez faire un rollback et ce sont toutes les transactions\* qui se produisent après qui sont affectées. Sur Ethereum, [du fait d'un] modèle basé sur le compte, vous pouvez seulement toucher The DAO sans toucher l'argent de quelqu'un d'autre [, donc] le seul impact négatif [...] c'est que maintenant l'algorithme de consensus\* a un morceau de code supplémentaire qui dit, dans un bloc de 3 millions, faites ceci au lieu de cela* » [Fabian Vogelsteller, Entretien n°12].

Du fait de cette majorité forte en faveur du Hard Fork\*, tous anticipent le même futur proche. Il est de connaissance commune (plus théorique qu'empirique) que, si deux chaînes apparaissent avec leur propre registre\* de comptes, leurs UCN\* et leurs règles protocolaires, seules les UCN\* de la chaîne majoritaire seront considérées comme légitimes, conservant leur Tickers sur les bourses d'échange auxquelles est liée leur valeur de marché. À l'époque, les bourses d'échange affichent explicitement leur intention de suivre les décisions exprimées de la majorité. De plus, du fait d'un partage du même algorithme de consensus\*, la chaîne minoritaire et ses utilisateurs (en particulier lesdites bourses) deviennent exposés aux attaques 51%, les opérateurs concurrents de la chaîne majoritaire disposant d'une puissance de calcul bien supérieure (cf. Annexe n°V.5). Dans ces conditions, la chaîne minoritaire doit rationnellement être désertée par les usagers, mais aussi par les mineurs restants. Leur profit en dépend : « *parce que cela n'a jamais été testé auparavant, [...] quand, des années avant même qu'Ethereum existe, les gens discutaient, que se passerait-il si vous Fork\*iez le Bitcoin ? Tout le monde était d'avis que, au début, il y aurait deux chaînes, puis, à un moment donné, l'une d'entre elles mourrait [...] la grande majorité des gens s'attendaient à ce que l'une d'entre elles meure et que l'autre survive* » [Van de Sande, Entretien n°13]. Tous les acteurs confirment cette croyance, « *cela nous a pris... cela m'a pris par surprise [car les] gens qui prédisaient [...] que les deux chaînes allaient survivre [...] étaient une minorité importante.* » [Van de Sande, Entretien n°13]. À « *l'époque, je pensais [que la chaîne non Fork\*ée allait] s'étioler et mourir [...] j'ai travaillé à la Fondation Ethereum à l'époque [...] une grande partie de mon état d'esprit, de mes croyances et tout le reste a été hérité de ça.* » [B. Summerwill, Entretien n° 26]. Pourtant, quelques heures plus tard, l'inimaginable se produit. La chaîne Fork\*ée Ethereum va reprendre vie, sous l'impulsion d'une poignée de mineurs : avec le Fork\*, « *quand les réseaux\* se sont divisés... au début toute la puissance de hachage est allée dans la chaîne de Fork\* et ensuite environ 10-20% du taux de hachage est revenu [...] il y a toujours une répartition 80/20* » [F. Vogelsteller, Entretien n°12, voir la répartition entre les deux en Annexe n°III.15.1]. Les membres de la cellule de crise observant le Fork\* peinent d'abord à comprendre : « *Que se passe-t-il ? Quelqu'un perd de l'argent en minant une chaîne non rentable ? Pourquoi ?* » (A. Van de Sande Russo 2020, p. 207). Contre toute attente, une minorité de nœuds\* du réseau\* décide de continuer d'opérer l'ancienne chaîne non Fork\*ée, qui devient « *un univers parallèle où l'Ethereum pré-Fork\* rest[e] intact. Les comptes de chacun* » restent inchangés, ils disposent du même montant d'UCN\* qu'avant le Fork\* et les fonds de « The DAO » sont « *toujours bloqués dans la "Dark DAO"* », à une différence près et pas des moindres : les UCN\* administrées au sein de cette chaîne ne sont pas des « *ether [mais] la cryptomonnaie\* propre à cette chaîne parallèle* » (*Ibid.*, p. 206-207), l'*« Ether Classic »*. L'évolution de la puissance de calcul dédiée à Ethereum avant le Fork\*

qui se maintient sur l'ancienne (voir Annexes n°III.5) est une mesure de l'intérêt des mineurs pour des UCN\* qui n'ont encore aucune valeur marchande : ces mineurs « *ignor[ent] les incitations économiques immédiates* [et font le pari] que la cryptomonnaie\* de la chaîne gagnerait plus tard en valeur et qu'ils seraient compensés ». Mais ce seul pari des mineurs ne peut expliquer à lui seul cette survie. Une CM n'est pas qu'un protocole que des machines font tourner. Leur attention étant absorbée par le *Fork*\*, peu d'*etheristes* se sont souciés de l'institutionnalisation du camp dissident.

### **Un Hard Fork contentieux inédit : la sécession d'Ethereum Classic**

Le 10 juillet, en amont du *Fork*\*, un anonyme avait créé un répertoire Github appelé « *Ethereum Classic* » (ETHC). Dans un article de *Bitcoin Magazine*, Wirdum (2016) souligne que, si « *Ethereum Classic semble être une blague, destinée à faire valoir un point de vue, le projet a gagné une certaine traction, avec une base d'utilisateurs petite mais croissante sur Reddit et Slack, et avec la bourse décentralisée Bitsquare offrant son jeton - l'ether classique - comme une option d'échange* ». Sur cette plateforme d'échange, dans « *le carnet d'ordres [...] pour les transactions\* Ethereum Classic/Bitcoin, [figurent] les trois premières offres à des prix allant de 6 800 ETHC/BTC (0,10 \$ par ETHC) à 10 000 ETHC/BTC (0,07 \$ par ETHC)* » (Shin 2022, p. 190). Le 21 juillet, Buterin reçoit un mail de Greg Maxwell, le *Core Dev Bitcoin Core* qui lui propose d'acheter ses ETHC, signalant son soutien à *Ethereum Classic*. Ce mail est interprété comme un camouflet : il « *enlevait son gant et giflait Vitalik au visage* » (Srir cité par Russo 2020, p. 207). Les réseaux\* servent à populariser les ressources communautaires en construction : *sur BitcoinTalk, [l']utilisateur Seccour, [...] "bitcoiner, crypto-anarchiste et cypherpunk"* [publie] un fil de discussion intitulé "[ETHC] Ethereum Classic Speculation", [présentant] un nouveau logo [...] avec un logo similaire en double tétraèdre, mais en vert sur un fond noir [et comprend] des liens vers un explorateur de blocs Ethereum Classic, le Reddit Ethereum Classic, le Slack Ethereum Classic et le Wiki Ethereum Classic. » (Shin 2022, p. 190). Arivicco est le « coordinateur du projet ». Originaire de Russie, il conserve un strict pseudonymat parce que « *la situation juridique autour de la crypto est changeante et incertaine* » et qu'il est « *également le propriétaire de BitNovosti.com, le plus grand média crypto en langue russe, qui gère un site d'actualités, une chaîne YouTube, produit des films, etc.* » (*Ibid.*). Comme il l'explique, il n'est ni un « *troll* », ni « *l'attaquant* » : « *Il s'agit d'une initiative qui a vu le jour sur des forums en langue russe ; probablement parmi quelques douzaines de mineurs actifs, de traders et de développeurs\* travaillant dans différents aspects de la crypto* », dont beaucoup se revendiquent « *partisans d'une position crypto-décentralisatrice radicale, [ils] pens[ent] que les systèmes de blockchain devraient toujours adhérer à trois caractéristiques : l'ouverture, la neutralité et l'immutabilité* [. Selon eux] le renflouement de la DAO sape deux des trois principales propositions de valeurs de la plateforme » (Arivicco cité par Wirdum 2016). Ces positions et les griefs envers Ethereum seront explicités dans une « *Déclaration d'Indépendance d'Ethereum Classic* », publiée le 15 août (Ethereum Classic et Arivicco 2016). Bien que reconnaissant de « *la création de la plateforme blockchain Ethereum par la Fondation Ethereum et ses développeurs\* fondateurs* », cette « *communauté d'individus souverains [est] unie par la vision commune de continuer la blockchain Ethereum originale [...] sans censure, fraude ou tierce interférence* ». À partir d'une liste de ce qui a été perçu comme « *une longue série d'abus, en particulier par la direction de la Fondation Ethereum* » du fait de sa participation aux événements, cette déclaration affirme les valeurs cardinales que se fixe la communauté de paiement de cette CM sous la forme d'« *un code de principe* » : « *nous croyons en une blockchain décentralisée, résistante à la censure et sans permission. Nous croyons en la vision originale d'Ethereum en tant qu'ordinateur mondial qui ne peut pas être arrêté, exécutant des contrats intelligents irréversibles. Nous croyons en une forte séparation des préoccupations, où les Forks\* de la base de code ne sont possibles que lors de la correction des vulnérabilités au niveau du protocole, des bogues ou de la*

*mise à niveau des fonctionnalités. Nous croyons en l'intention initiale de construire et de maintenir une plateforme de développement résistante à la censure, sans confiance et immuable. [signé] La communauté Ethereum Classic »* (Ethereum Classic et Arvicco 2016).

Bien qu'« Ethereum Classic » a « franchi la partie la plus difficile de la transition post-Fork\* [en assurant] la survie de [la] chaîne », il reste beaucoup à faire du côté de son développement infrastructurel. Le 22 juillet, la communauté se dote d'un *ticker* conventionnel, l'« ETC », qui « contraste bien avec le ticker ETH qui est revendiqué par la chaîne Fork\*ée, sans lui sembler de second ordre [car il] a "l'aspect et la convivialité" de pièces importantes telles que BTC, LTC... ETC » (Arvicco 2016b). C'est le 24, quatre jours après le *Hard Fork*\*, que l'importance structurelle des passerelles\* d'échange va apparaître à tous. Pour certains, si « Ethereum Classic [...] a survécu [, c'est] uniquement parce que certaines parties se sont dit que c'était [...] des opportunités de trading supplémentaire et donc ont maintenu le truc complètement sous perfusion [:] si "Poloniex" [une bourse] n'avait pas fait ça, [...] le lister un week-end, je pense juste que personne n'aurait rien fait et le truc serait mort naturellement. » [N. Bacca, Entretien n°8]. En effet, la bourse Poloniex se dédie de ses engagements à ne suivre que la chaîne majoritaire et ouvre finalement le trading pour l'UCN\* de la chaîne concurrente : par deux tweets, Poloniex annonce dans la journée l'ouverture des paires de trading « ETC/BTC et ETC/ETH » et que « tous les utilisateurs qui avaient un solde #Ethereum au moment du Fork\* ont maintenant un solde correspondant de \$ETC » (Shin 2022, p. 194)<sup>479</sup>. Les bourses Kraken et Bitfinex suivent quelques jours plus tard, et Coinbase les rejoint la semaine suivante (Russo, p. 208), Avec les listings de l'UCN\* ETC sur la plupart des grandes places de marché, le cours remonte brutalement (Annexe n°III.15.3), ce que célèbre la communauté en formation (Arvicco 2016a). Les incitations économiques s'affermisent et stimulent l'activité de minage : dès lors et pour quelque temps, il n'est pas rare que le rendement minier d'ETC soit supérieur à celui d'ETH, conduisant des mineurs à passer d'une CM à l'autre, sans tenir compte des sous-jacents philosophiques de chacune (cf. Annexes III.5.2). Le 25 juillet, Arvicco lance une campagne de recrutement, *via* un billet de blog intitulé « Que puis-je faire pour aider le projet Ethereum Classic ? » (Arvicco 2016c). Après les passerelles\* d'échange, ce sont désormais des investisseurs/entrepreneurs qui s'intéressent au concurrent rigoriste d'Ethereum. Ce 25 juillet, Barry Silbert, l'« un des acteurs les plus influents de l'industrie du bitcoin, [et fondateur du] Digital Currency Group (DCG), qui investissait dans toutes sortes d'entreprises du secteur », annonce publiquement sur twitter un premier investissement dans les Altcoins\* : « J'ai acheté ma première monnaie numérique non bitcoin... Ethereum Classic (ETC). À 0,50 \$, le rapport risque/rendement m'a semblé bon », avant d'annoncer que « Genesis Trading », qui lui appartient, facilitait les transactions\* OTC d'ETC de gros (25 000\$ minimum, Shin 2022, p. 197). D'autres profils de poids, également « hostiles à Ethereum », viendront en soutien à Ethereum Classic : l'ex co-fondateur d'Ethereum devenu entrepreneur dans le secteur, « Charles Hoskinson, toujours mécontent [...] depuis son expulsion deux ans auparavant » tweete qu'il « n'aurai[t] jamais pensé tweeter cela... [il] réintègre Ethereum pour commencer à apporter des contributions à Classic » (*Ibid.*).

---

<sup>479</sup>Son CEO, « *Tristan [d'Agosta] était [intéressé] de voir comment Ethereum Classic fonctionnerait [et a donc] codé un smart contrat de split* » permettant de sécuriser la procédure de fork contre un risque particulier lié à ce type de fork : les attaques par rediffusion (ou « *replays-attacks* ») permettant à un attaquant d'intercepter des données de transactions valides diffusées publiquement sur l'une des chaînes, afin de les rediffuser modifiées dans l'autre afin de voler les fonds. Toutes les bourses listant l'ETC n'implémentent pas rapidement ce type de sécurité et « *il y a des gens qui ont perdu de l'argent sur d'autres exchanges puisque justement les autres exchanges n'avaient pas encore fait leur « split » correctement [...] il me semble que Coinbase a perdu de l'argent suite à ce problème* » [N. Bacca, Entretien n° 8].

## Se séparer pour mieux se retrouver : fin d'une remise en ordre et ses enseignements

Du côté d'Ethereum, le retour à la vie d'*Ethereum Classic* pose de nouveaux ou plus exactement d'anciens problèmes au groupe du WHG : sur cette chaîne, « *the DAO Wars* » est toujours en cours, ils ne pourront empêcher l'attaquant de retirer ses ETC et, de leur côté, ils se retrouvent à devoir administrer des fonds liés au sauvetage libellés en ETC. C'est cette tournure prise par les événements qui conduit beaucoup des membres du « *Robin Wood Group* » à se désengager : le sauvetage des fonds sur Ethereum a été réalisé, ce qui se passe sur *Ethereum Classic* ne relève ni des mêmes considérations, ni des mêmes risques et incertitudes, particulièrement juridiques.

Le deuxième groupe, plus restreint, dit « *White Hat Group* », est alors constitué (cf. Tableau 10, Russo 2020, p. 207 ; Shin 2022, p. 202). « *Slock It* » s'était rapproché de Bity à des fins de conformité légale. Le WHG engage alors la même équipe pour « *protéger, sécuriser et plus tard distribuer les fonds équitablement sous une structure juridique suisse indépendante* » (Baylina, dans un post du 11 août, cité par Russo 2020, p. 209). Cette volonté de protection fait suite au fait que certains ont reçu « *des menaces juridiques, [...] et [Bity] a reçu des menaces [de] deux cabinets d'avocats [...] un en Suisse et un aux États-Unis [qui] étaient liés aux ETC.* » [A. Roussel, Entretien n° 11]. Restituer les fonds en Ether était assez simple et peu controversé. Mais le fait que lesdits fonds sont désormais dédoublés dans le monde parallèle d'*Ethereum Classic* pose des questions inédites, dont la première pour le WHG est de savoir s'ils restituent les fonds directement en ETC, sur la chaîne ETC, ou s'ils les convertissent en ETH et restituent sur le réseau\* Ethereum. Avec le *Fork\**, le WHG se retrouve à administrer « *7,2 millions d'ETC, soit environ 15 millions de dollars à l'époque, dans leur DAO enfant [afin de les] rendre à leurs propriétaires* » (Russo 2020, p. 207).

Cette période *post-Fork\** présente « *un risque légal beaucoup plus élevé* » [A. Van de Sande, Entretien n°13]. L'option d'une restitution sous forme d'ETC apparaît la plus simple, « *mais après avoir discuté de la question avec Bity, ils ont décidé qu'ils devraient retourner les fonds en ETH [car, d'après] Griff, les investissements avaient été faits en ether, donc ils devraient être libellés en ETH* ». À cela s'ajoutait bien entendu une forte « *animosité générale envers Ethereum Classic* », dont la majorité pensait que l'UCN\* allait perdre sa valeur rapidement et que ce n'était qu'une CM « *soutenue par les soi-disant maximalistes\* Bitcoin qui voulaient voir Ethereum échouer ; ils ne voulaient pas contribuer à son succès en distribuant l'ETC aux investisseurs DAO* » (Russo p 209.). Vendre près de « *7,2 millions d'ETC sur le marché du jour au lendemain n'était pas facile* », le WHG et Bity arrivent à échanger seulement 14% des fonds en ETH et en BTC « *avant que les bourses de crypto-monnaie Poloniex et Kraken ne gèlent les comptes de Bity pour examiner les transactions\** » (*Ibid.*, p. 209). Les fonds seront finalement libérés quelques jours plus tard afin d'être redistribués en ETC : au vu de la controverse et des difficultés suscitées, l'équipe échange ses ETH et BTC en sens inverse début septembre, l'opération réalisant même un profit. C'est le 13 août que Roussel (2016a) annonce le déploiement du « *Withdraw Contract* » sur *Ethereum Classic*, permettant de réclamer ses ETC contre ses DAO Tokens : « *ce contrat de retrait [,] déployé le 30 août [donnera à] tous les utilisateurs [...] 6 mois à partir de ce jour pour réclamer leur remboursement* » (*Ibid.*). Le 5 septembre, l'attaquant retire « *3,6 millions d'ETC, soit environ 5,5 millions de dollars à l'époque [...] du « dark DAO » sur la chaîne Ethereum Classic [et] une fois de plus fait un doigt d'honneur à Ethereum [réalisant un] don de 1 000 ETC au fonds de développement Ethereum Classic* » (Russo p. 2010). Le 6 septembre, les derniers fonds en possession du groupe sont versés au « *withdrawContract* » (Roussel 2016a). Le 30 janvier 2017, le délai d'activation du « *WithdrawContract* » servant à la résitution des ETC est étendu de deux mois, car si il « *a été largement utilisé par la communauté [avec] plus de 6 millions d'ETC [...] retirés, mais il y a encore des transactions\* de retrait quotidiennes* » (Roussel 2017b). C'est finalement

le 15 avril 2017, avec la désactivation du « WithdrawalContract », que le travail de remise en ordre prend fin pour le WHG (Roussel 2017a).

La crise semble éteinte et les inquiétudes restantes attendront encore quelques mois avant d'être levées. Cette crise est hantée par les questions juridiques et réglementaires (ce qui illustre que les autorités de régulation participent indirectement du cadre de la décision des acteurs de la gouvernance *sur l'infrastructure*, d'où leur présence en légende de la Figure 13, pour Bitcoin) : c'est le cas lorsque l'équipe de « Slock It » se pose des questions liées à la levée de fonds, quant il s'agit de qualifier les DAO Tokens en des titres, mais aussi quand se pose la question du statut juridique de « The DAO », ou de la constitution de DAOLink comme véhicule permettant les interactions économiques. Enfin, les responsabilités dans la gestion de crise ont été interrogées et sont sources de menaces ; il en est de même pour ce qui est du WHG et de leurs différentes interventions. Tous les acteurs seront fixés le 25 juillet 2017, avec la publication d'un rapport d'enquête sur « The DAO » par la SEC (d'où le choix d'arrêter notre Chronologie 5 de cette remise en ordre à cette date) : enquêtant « *pour savoir si la DAO, une organisation non constituée en société, Slock.it UG ("Slock.it"), une société allemande, les cofondateurs de Slock.it et des intermédiaires pourraient avoir enfreint les lois fédérales sur les valeurs mobilières [,] la Commission a décidé de ne pas prendre de mesures d'exécution dans cette affaire sur la base de la conduite et des activités dont elle a connaissance* », alors même qu'elle reconnaît avoir « *déterminé que les jetons DAO sont des valeurs mobilières en vertu de la loi sur les valeurs mobilières de 1933 ("Securities Act") et de la loi sur l'échange de valeurs mobilières de 1934 ("Exchange Act")* » (Securities and Exchanges Commission 2017). Le rapport finit par rappeler un ensemble de réglementations afférentes et par inciter tous les acteurs qui « *utiliseraient une organisation autonome décentralisée ("Entité DAO"), ou d'autres moyens basés sur le ledger distribué ou la blockchain pour lever des capitaux, à prendre les mesures appropriées pour assurer la conformité avec les lois fédérales américaines sur les valeurs mobilières* » (*Ibid.*).

Cette crise du *Hard Fork*\* consécutif à l'attaque de « The DAO » est à la fois fondatrice pour *Ethereum* et *Ethereum Classic*, mais, plus généralement, pour l'écosystème crypto-monétaire. Derrière cette sécession protocolaire et communautaire inédite se cache d'abord la résolution d'un conflit idéologique traversant la communauté originelle d'*Ethereum* [V. Zamfir, Entretien n°9]. Dès la conception et durant cette phase de preuve de concept, il y a encore « *deux Ethereum [reposant sur] deux visions différentes [...] coexista[nt] au sein du même projet [ :] certaines personnes étaient attirées par l'idée d'Ethereum en tant que Bitcoin programmable [, d'] autres voyaient Ethereum comme un "ordinateur mondial", une sorte d'Amazon décentralisé pour les applications (Dapps)* » [B. Summerwill, Entretien n° 26, mobilisant une présentation de Charles Hoskinson]. Cette crise va révéler que cette coexistence n'avait de pacifique que l'apparence. Ces sous-communautés ont finalement affirmé leur identité comme communautés de paiement séparées, « *ces deux visions bien que toutes deux intéressantes, étaient "mutuellement irréconciliables"* » [*Ibid.*]. Et c'est grâce au *Hard Fork*\* contentieux, et à la sécession monétaire qu'il permet, que ces communautés de paiement ont pu retrouver le semblant d'homogénéité en valeurs nécessaire, que la crise avait fait voler en éclat. Du côté d'*Ethereum* et malgré une culture *bitcoiners*\* qui leur faisait préférer la moindre intervention, la grande majorité se range du côté de la solution la plus radicale du *Hard Fork*\*, afin d'assurer la viabilité du jeune projet *Ethereum*. Les *Anti-Forks*\* considéraient que la réalisation d'un tel *Hard Fork*\* pour une faille d'application en ferait un précédent dangereux, entachant irrémédiablement la confiance dans *Ethereum*. Pourtant, et malgré les nombreux hacks et failles qui continueront de toucher à la couche applicative d'*Ethereum*, aucune autre intervention de ce type n'a été depuis réalisée : la communauté désapprouvera en effet par la suite ce type d'intervention [par exemple, dans le cas de bogues affectant l'implémentation multi-signature Parity et ses utilisateurs, J. de Tychet ; Entretien n° 4]. Finalement, Buterin (2017) et la communauté

Ethereum finiront par contester et nuancer ces *a priori* existants sur les *Forks\** hérités des *bitcoiners\** et feront du *Hard Fork\** le sentier d'évolution privilégié d'Ethereum. Tout *Fork\** qu'il soit, *Soft* ou *Hard*, il est coercitif à divers degrés. Mais quand on souhaite « *apporter un changement controversé* », les *Hard Forks*<sup>480</sup> relèvent d'une coercion moindre, car ils offrent, comparativement aux *Soft Forks\**, un plus grand éventail de choix, ce qui permet de « *mieux préserver la liberté des utilisateurs* ». Les *Hard Forks\**, contrairement aux *Soft Forks\**, sont « *opt in* ». En effet, l'ensemble des participants doit prendre part au processus de décision suivant qu'ils imposent une gouvernance publique et hybride : tout « *opérateur de nœuds\** doit décider consciemment s'il doit installer un *hard Fork\** pour que son *nœud\** soit compatible avec les *nœuds\** des opérateurs qui ont également décidé d'installer ce *hard Fork\** » (Zamfir 2017). Les *Hard Forks\** fournissent enfin un mécanisme de sécession sans lequel impossible de clamer son indépendance, comme le fait « *Ethereum Classic* » (The Ethereum Classic Community 2016), car l'ancienne chaîne peut continuer à exister, là où les *Soft Forks\** « *favorisent institutionnellement la coercion par rapport à la sécession* », forçant les utilisateurs à accepter les nouvelles règles du protocole puisque la chaîne originale cesse d'exister. Ce cas a souligné à nouveau l'importance d'une diversité d'acteurs. Dans la réussite ou l'échec de cette sécession, si les mineurs et développeurs\* Core sont nécessaires, d'autres acteurs tout aussi importants de la gouvernance *sur l'infrastructure* sont apparus, comme les bourses, qui jouissent de pouvoirs structurels importants (leur décision de listing donne vie aux incitations économiques de la chaîne sécessionniste). L'expérience *Ethereum Classic* apparaît sur une plus longue période comme un échec, la CM restant peu utilisée et n'ayant jamais vraiment concurrencé *Ethereum*. En fin de compte, la résolution de la crise de « *The DAO* » démontre que « *la partie importante de tout Fork\*, Soft ou Hard Fork\*, est que la grande majorité des nœuds\* se mettent à jour* » [Corallo, Entretien n° 15] et que cette majorité d'acteurs non humains soit soutenue par l'ensemble des parties prenantes humaines qui en constitue la communauté d'usage.

Si cette crise a ouvert des précédents, c'est justement au niveau de sa gouvernance. À travers elle, la communauté Ethereum précise les voies permettant d'établir quelles modifications/corrections du protocole étaient pour elle désirables et légitimes. De bonnes pratiques et des procédures d'expression des désaccords et d'élaboration de consensus *ad hoc* ont été institutionnalisées : la procédure des EIP, inspirée des BIP Bitcoin, allait être complétée de différents mécanismes permettant de coordonner une diversité d'équipes d'implémentation client différentes, inclure des arènes de discussion vidéo avec transcription accessible à la communauté (les *All Core Dev Meeting*, J. de Tychet, Entretien n° 4 ; B. Summerwill, Entretien n° 26]. Les problématiques posées par la mesure du soutien communautaire aux *Forks\** ont montré que : « *la gouvernance sur Ethereum, elle fonctionne vraiment avec des signaux. C'est vraiment [...] ce qui s'est passé autour de la DAO, ça a été un bon, un bon stress test, on va dire et en fait, tout ce qui s'est passé après, ça a été tiré des leçons de ce qui s'est passé au moment de la DAO pour essayer de clarifier les signaux et d'être moins dans... des signaux qui sont moins facilement manipulables* ». » [S.Polrot, Entretien n°16]

---

<sup>480</sup> Au sein des *Hard Forks*, Buterin (2017) distingue : les « *Stricky expending Hard Forks* » qu'il préfère en ce qu'ils correspondent à une extension stricte de l'ensemble des transactions valides au sein des anciennes règles canoniques offrant une rétrocompatibilité et les « *Bilateral Hard Forks* », qui induisent, eux, que les deux ensembles de règles protocolaires sont mutuellement incompatibles.

### III.4 CONCLUSION DU CHAPITRE III

Ce troisième chapitre portait sur la gouvernance – *par et sur* l’infrastructure – des CM à l’aune d’une enquête sur la fabrique et la gouvernance de leurs crises. Le caractère polycentrique de leur gouvernance identifié comme singularité monétaire (cf. hypothèse conclusive du chap. II) y a été étudié au travers de la documentation et de l’analyse de deux cas de crises situées : la crise Bitcoin CVE 2018 et la crise du *Hard Fork*\* d’Ethereum consécutive à l’attaque de « The DAO ». Cette focale des crises de CM nous a permis de réfuter très directement l’ensemble des prétentions libérales-technicistes véhiculées qui font des CM des monnaies acéphales et décentralisées, autonomes et parfaitement apolitiques du fait qu’elles seraient régulées uniquement par le code et non par des entités gouvernantes. Cette même focale a permis de montrer que la confiance qu’accordent les *coiners*\* à leur CM, loin d’apparaître fondée exclusivement sur leur autorité algorithmique, repose bien plus sur des autorités communautaires et l’institutionnalisation de capacités communes d’intervention permettant de remédier à une situation au cas où le code et ses régulations déraillent. Ce travail nous a aussi offert un point de vue privilégié sur l’hétérogénéité des représentations traversant les communautés de *coiners*\*, sur ce qui fait des CM de « bonnes » ou « mauvaises » monnaies. En effet, à travers la normalité qu’ont dessiné nos états de crise, ce sont les propriétés désirées des CM qui étaient éprouvées et renégociées. Finalement, ce chapitre a permis de préciser dans quelle mesure cette gouvernance polycentrique pouvait soutenir effectivement la « *formation de consensus entre des individus mis par des intérêts politiques et commerciaux* » différents (De Filippi et Loveluck 2016, p. 15) en offrant à l’ensemble des *coiners*\* la capacité de participer à l’érection des décisions les concernant. La résolution de la crise d’Ethereum, qui a conduit à la sécession d’Ethereum Classic, a permis notamment de mettre en perspective l’idée que la gouvernance des CM, par la pratique toujours possible du *Fork*\*, garantit qu’aucun groupe ou entité issu(e) d’une des composantes communautaires n’apporte discrétionnairement « *au code une modification que la communauté désapprouve [car] celle-ci pourrait tout simplement refuser d’exécuter le nouveau code* [à la manière d’un] “*pouvoir de veto*” [assurant] que la légitimité du code repose en fin de compte sur les utilisateurs » (*Ibid.* p. 14).

Le premier temps de la démonstration a été consacré à la présentation périodisée de la crise Bitcoin CVE 2018, ouverte suite à la réception par des membres de l’équipe Bitcoin Core d’un rapport de divulgation responsable les informant de l’identification d’un bogue dans les codes logiciels permettant de contourner les régulations contre la double dépense\*, donc de son monnayage. La restitution des évènements, de la mise en crise à la remise en ordre, a permis de retracer les modifications du protocole Bitcoin, en explicitant leurs contextes, les acteurs à l’œuvre et les justifications qui président à leur développement, les procédures collectives de contrôle des modifications et les canaux de communication spécifiques mobilisés. Nous avons encore explicité les acteurs et les dispositifs socio-techniques clefs de la maintenance des codes protocolaires d’une CM, et interrogé les conditions de la découverte du bogue, de son évaluation, de sa correction et de sa publicisation, sous la forme d’abord d’un correctif mis à disposition de la communauté sans que soit révélée l’étendue des changements qu’il contient. Les informations critiques ont finalement été rendues publiques tardivement, à la faveur d’un processus de publication graduel. Pour mieux saisir le cadre et les enjeux de cette crise, nous l’avons ensuite resituée dans une histoire plus large des crises traversées par Bitcoin et sa communauté (cf. Chronologie 4) : bogue d’inflation, de scission de chaîne, DOS, PR, BIP, merge, *Soft Fork*\* ou *Hard Fork*\*, etc.

Le second temps du chapitre a été consacré à l’analyse de la politique de la crise et à l’identification d’une structure générale de gouvernance de Bitcoin, avec un code largement dominé par l’implémentation et les versions Bitcoin Core, une situation qui conduit à donner un poids important à son équipe de développement – les Core Devs – et au répertoire d’administration de ses

codes – le repo Bitcoin Core Github. Si l’analyse de l’administration des codes Bitcoin Core a démontré l’existence d’une hiérarchie formelle entre les « Core Devs », dotant certains acteurs de priviléges étendus, voire léonins (pour le mainteneur principal), il est apparu que la communauté Bitcoin s’était dotée de garde-fous permettant d’encadrer strictement l’ensemble des activités de développement. Des dispositifs et procédures variés sont mis en œuvre afin d’assurer la traçabilité des modifications proposées et implémentées (le *système d’intégration continu basé sur des vérifications de clefs PGP de confiance*), comme l’intégrité des nouveaux codes sources Bitcoin Core publiés (*Gitian Building*) . Ces dispositifs visent à préserver la possibilité pour les participants d’accepter ou de refuser librement, et de manière éclairée, toute nouvelle version publiée (existence de dispositifs de mesure du consentement et de fixation de la majorité *via* des dispositifs de vote, de signalement et d’activation). La crise Bitcoin CVE 2018 et la gouvernance qu’elle nous a permis d’analyser, bien que d’apparence hautement centralisée et technocratique et à l’opposé de l’idée de gouvernance polycentrique où « *tout le monde [est] d’accord avec la direction que prennent les choses* » [M. Corallo, Entretien n°15], ne représentait en fait que l’une des deux faces de la gouvernance de crise des CM : sa face routinière, que nous qualifions de *huis clos*. Sa caractéristique est justement d’être réservée à des crises dont la remise en ordre induit *a priori* un consensus fait d’absence de dissensus. Dans le cadre de cette gouvernance de *huis clos*, les « Core Devs » bénéficient de discrétion dans la production d’un consensus d’abord local au sein d’un groupe de quelques techniciens amis. Ce cas présente un type particulier et renvoie à une crise que nous qualifions de *crise de vulnérabilité*, car relevant d’une situation où les résultats des codes sont en contradiction flagrante avec les attendus communautaires. Ce type de crise s’oppose aux *crises d’évolution*, qui concernent des situations où le code, bien qu’il fasse jusque-là ce que l’on attend de lui, est mis en crise par l’expression d’une volonté communautaire de le faire évoluer. La remédiation de la crise de vulnérabilité était simple et consensuelle, ce qui explique l’absence de dissensus observé localement d’abord, puis globalement après la divulgation complète de l’équipe Core. Cette gouvernance de *huis clos* met au jour une reconnaissance routinière, tacite et sans ambages de l’autorité des « Core Devs ». Mais celle-ci reste néanmoins suspendue au maintien du consensus autour des codes ainsi publiés. Qu’un acteur en conteste le bien-fondé et arrive à faire apparaître un dissensus les concernant dans la communauté, et la crise verra sa gouvernance se transformer en sa face opposée : la gouvernance « *publique* », spécifiquement taillée pour produire un consensus large concernant des modifications de codes *a priori* controversées.

Le **troisième temps** du chapitre fut dédié au cas de la crise du *Hard Fork*\* consécutif à l’attaque de « The DAO ». Ce cas illustre une crise *d’évolution* à gouvernance *publique* conflictuelle. Le protocole Ethereum fonctionnait comme attendu, mais il a été mis en crise par la proposition de l’utiliser comme moyen de remédiation afin d’annuler l’attaque et de restituer les fonds aux investisseurs. Ce type de crise, exceptionnel, conduit inéluctablement à des controverses, dont il est attendu qu’elles soient résolues en public et à grand bruit. Dans de tels cas, les stratégies de remédiation sont multiples - sont possibles : *Soft Fork*\*, *Hard Fork*\*, contre-attaque, ne rien faire - selon l’évaluation et les cadrages retenus des enjeux de la crise. Au centre de ces choix réside la question de leur légitimité reflétant l’hétérogénéité des vues communautaires sur les propriétés désirées de leur CM (immutabilité *versus* sauvegarde de la communauté) et de la « bonne » gouvernance qui y est associée (non-intervention par principe *versus* adaptation à une situation donnée). Finalement, dans une situation complexe et contrainte par l’urgence, la gouvernance de cette crise *publique* d’Ethereum lui aura permis de produire un consensus majoritaire relativement massif, incluant ses parties prenantes non humaines (nœuds\* mineurs et complets), mais aussi humaines (utilisateurs finaux, services marchands et passerelles\*, mineurs, etc.) *via* l’élaboration distribuée de mécanismes d’expression d’accords ou de désaccords variés et adressés aux différentes composantes communautaires. Ainsi, la minorité d’*etheristes* qui refusait cette solution du haut de leur interprétation rigoriste du slogan « *Code is Law* » ne se l’est pas vu imposée de manière

coercitive. Là où une modification de type *Soft Fork*\*, traditionnellement privilégiée sur Bitcoin, n'aurait pas permis à une nouvelle chaîne d'émerger, celle de type *Hard Fork*\* a bien permis de faire souverainement sécession et ce, hors coercition.

Ce chapitre a démontré que les CM ne pouvaient se prévaloir de s'être détachées de toute gouvernance humaine, comme l'affirment certains de leurs promoteurs. Ce n'est pas une mauvaise nouvelle car, en leur absence, Bitcoin, Ethereum ou toute autre CM n'aurait pas dépassé le stade de la preuve de concept et aurait été incapable de traverser leurs premières crises *de vulnérabilité* et d'arriver à s'optimiser, ou à évoluer radicalement pour s'adapter à un environnement changeant – *via des crises d'évolution*. N'en déplaise aux *coiners*\* du camp de la *règle radicalisée*, quand la lettre du code n'en respecte pas l'esprit, il reste - en dernier ressort – la primauté du consensus social sur les règles protocolaires. Une primauté dont toutes les crises, qu'elles soient *de vulnérabilité* ou *d'évolution* attestent, indépendamment de la forme prise de la gouvernance (de *huis clos* ou *publique*).

Ce chapitre a aussi permis d'ordonner et d'analyser en partie la complexité et la diversité des mécanismes de gouvernance des CM, Bitcoin et Ethereum. Néanmoins, les éclairages apportés par ce travail découvrent des zones d'ombres et des angles morts. Notre focalisation sur les crises protocolaires a conduit à s'intéresser principalement à la gouvernance *sur* l'infrastructure de Bitcoin et Ethereum, leur protocole, alors que des crises infrastructurelles, comme dans les cas de Mt Gox et Silk Road (Musiani, Mallard et Méadel 2018; cf. chap. I), peuvent impacter leur communauté et questionner leur monétisation. De par les choix de crise que nous avons faits, notre analyse octroie une place centrale à l'étude de l'administration du répertoire Github des implémentations protocolaires par le groupe des « Core Devs ». Cette place donnée à l'un des systèmes de ressources (essentiel il est vrai) participant du système de ressources plus large que représente l'infrastructure d'une CM laisse aux marges les autres composantes (et les systèmes de ressources qu'elles constituent) de ces communautés, ce qui mériterait d'être interrogé et réarticulé par des recherches spécifiques (sur les mineurs, les services marchands et les passerelles\* en particulier, plus difficiles d'accès). Des questions importantes ont donc été soulevées sans toutes trouver de réponses suffisamment étayées, comme la question du financement des développeurs\*, donc à la fois du renouvellement des compétences communautaires nécessaire à la gouvernance des CM . Ou encore, la question de la dépendance économique induite par les voies de financement actuelles qui posent des questions de conflit d'intérêts. Le poids relatifs de certains acteurs clefs, comme les bourses d'échange dont le rôle dans l'apparition d'Ethereum Classic a été souligné, mériteraient aussi d'être mieux compris. Toutes ces questions sont donc renvoyées à des recherches ultérieures.

## CONCLUSION GÉNÉRALE

« La méconnaissance des mécanismes de croissance des coquilles Saint-Jacques est totale. La communauté scientifique ne s'y est jamais vraiment intéressée ; les marins-pêcheurs n'étant héritiers d'aucune tradition puisque l'exploitation intensive est récente, ne savent rien des premiers instants des coquilles Saint-Jacques qu'ils ne connaissent qu'à l'état adulte lorsqu'ils les remontent dans leurs dragues. Au début [, ] il n'existe donc aucune relation directe entre les larves de coquilles et les marins-pêcheurs [et] c'est par l'entremise des chercheurs que ce lien sera progressivement construit. »

“ÉLÉMENTS POUR UNE SOCIOLOGIE DE LA TRADUCTION: La domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc”,  
Michel Callon, 1986, p. 179

Cette thèse aborde divers enjeux liés à notre intérêt pour la monnaie et à l'étonnement suscité par les ambitions monétaires des promoteurs les plus en vue des crypto-monnaies. En réactivant de manière unique le débat entre règle et discréction, ces ambitions, qualifiées de libérales-technicistes, se présentent sous la forme d'un syllogisme dont la validation\* ou la réfutation des prémisses et de leurs connexions constitue le fil conducteur de nos chapitres. Ce syllogisme postule que, puisque (i) la technique est autonome et neutre vis-à-vis du monde social et que (ii) les CM sont des monnaies purement techniques ; alors (iii) elles sont immunisées de la gouvernance humaine et de ses intérêts socio-politiques, ce qui en fait (iv) de « meilleures » monnaies que les monnaies nationales. L'objectif premier de cette thèse était d'étudier les CM Bitcoin et Ethereum pour contribuer à enrichir un champ de recherche émergent sur les CM encore peu exploré, notamment en sciences humaines. Nous nous proposons de dépasser deux écueils. Le premier est le « technologisme » majoritairement présent dans les analyses – indigènes, grises ou académiques - présentant les CM comme des entités purement techniques, neutres, autonomes et stabilisées, en se concentrant uniquement sur leurs caractéristiques techniques et protocolaires. Le second est le « sociologisme », qui, à l'inverse, réduit les CM à leur origine libertarienne. Pour ce faire, nous avons appréhendé les CM comme des objets, des infrastructures socio-techniques même, en perpétuelle recomposition, nécessitant d'en restituer le contexte relationnel et socio-historique.

## RÉSUMÉ DE LA THÈSE

**Le premier chapitre** a proposé une présentation circonstanciée de nos deux objets d'étude permettant d'expliciter : le contexte et les caractéristiques de leur conception, les composants et processus clefs de leurs fonctionnements, leur développement par étape, les acteurs (humains ou non) et les domaines de développement participant de leur infrastructure, comme les ressources et contraintes de ce développement. C'est au travers de la restitution de l'épaisseur socio-historique de l'émergence du pionnier Bitcoin d'abord, de certains Altcoins\* ensuite et d'Ethereum enfin, qu'il nous a été permis de questionner l'apolitisme, la neutralité et l'autonomie prétendument « techniques » des CM.

Nous avons mis en évidence que les agencements sociotechniques clefs de Bitcoin et le scénario type de son fonctionnement renvoient aux inspirations et pratiques singulières de Nakamoto, couplées aux contraintes théoriques qu'il rencontrait, et souligné que les choix architecturaux effectués - en particulier son consensus fondé en PoW\* associé à l'émission monétaire des UCN\* - étaient hybrides, négociés et donc politiques. Cet entrelacs politico-technique originel du protocole s'est compliqué avec le développement infrastructurel, car un simple protocole

ne fait pas CM sans *confrontation* à des utilisateurs. Nous avons montré que Bitcoin, en tant qu'infrastructure « sans couture », n'est réductible ni aux desseins et mises en scène de son concepteur, ni à ses frontières protocolaires, puisqu'il est sans cesse renégocié par les improvisations d'acteurs. C'est ainsi que nous avons identifié trois phases – *phase de preuve de concept, phase de péché, phase de maturation* – dans son développement *carnavalesque* qui a donné lieu à une variété d'arrangements et de travaux d'acteurs, au fur et à mesure plus nombreux, différenciés et intégrés au système monétaire et financier. La présentation d'Ethereum a permis de conclure le chapitre et sa démonstration : l'explicitation des points saillants de la normativité de ses agencements et de son développement infrastructurel propre a également mis en lumière, par contraste, la normativité de Bitcoin. Car la conception d'Ethereum ajoutait, aux critiques de Nakamoto envers le système monétaire traditionnel, des critiques sur les rigidités protocolaires et infrastructurelles de Bitcoin et des expériences d'Altcoins\* qui l'ont suivi.

**Le deuxième chapitre** apporte une contribution critique à la controverse sur le statut monétaire des CM. Depuis une position ancrée dans un institutionnalisme monétaire intéressé par les usages, nous y affirmons qu'elles sont bien des monnaies, tout en rejetant les perspectives monétaires orthodoxes – d'homogénéité, d'unicité et d'exclusivité – partagées tant par les *coiners*\* que par leurs critiques académiques et praticiens. De ce point de vue, les CM s'intègrent au champ monétaire en tant que forme inédite, non pas en raison de l'absence (présupposée par les uns et les autres), mais *a contrario* du fait de la présence d'une gouvernance singulière d'apparence polycentrique.

Notre revue de la littérature a mis en évidence que deux familles d'approches distinctes – instrumentale et nominaliste/chartaliste –, mais partageant une définition réifiée de la monnaie réduite à ses formes modernes. Ces deux approches relèguent les CM au statut d'actifs financiers sans valeur : la monnaie, selon ces approches, doit porter parfaitement les fonctions monétaires canoniques, et ce, au sein d'un espace économique unitaire et exclusif administré par un centre souverain. En revanche, pour les approches nominalistes *non étatistes* partant des usages dans lesquelles nous nous inscrivons, l'argent d'hier et d'aujourd'hui n'est pas universel et exclusif, il connaît marquages et circulation de monnaies parallèles, et le seul critère discriminant donnant la qualité monétaire est la présence d'usages en compte et en paiement. Nous faisons valoir ces usages par l'étude des pratiques, soulignant notamment que les UCN\* servent un type d'usage primordial qui leur est exclusif et souverain au sein de leur protocole : elles seules permettent l'expression nominale et le paiement réel de la dette ouverte par la demande transactionnelle que les frais de transaction\* permettent de régler. Ainsi, les CM, en tant que créances au porteur sur le protocole d'émission qui les acceptent en paiement des services qu'il offre, sont des monnaies parallèles de type communautaire : leur monétisation au sein de leur communauté de paiement relève d'une fiduciarité similaire aux monnaies fiat nationales, dont la valeur et le pouvoir d'achat sont garantis par des institutions et des acteurs sociaux. L'examen de l'absence présumée de gouvernance des CM, centrale dans la controverse sur leur qualité, supposée meilleure comparativement aux monnaies fiat, a révélé que les CM réactivent un débat ancien sur la « bonne » gouvernance monétaire, impliquant des enjeux idéels (rôle de l'État et des banques centrales) et matériels (risque d'érosion des capacités de régulation). Nous opposons une vision positive à la normativité de ces approches, décalant les enjeux et formulant l'hypothèse que la singularité monétaire des CM réside dans une gouvernance polycentrique révélée par les crises et conflits agitant leur communauté concernant les qualités monétaires désirées. Les CM constituent une catégorie monétaire inédite, distincte des monnaies nationales et privées, fondée non sur une logique fiduciaire de sceau ou contractuelle de signature, mais sur une logique de consensus distribué, qui s'établit comme critère de clarification catégoriel dans le champ monétaire.

**Le troisième chapitre** examine deux cas de crises - la crise Bitcoin CVE 2018 et la crise du *Hard Fork*\* d’Ethereum après l’attaque de « The DAO » - pour étudier la gouvernance polycentrique des CM et la formation du consensus au sein de leur communauté. Nous avons identifié que les crises de CM recouvrivent deux types : *les crises de vulnérabilité*, où le code contredit les attentes communautaires, et *les crises d’évolution*, où le code fonctionne mais la communauté désire le modifier. Nous avons également mis au jour une gouvernance de crise à deux volets, aux procédures et attendus différents : la *gouvernance de huis clos, routinière et à consensus local* et la *gouvernance publique, conflictuelle et à consensus global*. Cette analyse réfute les prétentions libérales-technicistes selon lesquelles les CM sont régulées uniquement par le code, donc apolitiques : quand la lettre du code n’en respecte pas l’esprit, le consensus social prime.

L’analyse de la crise Bitcoin CVE 2018, de la mise en crise à la remise en ordre, a permis de retracer les modifications du protocole Bitcoin, en explicitant les contextes, les dispositifs et les acteurs impliqués dans la découverte, l’évaluation, la correction, la publicisation des correctifs et des bogues, ainsi que de la mise à jour du réseau\*. Replacé dans l’histoire des crises de Bitcoin, ce cas fut aussi l’occasion de dresser un panorama exhaustif des crises déjà traversées par la CM. Les nomenclatures et catégories découvertes à cette occasion mettent au jour l’existence d’une politique de crise, dont l’examen permet de décrire une structure de gouvernance. Bitcoin étant dominé par l’implémentation et les versions Bitcoin Core, le répertoire d’administration des codes et les membres de l’équipe de développement, qui jouissent de priviléges d’administration, notamment le mainteneur principal, prennent *de facto* dans la gouvernance une place centrale. Mais ces priviléges sont encadrés afin de garantir la traçabilité des modifications, l’intégrité des codes sources publiés, et la formation d’un consensus entre participants sur le fait d’accepter ou non la nouvelle version, *via* des dispositifs d’expression des accords ou désaccords. L’examen de la remise en ordre révèle que la production du correctif, la publication et à la mise à jour rapide du réseau\* ont reposé sur une information partielle et la formation d’un consensus local entre une poignée d’acteurs. Ce cas nous a permis de décrire une gouvernance de crise de *huis clos, routinière et consensuelle locale*.

Le cas de la crise du *Hard Fork*\* d’Ethereum après l’attaque de « The DAO » met en lumière le passage de la gouvernance *de huis clos* à une gouvernance *publique*, plus exceptionnelle, conditionnée à l’apparition de dissensus. Le récit que nous en faisons explicite comment l’exploitation d’une faille dans un fonds décentralisé a ouvert une dispute sur les stratégies d’intervention désirables, reflétant l’hétérogénéité des vues communautaires en termes de gouvernance : agir *au sein* de la lettre du code (ne rien faire ou contre-attaquer) ou *sur* la lettre du code (*Soft* ou *Hard Fork*\*). La gouvernance publique a produit un consensus majoritaire et sans coercition entre l’ensemble des composantes communautaires *via* l’élaboration distribuée de mécanismes d’expression d’accords ou de désaccords variés : la minorité d’*etheristes* refusant la mise à jour au nom du « *Code is Law* » a souverainement fait sécession.

À la suite de ce résumé, nous proposons de mettre en avant ce qui nous apparaît être les principales contributions de cette thèse en cinq points.

## DÉCRYPTER LA CRYPTO PAR L’APPROCHE INFRASTRUCTURELLE

L’inscription de notre recherche dans le champ des *études infrastructurelles* initié par Leigh Star et Ruhleder (2010 ; Star 1999) est la source selon nous de plusieurs contributions. La transposition de ce cadre d’analyse aux CM a permis de mettre en lumière les aspects invisibles et négligés soutenant leurs usages et leur monétisation.

Le principal défi des études infrastructurelles réside dans la nature composite des objets étudiés (matérielle, immatérielle et relationnelle) et leur échelle, ce qui les rend difficilement visibles (sauf *en cas de panne* ! L'une des neuf propriétés infrastructurelles, Star 1999, p. 380-382, que notre chap. III permet d'interroger). Cette caractéristique soulève une question fondamentale relative à la visibilisation (Edwards et al. 2009). Les CM illustrent cette faible visibilité, encore exacerbée par le technologisme (vecteur d'invisibilisation) qui les entourent. Notre démarche révèle la nature sociotechnique composite des CM : elles ne sont pas de purs protocoles techniques (neutres et autonomes), mais *a contrario* des infrastructures socio-techniques complexes façonnées de tous côtés par des enjeux sociaux, politiques et économiques. Le chapitre I éclaire l'émergence de Bitcoin et d'Ethereum comme CM, en les replaçant dans leur contexte socio-historique. Il révèle les arbitrages, problématiques et compromis hybrides qui ont marqué chaque étape de leur développement, depuis leurs conceptions initiales jusqu'à leurs phases de développement infrastructurel. Les CM sont intégrées dans des pratiques organisées, se composent d'entités matérielles (briques, machines, câbles, serveurs, centrales électriques) et abstraites (protocoles, standards, conventions de pratique, représentations de la « bonne » monnaie et gouvernance) soulignant l'importance cruciale de la dimension relationnelle dans leur analyse (Star et Ruhleder, 2010). Bitcoin et Ethereum deviennent des monnaies grâce au travail continu de divers acteurs (Bowker 1996, p. 50 ; Star 1999 ; Edwards et al. 2009), tels que des pirates, ingénieurs, gamers, traders et investisseurs en capital-risque. Ce travail met en lumière des problématiques clés, telles que les tensions entre besoins locaux et globaux, et les défis d'intégration au système monétaire et financier existant. Ces tensions influencent les pratiques et les structures organisationnelles, agissant à la fois comme moteurs et obstacles au changement. Ces tensions sont particulièrement illustrées par les paradoxes de réintermédiation observés lors de leur développement. Alors que d'autres travaux ont étudié les CM et leur gouvernance (Kavanagh et Miscione 2017 ; rejoint par Musiani 2018 ; Musiani, Mallard et Méadel 2018) au travers de cas isolés, notre contribution est d'avoir visibilisé le développement infrastructurel de Bitcoin, en tissant ensemble ces cas pour créer une trame plus large et révéler un *tissu sans couture* au motif *arlequin* (cf. Chronologie 2, Chap. I section I.1.2). Par-delà la transposition du modèle de développement infrastructurel en trois étapes successives (*construction / lancement, développement / succès, sédimentation / stabilisation*), nous avons éclairé les problématiques d'intégration à un existant constitué d'artefacts, d'habitudes, de normes et de rôles humains (Edwards et al. 2009, p. 366-367). Révélant la dynamique carnavalesque du développement infrastructurel des CM, cette méthode a permis d'éclairer les propriétés infrastructurelles d'encastrement, de transparence, d'apprentissage lié à l'appartenance, de liaison à des conventions de pratiques, d'incorporation de standards et de normes, de construction sur une base installée, de visibilité lors de panne et de modification par incrément modulaire (Star, 1999, p. 380-382). Elle offre aussi une mise en lumière de la propriété *de portée*, spatiale et temporelle, soulignée par Star (1999), qui pointe l'étendue des infrastructures excédant l'événement et la pratique isolée. Les autres travaux sur les CM n'avaient pas, selon nous, pleinement révélé cette dimension.

Enfin, notre travail contribue directement à la partie de ce corpus des *infrastructure studies* consacrée « à explorer les dynamiques de pouvoir, les conflits et contestations, les significations et rapport sociaux incarnés » dans les infrastructures (Musiani 2018, p. 1), ce que nous proposons de faire au travers de l'étude de la gouvernance de crises. Notre approche montre que, au-delà d'une gouvernance *par* l'infrastructure, la gouvernance *sur* l'infrastructure des CM est conflictuelle et polycentrique, révélant l'hétérogénéité des représentations au sein des communautés de *coiners*\* et la manière dont les propriétés des CM sont renégociées. Les infrastructures de Bitcoin et d'Ethereum apparaissent comme des lieux de pouvoir où se jouent en permanence des enjeux politiques, économiques et idéologiques. Les crises de *vulnérabilité* et *d'évolution* analysées ont démontré que la gouvernance polycentrique repose sur des autorités communautaires variées et des capacités

d'intervention institutionnalisées, soutenant (pour l'heure) la formation de consensus entre des individus aux intérêts divergents. Ces crises révèlent une gouvernance polycentrique combinant des formes de gouvernance locales et publiques, qui prime sur la régulation du code.

Ces éléments rendent les CM particulièrement intéressantes, car loin d'un énième cas de *e-infrastructure*, elles intègrent une perspective monétaire peu étudiée, offrant des enseignements sur les questions de signification et de valeurs partagées.

## DE L'ACÉPHALISME APOLITIQUE DES CM À L'ÉPREUVE D'UNE SOCIOLOGIE DES CRISES

Ce travail contribue aussi à la sociologie des crises à partir des cas de Bitcoin et d'Ethereum. Nous ajoutons tout d'abord l'objet CM à la richesse des études de cas qui constituent ce corpus. La volonté de dévoiler la gouvernance socio-politique des CM, à partir de l'étude des crises traversées par Bitcoin, Ethereum et leurs communautés, a permis de valider à nouveau (en les épousant) les enjeux théoriques et méthodologiques, ainsi que les outils développés par ce corpus. Le chapitre III démontre l'intérêt heuristique d'analyser « la politique de la crise » et « son gouvernement » de *la mise en crise à la remise en ordre* (Aquiton, Cabane et Cornilleau 2019, p. 4) : cette approche nous permet de réfuter les prétentions libérales-technicistes présentant les CM comme des monnaies acéphales et apolitiques, régulées uniquement par le code, en visibilisant la complexité et la diversité des mécanismes de gouvernance de Bitcoin et d'Ethereum.

Partant du hiatus entre l'état routinier et le phénomène critique que dessinent les crises et leurs nomenclatures produites par les *coiners*\* eux-mêmes, nous avons mis en lumière deux types de crises – les crises de *vulnérabilité* et les crises *d'évolution* -, ainsi que les processus complexes qui permettent aux *coiners*\* de qualifier certaines situations de crise et de les gérer comme telles. Comme l'illustre chacun de nos cas, l'établissement d'un diagnostic de crise est un acte politique essentiel au travers duquel il s'agit de désigner, outre la « nature » de la pathologie (et sa gravité), le prescripteur, le malade, les traitements et le parcours de soin. Tout diagnostic de crise renvoie à un cadrage qui peut être controversé, comme le prouve le schisme d'Ethereum Classic.

Ce travail a offert un point de vue privilégié sur l'hétérogénéité des représentations des CM et de leurs propriétés désirées, éprouvées et renégociées en temps de crise. Nous avons étudié comment ces communautés s'organisent pour remédier à ces crises et réguler les activités critiques que cela implique. De ce fait, nous avons identifié les acteurs, institutions, arènes de débats et dispositifs participant à la fabrique et à la gouvernance des crises. Ainsi, nous avons mis au jour une gouvernance de crise à deux volets - de *huis clos* et *publique* – reflétant des relations d'autorité, de pouvoir et de contre-pouvoir différenciés et évolutifs. Nous avons montré comment la gouvernance polycentrique des CM relève de différents modes de gouvernement de crises, impliquant différents groupes de parties prenantes, arènes de débats, outils et dispositifs, renvoyant à des attendus communautaires variés et susceptibles de soutenir la formation de consensus entre des individus aux intérêts divers (De Filippi et Loveluck 2016, p. 15). Pris ensemble, ils permettent aux CM de s'adapter à un environnement changeant. La résolution de la crise d'Ethereum, qui a conduit à la sécession d'Ethereum Classic, illustre comment la pratique du *Fork*\* apparaît comme une garantie qu'aucun groupe ne peut imposer des modifications au code sans l'accord de la communauté. En fin de compte, cette démarche de sociologie des crises nous a permis de montrer que, en dernier ressort, dans le cas des CM, le consensus social prime sur les règles protocolaires, comme l'attestent toutes les crises, quel que soit leur type (de *vulnérabilité* ou *d'évolution*) et leur gouvernance (*de huis clos* ou *publique*).

## UNE INTÉGRATION COHÉRENTE DES CM DANS LE CHAMP DE LA THÉORIE MONÉTAIRE

Le chapitre II contribue à la théorie de la monnaie, en particulier à l'institutionnaliste monétaire, en intégrant en son sein les CM sans compromettre la cohérence de ce corpus. Nous y avons proposé une revue critique de la littérature sur les CM, présentant les principales critiques et les replaçant dans leur corpus théorique et épistémologique. Les CM, en tant qu'innovation monétaire, constituent pour la théorie monétaire une épreuve d'explicitation. Nous avons montré que ces objets monétaires s'intègrent plus facilement au sein d'une approche institutionnaliste monétaire intéressée par les usages. Cet appareillage nominaliste non étatiste nous a permis de souligner les incohérences et les angles morts des analyses dominantes des CM : ni les fonctions canoniques de la monnaie, ni l'exclusivité étatique ne peuvent reléguer les CM hors du champ de la monnaie. Les pratiques des communautés Bitcoin et Ethereum montrent que les CM présentent les caractéristiques minimales de la monnaie : elles sont usées en compte et en paiement.

Nos données empiriques constituent en soi une contribution puisque nous proposons une cartographie des acteurs et des parties prenantes constitutives de leur communauté de paiement, et mettons en exergue des représentations monétaires disparates (et potentiellement en conflit). On retrouve au cœur de nos analyses les invariants monétaires reconnus de l'institutionnalisme. Nous avons mis en lumière la souveraineté communautaire qui fait des UCN\* de CM des créances aux porteurs sur le protocole et la confiance que ces relations de dettes supposent. La confiance méthodique, hiérarchique et éthique, loin d'être uniquement dans l'autorité algorithmique, est distribuée entre les codes protocolaires, le repo Github, les bourses, les portefeuilles\*, les acteurs, les médias, etc. Cette distribution de la confiance, ne relevant ni de la logique de sceaux des monnaies publiques, ni de la logique de signature des actifs et monnaies privées, permet d'affirmer la singularité conceptuelle des CM et de dresser une typologie des actifs numériques : leur monétisation procède d'une logique fiduciaire comme les monnaies publiques, mais nous parlons de *logique de consensus distribué* pour souligner une différence clé. Les institutions et acteurs garantissant ce pouvoir d'achat diffèrent des monnaies nationales, la confiance reposant ultimement sur un réseau\* d'acteurs volontaires et d'institutions formant une gouvernance duale et polycentrique.

Les CM, en tant que tentatives radicales d'instituer une monnaie protégée du politique et de la délibération citoyenne, apportent une contribution paradoxale : si elles réussissent en tant que monnaie, c'est « *en contradiction directe avec l'idéologie politique et la théorie de la monnaie qui les sous-tendent* » (Dodd 2017, p.1). Bien qu'elles visent à dépolitiser la monnaie, elles la repolitisent de manière singulière : même crypto, la monnaie est une institution co-produite par les membres de sa communauté de paiement. Les CM invitent à la négociation de leurs propriétés, ce que révèlent les *crises d'évolution à gouvernance publique*.

## UN EFFORT DE TRADUCTION ATTENTIF AUX ET À L'ATTENTION DES ACTEURS

Le positionnement de cette thèse dans le champ de la sociologie des sciences et techniques et de la sociologie des controverses technologiques a soulevé des questions formelles en termes de « traduction » pour nos « acteurs-réseaux\* ».

La société résulte d'actions en cours, où les objets socio-techniques et les interactions entre humains et non-humains forment des réseaux\* complexes influençant les actions et décisions. En tant que chercheur, nous sommes parti de ces réseaux\*, d'où un effort de réflexivité poussant à nous interroger sur les interactions et les traductions mutuelles entre les acteurs (humains et non humains)

que nous contribuions à former sur le monde des CM. Le chapitre II a montré qu'un certain mépris et une méconnaissance réciproque fondaient pour partie la controverse entre les *coiners*\* et les professionnels de l'argent (économistes, banquiers, banquiers centraux).

Notre travail, par le choix (évalué et discuté) d'une forme « encyclopédique », permet une contribution en termes de traduction entre différents espaces sociaux : nous avons souhaité qu'il puisse faciliter le dialogue entre le monde académique (surtout les sciences humaines) et celui des CM. La granularité fine de certains exposés, la présence de notes de bas de page foisonnantes, la place donnée aux paroles d'acteurs, sont conçues comme des ponts offrant des espaces de traduction (accéder à une discussion sur BitcoinTalk, découvrir un explorateur de block et l'activité *on chain*\* qu'il permet d'observer, etc.). Malgré sa lourdeur, ce dispositif formel a permis de faire une thèse généreuse en matériaux, offrant aux chercheurs des voies d'accès aux arcanes des réseaux\* sociotechniques des CM. Notre travail ne se conçoit pas comme une critique extérieure aux acteurs cibles, adressée au seul monde académique, mais adressée aussi aux *coiners*\*. La constitution d'un langage *etic* fondé sur le langage *emic* des *coiners*\* (traduit par la construction d'un glossaire et d'annexes riches) doit nous permettre non seulement de parler d'eux, mais aussi de dialoguer avec eux.

À l'instar des larves de coquilles Saint-Jacques et des marins-pêcheurs de la baie de Saint-Brieuc étudiés par Callon (en exergue de cette conclusion générale), nous avons voulu être de ces chercheurs permettant l'entremise entre les *coiners*\* et les professionnels de l'argent.

## LES CM : BOUCS ÉMISSAIRES COMMODES D'UN SYSTÈME MONÉTAIRE EN CRISE ?

Nous conclurons ce travail par une question ouverte, qui nous a accompagné depuis le début de nos réflexions sur les CM jusqu'à la fin de cette thèse. Cette question explique en partie pourquoi le lecteur ne trouvera pas ici de réponse définitive sur la qualité « bonne » ou « mauvaise » des CM par rapport aux monnaies nationales, ni de critiques sur leur dangerosité, soulignée par les professionnels de la finance.

Les CM sont accusées d'être un désastre écologique (Dupré, Ponsot et Servet 2015 ; Bank of International Settlements 2018 ; Servet et Dufrêne 2021, entre autres) en raison de leur fonctionnement basé sur la PoW\*. Elles sont également vues comme une menace pour la capacité des États à percevoir des impôts et à surveiller les transactions\* financières (Krugman 2013), et comme forces déstabilisatrices pour l'économie. À Davos, le président E. Macron rangeait le Bitcoin et les crypto-actifs\* aux côtés du *shadow banking*, les qualifiant de forces les plus dérégulées et dérégulatrices du système bancaire et financier mondial<sup>481</sup>. « *Mais n'en est-il pas de même de la monnaie traditionnelle, créée en continu par les banques centrales ? En braquant les projecteurs sur l'enfer des CM, ne révèle-t-on pas les faiblesses de la monnaie bancaire ?* » (Couppey-Soubeyran 2021).

De notre point de vue théorique et citoyen, ces problèmes sont importants, mais transversaux à nos objets d'études. Les CM ne sont pas la cause de nouveaux maux, mais le symptôme d'un monde financiarisé et des passe-droits qui s'y trouvent institués. Le président Macron devait savoir que le *shadow banking*, les paradis fiscaux et la fraude existaient bien avant les CM et sont intégrés

---

<sup>481</sup> « Le FMI ne regarde pas les acteurs les plus dérégulés et dérégulateurs du système : le bitcoin, les crypto-monnaies, le shadow banking... Nous devons lancer cette discussion et la lancer dans le cadre du G20. » Le président Macron au Forum économique mondial de Davos, 24 janvier 2018 [consultation au 25/03/2018].

au système bancaire et financier traditionnel, sur lesquels les régulateurs peuvent agir. Par ce procédé rhétorique, un secteur émergent dont la taille et les encours restent aujourd’hui relativement limités et contingentés, était singularisé alors que, à bien des égards, il est amalgamé à d’autres, dont la taille, les volumes et la dispersion sont incommensurablement plus importants et dangereux<sup>482</sup>. Il est paradoxal de vouloir encadrer fortement un secteur émergent - ce que les acteurs demandent face à l’incertitude juridique qu’ils rencontrent -, alors que la finance traditionnelle, responsable de la crise de 2008, bénéficie de toujours plus de marges de manœuvre et d’injection de liquidités ? En France, le débat public, mettant l’accent sur les risques au détriment des opportunités<sup>483</sup>, détonne en comparaison de ceux, plus nuancés, qui prennent place dans d’autres pays ou au sein de certaines institutions financières (BoE<sup>484</sup>, FMI<sup>485</sup>, BRI<sup>486</sup>).

Les CM sont un puissant agent de contraste visibilisant la finançarisation de nos sociétés et ses effets, comme la régulation marchande de l’énergie et l’évasion fiscale. Bien qu’elles participent à ces phénomènes, elles le font avec des propriétés singulières. Oui, elles permettent des évitements fiscaux, mais ces transactions\* sont consignées dans un registre\* public accessible à tous, contrairement aux bases de données fermées des institutions financières. Peut-être alors, en étant accessible à tous, que c’est l’échelle de la fraude qui devient intolérable, soulignant que, quand il s’agit d’une minorité, cela est toléré (raisonnement qu’un auditeur, travaillant sur des questions de défense, a fait en séminaire). Notre approche infrastructurelle montre que les CM sont intégrées au système monétaire et financier, et peuvent à ce titre être régulées au niveau des acteurs et services : les paiements *on chain\**, suivis d’échanges *off chain\**, notamment pour les gros montants, sont plus facilement traçables que ceux de la monnaie bancaire traditionnelle (E. Klein, gendarme spécialisé dans le cyber, Observation participante n°12). La consommation énergétique des CM est légitimement questionnée, mais il faut la comparer à celle du système financier traditionnel. Des études récentes montrent que « *dans ce face à face [...] la finance traditionnelle* » doit aussi rendre des comptes : une « *étude [de Valuechain] arrive à un total de 4981 TWh/an* » (Magali 2022) et une autre « *l'estime à 2 340 et 3 861 TWh par an, soit entre 23 et 38 fois plus que le bitcoin* » (Dumas 2023). La consommation d’énergie des systèmes en PoW\* dépend de la source d’énergie utilisée pour le minage, et il est de la responsabilité des États de réguler et promouvoir des énergies plus vertueuses. Les CM en PoW\* offrent de rentabiliser les surplus énergétiques potentiels des nouvelles unités de production créées, rendant profitable la revente directe de ces surplus, face à des incapacités de stockage et de transmission (A 2020, S. Gouspillou, Entretien n° 17).

Enfin, avec Couppey-Soubeyran (2021), on peut s’interroger légitimement : la monnaie nationale est-elle vraiment « *le bien public qu’elle prétend être ?* » En réalité, « *la dangereuse privatisation de la monnaie* » n’est pas due aux CM, mais « *à son accaparement par le secteur*

<sup>482</sup> Ce que rappelle Marc Carney du Conseil de stabilité financière (FSB), les crypto-actifs\* ne représentent pas pour l’heure un risque systémique, de par une capitalisation boursière n’excédant pas plus de 1% du PIB mondial, quand les CDS qui ont largement participé à la crise financière représentaient à eux seuls pas moins de 100% du PIB d’alors. Voir sa déclaration officielle faite en direction des membres du G20, <http://www.fsb.org/wp-content/uploads/P180318.pdf> [consultation au 25/03/2018].

<sup>483</sup> Voir par exemple le dernier Focus de la Banque de France de Mars 2018, voir [https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16\\_2018\\_03\\_05\\_fr.pdf](https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf) [consultation au 25/03/2018].

<sup>484</sup> La Banque d’Angleterre est pionnière dans les réflexions sur les monnaies digitales et les crypto-actifs\*, comme le rappelle à l’envi Broadbent (2016). En 2014, elle publiait des articles qui leur étaient consacrées, voir <https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/quarterly-bulletin-2014-q3.pdf?la=en&hash=874BAD99E54170C8DB5C082D6E8962D3F10997DF> [consultation au 25/03/2018].

<sup>485</sup> Voir les déclarations de C. Lagarde, <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world> [consultation au 25/03/2018].

<sup>486</sup> Voir le rapport du comité sur les paiements et les infrastructures de marché, de la BRI, <https://www.bis.org/cpmi/publ/d174.pdf> [consultation au 25/03/2018].

*bancaire et financier* » dont cherchent à s'émanciper les innovations « *comme les cryptomonnaies\* ou les monnaies complémentaires* » (*Ibid.*). Les Banques centrales ne sont-elles pas plus technocratiques que les CM, au travers d'une indépendance statutaire qui soustrait à la délibération démocratique la « discrétion contrainte » qu'elles suivent ? Les CM, en critiquant le système monétaire et financier traditionnel, reflètent une époque de défiance envers le politique, les administrations publiques et les gouvernements. Paradoxalement, si elles constituent des tentatives radicales d'instituer une monnaie protégée du politique, elles la re-politisent singulièrement. Non fondées sur la logique contractuelle de signature, les CM apparaissent moins comme des monnaies privées que publiques. Elles ne se soustraient pas à la délibération communautaire, l'étude de leur gouvernance de crise démontre qu'elles sont co-produites par les membres de leurs communautés, et leur gouvernance polycentrique invite chacune des composantes à la renégociation de leur propriété. Rien ne nous permet de dire que ces infrastructures et leurs communautés arriveront à traverser toutes les crises que l'avenir leur réserve, et si la gravité de l'une d'entre elles n'arrivera pas à saper définitivement la confiance qu'elles pouvaient susciter. Mais notre travail d'enquête contribue à montrer que ces infrastructures monétaires et financières nous ont permis d'en user et d'y enquêter sans qu'aucune autorisation ne nous soit nécessaire. Or, à bien des égards, une monnaie nationale a aussi besoin de tout ce ramassis de dispositifs socio-techniques, de logiciels, de procédures de validation\*, etc. Et forcément, il y a des bugs, des problèmes, des malversations, comme « *après avoir découvert qu'une cyberattaque avait détourné 81 M\$ de la Banque centrale du Bangladesh, le réseau\* interbancaire Swift a averti ses utilisateurs qu'il ne s'agissait pas d'un cas isolé et diffusé une mise à jour de sécurité pour son logiciel client, à installer impérativement* » (Gross 2016). Mais, dans ce cas, la base de données transactionnelle est privée, non publique, et il est possible de falsifier « *des accréditations valides pour créer et diffuser des messages sur le réseaux\** » (*Ibid.*), ce que les preuves cryptographiques régulent strictement : dans le cas de la banque centrale, les codes logiciels sont propriétaires et non libres, donc le patch est obligatoire, n'est pas auditable, ni « Fork\*able » par les clients qui sont déjà chanceux d'avoir été mis au courant... là où une telle crise aurait été visible de tous dans le cadre d'une CM. Toute monnaie est le produit d'une infrastructure, les monnaies nationales comme les CM, alors plutôt que de leur reprocher « *ce qui peut l'être tout autant à la monnaie légale, interrogeons-nous sur les raisons de leur développement* » et sur les propriétés infrastructurelles - comme l'ouverture, la transparence - dont le système traditionnel pourrait gagner à s'inspirer.

## BIBLIOGRAPHIE

ABDELATIF HAFID, 2022, « Probabilistic Models to Analyze the Security of Sharding-Based Blockchain Protocols », Unpublished, Montréal, 120 p.

ABRAHAM Michelle, 2020, « Les prestataires de services sur actifs numériques : cadre légal », *RFCComptable*, janvier 2020, vol. 20, n° 478, p. 3.

AFP, 2018, « Le marché du bitcoin fait fureur au Japon », *Le Point*, 5 janv. 2018.

AGLIETTA Michel, 1988, « L'ambivalence de l'argent », *Revue française d'économie*, 1988, vol. 3, n° 3, p. 87-133.

AGLIETTA Michel et CARTELIER Jean, 1998, « Ordre monétaire des économies de marché » dans *La monnaie souveraine*, s.l., p. 129-157.

AGLIETTA Michel et ORLÉAN André, 2002, *La monnaie entre violence et confiance*, Odile Jacob, Paris, 384 p.

AGLIETTA Michel et ORLÉAN André (dir), 1998, *La monnaie souveraine*, Odile Jacob, Paris, 398 p.

AGLIETTA Michel, PONSOT Jean-François et OULD-AHMED Pepita, 2014, « La monnaie, la valeur et la règle - Entretien avec Michel Aglietta », *Revue de la régulation*, 2014, vol. 16, p. 17.

AGLIETTA Michel et SCIALOM Laurence, 2002, « Les risques de la monnaie électronique », *L'Économie politique*, 2002, vol. 2, n° 14, p. 82-95.

AGUITON Sara Angeli, CABANE Lydie et CORNILLEAU Lise, 2019, « Politiques de la « mise en crise » », *Critique internationale*, 1 décembre 2019, vol. 85, n° 4, p. 9-21.

AILLEURS, 2015, « Dictateur bénévole », <https://bitcoin.fr/dictateur-benevole/>, 31 août 2015, consulté le 6 décembre 2021.

AKRICH Madeleine, 2010, « Comment Décrire Les Objets Techniques? », *Techniques & Cultures*, 2010, vol. 54-55, n° 9, p. 205-219.

AKRICH Madeleine, 1989, « La construction d'un système socio-technique – Esquisse pour une anthropologie des techniques », *Anthropologie et Sociétés*, 1989, vol. 13, n° 2, p. 31-54.

ALARY Pierre, 2009, « La genèse de la monnaie : les théories économiques face aux enseignements de l'anthropologie et de l'histoire », *Cahiers d'économie Politique / Papers in Political Economy*, 2009, n° 56, p. 129-149.

ALARY Pierre, BLANC Jérôme, DESMEDT Ludovic et THÉRET Bruno, 2016, « Colloque international : « Institutionnalismes monétaires francophones : (...) - Triangle - UMR 5206 ».

ALI Robleh, BARRDEAR John, CLEWS Roger et SOUTHGATE James, 2013, « The economics of digital currencies », *Bank of England Quarterly Bulletin*, 2013, vol. Q3, n° 1, p. 38-47.

ALISIE Mihai, 2014, « The ethereum project: learning to dream with open minds », <https://blog.ethereum.org/2014/07/14/the-ethereum-project/>, 14 juillet 2014, consulté le 11 octobre 2020.

ALLAIRE Gilles, 2013, « Les communs comme infrastructure institutionnelle de l'économie marchande », *Revue de la régulation. Capitalisme, institutions, pouvoirs*, 12 décembre 2013, n° 14.

ALLARD Laurence, 2018, « Cryptomonnaies: usages et pratiques », Science, Travail & Environnement, *Revue Progressistes*, 11 mai 2018, n° 19.

ALLARD Laurence, 2017, « Le bitcoin s'adresse aussi aux exclus du système bancaire », <https://www.humanite.fr/laurence-allard-le-bitcoin-sadresse-aussi-aux-exclus-du-systeme-bancaire-647243>, 12 décembre 2017, consulté le 4 mars 2021.

AMABILE Serge, PENERANDA Adrien et HALLER Coralie, 2018, « Management des biens communs de la connaissance : principes de conception et gouvernance de l'action collective », *Systèmes d'information & management*, 2018, vol. 23, n° 1, p. 11.

AMATO Étienne Armand, 2008, « Quelle ethnométhodologie appliquer aux jeux vidéo multijoueurs persistants ? », *Sens Public*, mars 2008, p. 24.

AMMOUS Saifedean, 2018, *The Bitcoin Standard - The Decentralized Alternative to Central Banking*, John Wiley & Sons, Inc., Hoboken, New Jersey, 305 p.

ANDOLFATTO David, 2016, « MacroMania: Is Bitcoin a Safe Asset? », <https://andolfatto.blogspot.com/2016/03/is-bitcoin-safe-asset.html>, 27 mars 2016, consulté le 19 février 2021.

ANDOLFATTO David, 2013, « MacroMania: Why gold and bitcoin make lousy money », <https://andolfatto.blogspot.com/2013/04/why-gold-and-bitcoin-make-lousy-money.html>, 24 avril 2013, consulté le 19 février 2021.

ANDRESEN Gavin, 2016, « One-dollar lulz • Gavin Andresen », <http://gavinandresen.ninja/One-Dollar-Lulz>, 3 mars 2016, consulté le 8 novembre 2021.

ANDRESEN Gavin, 2012, « Blockchain Rule Update Process », <https://gist.github.com/gavinandresen/2355445>, 11 avril 2012, consulté le 11 décembre 2019.

ANDRESEN Gavin, 2011, « Bitcoin / [bitcoin-list] Bitcoin version 0.3.20.01 released ».

ANDRI OLAFSSON Isak, 2014, « Is Bitcoin money? An analysis from the Austrian school of economic thought », School of Social Sciences at the University of Iceland, s.l.

ANONYME, 2018, « reward schedule - How does the most recently found critical vulnerability (CVE-2018-17144) work? »

ANSELLINDER et BTCMRKT, 2018, « Bitcoin History », <https://github.com/Bitcoin-and-Markets/resources/wiki/Bitcoin-History>, 6 septembre 2018, consulté le 26 janvier 2023.

ANTONOPoulos Andreas, 2013, « Bitcoin Neutrality - Bitcoin 2013 Conference ». <https://www.youtube.com/watch?v=EiW4lKrMXQ4>, consulté le 16 octobre 2016

ANTONOPoulos Andreas, « *Bitcoin Q&A: What is the Appeal of Sound Money?* », 2018, <https://www.youtube.com/watch?v=tfba4FFErrQ>, consulté le 8 juillet 2023.

ANTONOPoulos Andreas, « *Bitcoin Q&A: CVE-2018-17144 Vulnerability* », 2018, <https://www.youtube.com/watch?v=5GD0kGT0SU0>, consulté le 17 mars 2021.

APODACA Rich, 2017, « An Introduction to Bcoin », *Bitzuma*, <https://bitzuma.com/posts/an-introduction-to-bcoin/>, 7 novembre 2017, consulté le 13 octobre 2021.

APODACA Rich, 2015, « script - Which release fixed CVE-2010-5141 (attacker can spend any coin) ».

ARVICCO, 2016a, « ETC exchange trading and other news », *Ethereum Classic*, <https://ethereumclassic.github.io/blog/2016-07-24-polo-trading/>, 24 juillet 2016, consulté le 27 mars 2019.

ARVICCO, 2016b, « ETC - new Ethereum Classic ticker symbol », *Ethereum Classic*, <https://ethereumclassic.github.io/blog/2016-07-22-etc-ticker/>, 22 juillet 2016, consulté le 27 mars 2019.

ARVICCO, 2016c, « What can I do to help Ethereum Classic project? », *Ethereum Classic*, <https://ethereumclassic.github.io/blog/2016-07-25-call-for-action/>, 25 avril 2016, consulté le 27 mars 2019.

ATTAQUANT AUTO-PROCLAMÉ Anonyme, 2016, « An Open Letter », <https://pastebin.com/CcGUBgDG>, 18 juin 2016, consulté le 3 juin 2020.

ATZEI Nicola, BARTOLETTI Massimo et CIMOLI Tiziana, 2017, « A Survey of Attacks on Ethereum Smart contracts (SoK) » dans Matteo Maffei et Mark Ryan (dir.), *Principles of Security and Trust*, Berlin, Heidelberg, Springer Berlin Heidelberg (coll. « Lecture Notes in Computer Science »), vol.10204, p. 164-186.

AURYN Macmillan, 2016, « Who or What is DAOhub.org? – DAOhub », <https://archive.is/U9Z54>, 16 juin 2016, consulté le 10 mai 2024.

AVENIER Marie-josé et THOMAS C., 2011, « Mixer quali et quanti pour quoi faire ? Méthodologie sans épistémologie n'est que ruine de la réflexion ! », *Cahier de recherche*, 2011, n° 2011-06, juillet, p. 1-26.

AWEMANY, 2018, « 600 Microseconds - A perspective from the Bitcoin Cash and Bitcoin Unlimited developer who discovered CVE-2018-17144 », <https://medium.com/@awemany/600-microseconds-b70f87b0b2a6>, consulté le 20 septembre 2019.

BAKER Paddy, 2020, « Swiss Canton Zug to Accept Taxes in Bitcoin, Ether From Next Year », <https://www.coindesk.com/swiss-canton-zug-accept-taxes-crypto-bitcoin-ether-2021>, 3 septembre 2020, consulté le 10 octobre 2020.

BALAKRISHNAN Ashwath, 2020, « After Second Double Spend Attack, Ethereum Classic's Future Is in Question », <https://cryptobriefing.com/after-second-double-spend-attack-ethereum-classics-future-is-question/>, 6 août 2020, consulté le 4 octobre 2022.

BALTAZARD M Maurice, 1956, « Le Franc et son histoire », s.é., s.l, p. 14.

BANK OF INTERNATIONAL SETTLEMENTS, 2018, V. « Cryptocurrencies: looking beyond the hype », <https://www.bis.org/publ/arpdf/ar2018e5.pdf>, consulté le 24 juin 2019.

BANO Shehar, ALBERTO Sonnino, AL-BASSAM Mustafa, AZOUI Sarah, MCCORRY; Patrick, MEIKLEJOHN Sarah et DANEZIS George, 2017, « SoK: Consensus in the Age of Blockchains », <https://arxiv.org/pdf/1711.03936.pdf>, consulté le 5 mai 2018.

BANQUE DE FRANCE, 2013, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus*, vol. 05/12/2013, n° 10.

BARLOW John Perry, 2016, « A Declaration of the Independence of Cyberspace », <https://www.eff.org/fr/cyberspace-independence>, 20 janvier 2016, consulté le 6 mai 2020.

BARON Catherine, 2003, « La gouvernance : débats autour d'un concept polysémique », *Droit et société*, 2003, vol. 2, n° 54.

BARRO Robert J., 1986, « Recent Developments in the Theory of Rules Versus Discretion », *The Economic Journal*, 1986, vol. 96, p. 23-37.

BARTOLETTI Massimo et POMPIANU Livio, 2017, « An analysis of Bitcoin OP RETURN metadata », *arXiv preprint arXiv:1702.01024.*, 2017.

BERCY INFOS, 2020, « Crypto-monnaies, crypto-actifs... Comment s'y retrouver ? », <https://www.economie.gouv.fr/particuliers/cryptomonnaies-cryptoactifs>, 4 décembre 2020, consulté le 29 janvier 2021.

BERRY Vincent, 2012, « Ethnographie sur Internet : rendre compte du « virtuel » , *Les Sciences de l'éducation - Pour l'Ère nouvelle*, 2012, vol. 45, n° 4, p. 35.

BEZBAKH Pierre, 2019, *Inflation et désinflation*, Paris, La Découverte (coll. « Repères »), vol.7e éd., 128 p.

BIER Jonathan, 2021a, « The Blocksize War – Chapter 16 – Litecoin » dans *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, s.l., s.é., 227 p.

BIER Jonathan, 2021b, « The Blocksize War – Chapter 3 – Scaling I – Montreal » dans *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, s.l., s.é., 227 p.

BIER Jonathan, 2021c, « The Blocksize War – Chapter 8 – Hong Kong Roundtable » dans *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, s.l., s.é., 227 p..

BIER Jonathan, 2021d, « The Blocksize War – Chapter 2 – March To War » dans *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, s.l., s.é., 227 p.

BIER Jonathan, 2021e, « The Blocksize War – Chapter 4 – Scaling II – Hong Kong » dans *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, s.l., s.é., 227 p.

BIER Jonathan, 2021f, « The Blocksize War – Chapter 18 – New York Agreement » dans *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, s.l., s.é., 227 p.

BIER Jonathan, 2018, « BitMEX Research Sponsors Fork Monitoring Website », <https://blog.bitmex.com/bitmex-research-sponsors-Fork-monitoring-website/>, 5 novembre 2018, consulté le 4 octobre 2022.

BIT2ME ACADEMY, « Qui est Martti Malmi ? », <https://academy.bit2me.com/fr/qui-est-martti-malmi/>, consulté le 12 octobre 2021.

BIT2MEACADEMY, 2020, « Who Is Wladimir Van Der Laan? », <https://academy.bit2me.com/en/who-is-wladimir-van-der-laan/>, 7 juillet 2020, consulté le 3 janvier 2022.

BITCOIN CORE, 2018a, « CVE-2018-17144 Full Disclosure », <https://bitcoincore.org/en/2018/09/20/notice/>, 20 septembre 2018, consulté le 20 septembre 2019.

BITCOIN CORE, 2018b, « CONTRIBUTING to Bitcoin Core », <https://github.com/chaintope/tapyrus-core/blob/master/CONTRIBUTING.md>, 2018, consulté le 24 septembre 2024.

BITCOIN CORE, 2014, « Bitcoin Core version 0.9.0 released », <https://bitcoin.org/en/release/v0.9.0#downgrading-warnings> , 19 mars 2014, consulté le 2 juin 2023.

BITCOIN FONDATION, 2014, « The Foundation's Vision », *The Bitcoin Foundation*, <https://web.archive.org/web/20141017203338/https://bitcoinfoundation.org/the-foundations-vision/>, 17 octobre 2014, consulté le 23 juin 2020.

BITCOIN FONDATION, 2013, « Bitcoin Foundation: About », <https://web.archive.org/web/20130702232207/https://bitcoinfoundation.org/about/>, 2 juillet 2013, consulté le 6 août 2020.

BITCOIN OPTECH, 2018, « Bitcoin Optech Newsletter #13 ».

BITCOIN WIKI, « Common Vulnerabilities and Exposures », [https://en.bitcoin.it/wiki/Common\\_Vulnerabilities\\_and\\_Exposures](https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures), consulté le 22 février 2024.

BITCOIN.FR, « Les grandes dates de Bitcoin », <https://bitcoin.fr/histoire/>, consulté le 22 avril 2020.

BITMEX RESEARCH, 2020a, « Who Funds Bitcoin Development? », *BitMEX Blog*, <https://blog.bitmex.com/who-funds-bitcoin-development/>, 28 mars 2020, consulté le 21 août 2020.

BITMEX RESEARCH, 2020b, « Growth In The Level Of Precision Of Bitcoin Spending », *BitMEX Blog*, <https://blog.bitmex.com/bitcoin-transaction-output-value-precision/>, 27 janvier 2020, consulté le 28 juillet 2020.

BITMEX RESEARCH, 2018, « Competing with Bitcoin Core », *BitMEX Blog*, <https://blog.bitmex.com/bitcoin-cores-competition/>, 15 octobre 2018, consulté le 17 octobre 2019.

BITMEX RESEARCH, 2018a, « The bitcoin flash crash to \$0.01 in June 2011 », *BitMEX Blog*, <https://blog.bitmex.com/the-june-2011-flash-crash-to-0-01/>, 19 juillet 2018, consulté le 24 août 2020.

BITMEX RESEARCH, 2018b, « The Ripple story », *BitMEX Blog*, <https://blog.bitmex.com/the-ripple-story/>, 6 février 2018, consulté le 24 septembre 2020.

BITMEX RESEARCH, 2017a, « A complete history of Bitcoin's consensus Forks », *BitMEX Blog*, <https://blog.bitmex.com/bitcoins-consensus-Forks/>, 28 décembre 2017, consulté le 10 décembre 2019.

BITMEX RESEARCH, 2017b, « Revisiting “The DAO” », *BitMEX Blog*, <https://blog.bitmex.com/revisiting-the-dao/>, 22 novembre 2017, consulté le 27 mars 2019.

BITMEXRESEARCH, 2022, « The OP\_Return Wars of 2014 - Dapps Vs Bitcoin Transactions », <https://blog.bitmex.com/dapps-or-only-bitcoin-transactions-the-2014-debate/>, 12 juillet 2022, consulté le 2 août 2022.

BLANC Jérôme, 2009a, « Contraintes et choix organisationnels dans les dispositifs de monnaies sociales », *Annales de l'économie publique, sociale et coopérative*, 2009, 80:4, p. 547-577.

BLANC Jérôme, 2009b, « Usages de l'argent et pratiques monétaire » dans Presses Universitaires de France (ed.), *Traité de sociologie économique (sous la direction de P. Steiner et F. Vatin)*, Quadrige., Paris, p. 649-688.

BLANC Jérôme, 2008, « Usages de l'argent et pratiques monétaires », [halshs-00278345](https://halshs.archives-ouvertes.fr/halshs-00278345), 2008, p. 30.

BLANC Jérôme, 1998a, « Les monnaies parallèles. Approches historiques et théoriques », Université Lumière - Lyon II, 1998. French., s.l.

BLANC Jérôme, 1998b, « Les monnaies parallèles : évaluation du phénomène et enjeux théoriques », *Revue d'économie financière*, 1998, AEF, p. 81-102.

BLANC Jérôme et FARE Marie, 2017, « La monnaie, éclairages et débats institutionnalistes », *Économie et Institutions*, 31 décembre 2017, n° 26.

BLANC Jérôme et FARE Marie, 2013, « Understanding the Role of Governments and Administrations in the Implementation of Community and Complementary Currencies », *Annals of Public and Cooperative Economics*, 2013, vol. 84, n° 1, p. 63-81.

BÖHME Rainer, CHRISTIN Nicolas, EDELMAN Benjamin et MOORE Tyler, 2015, « Bitcoin: Economics, Technology, and Governance », *Journal of Economic Perspectives*, 2015, vol. 29, n° 2, p. 213-238.

BÖHME Rainer, ECKEY Lisa, MOORE Tyler, NARULA Neha, RUFFING Tim et ZOHAR Aviv, 2020, « Responsible vulnerability disclosure in cryptocurrencies », *Communications of the ACM*, 23 septembre 2020, vol. 63, n° 10, p. 62-71.

BOLLIER David, 2007, « The Growth of the Commons Paradigm » dans *Understanding knowledge as a commons: From theory to practice*, s.l.

BONNEAU Joseph, MILLER Andrew, CLARK Jeremy, NARAYANAN Arvind, KROLL Joshua A, FELTEN Edward W et FOUNDATION Electronic Frontier, 2015, « SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies », s.l.

BOUNIE David, 2001, « Quelques incidences bancaires et monétaires des systèmes de paiement électronique », *Revue économique*, 2001, vol. 52, n° 7, p. 313.

BOUNIE David et LAVOISIER Soriano, 2003, *La monnaie électronique*, Ed. Lavoisier, n°1/2003, vol. 4.

BOWKER Geoffrey C, 1996, « The history of information infrastructures: The case of the international classification of diseases », *Information Processing & Management*, janvier 1996, vol. 32, n° 1, p. 49-61.

BOYER DES ROCHES Jérôme; DE et ROSALES Ricardo Solis, 2003, « Les approches classiques du prêteur en dernier ressort : de baring à hawtrey », *Cahiers d'économie Politique*, 2003, p. 79-100.

BRADBURY Danny, 2014, « Bitcoin Transaction Fees To Be Slashed Tenfold », <https://www.coindesk.com/markets/2014/02/28/bitcoin-transaction-fees-to-be-slashed-tenfold/>, 28 février 2014, consulté le 8 novembre 2021.

BREED Cathy, 2020, « Why Work in Blockchain? — Journey from C++ to Rust Developer », <https://medium.com/centrality/why-work-in-blockchain-journey-from-c-to-rust-developer-eddbc9ccdc3d>, 22 novembre 2020, consulté le 13 octobre 2021.

BRITO B Y Jerry et CASTILLO Andrea, 2013, « Bitcoin A Primer for Policymakers », *Mercatus Center at George Mason University*, 2013.

BROADBENT Ben, 2016, « Central banks and digital currencies », *Bank of England*, 2016, March, p. 1-14.

BROKAW Alex, 2014, « The People Who Burn Bitcoins », Editor's Pick, *Minyanville's Wall Street*, <https://web.archive.org/web/20140429075927/http://www.minyanville.com/business-news/editors-pick/articles/The-People-Who-Burn-Bitcoins-bitcoin/4/16/2014/id/54627>, 29 avril 2014, consulté le 23 février 2023.

BUÉ Nicolas, 2010, « Gérer les relations d'enquête en terrains imbriqués: Risque d'enclage et distances aux enquêtés dans une recherche sur une coalition partisane locale », *Revue internationale de politique comparée*, 2010, vol. 17, n° 4, p. 77.

BUTERIN Vitalik, 2021, « Why sharding is great: demystifying the technical properties », <https://vitalik.ca/general/2021/04/07/sharding.html>, 7 avril 2021, consulté le 12 juin 2023.

BUTERIN Vitalik, 2017a, « The very earliest versions of ETH protocol were a counterparty-style metacoin on top of primecoin. Not Bitcoin because the OP\_RETURN wars were happening at the time », <https://twitter.com/VitalikButerin/status/929804867568373760>, 12 novembre 2017, consulté le 2 août 2022.

BUTERIN Vitalik, 2017b, « A Prehistory of the Ethereum Protocol », <https://vitalik.ca/general/2017/09/14/prehistory.html> , 14 septembre 2017, consulté le 7 octobre 2020.

BUTERIN Vitalik, 2017c, « Hard Forks, Soft Forks, Defaults and Coercion », [https://vitalik.ca/general/2017/03/14/Forks\\_and\\_markets.html](https://vitalik.ca/general/2017/03/14/Forks_and_markets.html) , 14 mars 2017, consulté le 29 mars 2022.

BUTERIN Vitalik, 2016a, « Uncle Rate and Transaction Fee Analysis », <https://blog.ethereum.org/2016/10/31/uncle-rate-transaction-fee-analysis/>, 31 octobre 2016, consulté le 23 octobre 2020.

BUTERIN Vitalik, 2016b, « Hard Fork Completed », <https://blog.ethereum.org/2016/07/20/hard-Fork-completed/> , 20 juillet 2016, consulté le 27 mars 2019.

BUTERIN Vitalik, 2016c, « Signature looks shad... »; [www.reddit.com/r/ethereum/comments/4oo1io/an\\_open\\_letter\\_from\\_the\\_hacker/d4e7bv3/](https://www.reddit.com/r/ethereum/comments/4oo1io/an_open_letter_from_the_hacker/d4e7bv3/). consulté le 24 mars 2023.

BUTERIN Vitalik, 2016d, « Is anyone in the pro... », [www.reddit.com/r/ethereum/comments/4oi2ta/i\\_think\\_thedao\\_is\\_getting\\_drained\\_right\\_now/d4csoa8/](https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/d4csoa8/), consulté le 24 mars 2023.

BUTERIN Vitalik, 2016e, « Critical update re: DAO vulnerability », <https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/>, 17 juin 2016, consulté le 17 juin 2016.

BUTERIN Vitalik, 2016f, « history - The Ether denominations are called Finney, Szabo, and Wei. What/who are these named after? », <https://ethereum.stackexchange.com/questions/253/the-ether-denominations-are-called-finney-szabo-and-wei-what-who-are-these-na>, consulté le 04 janvier 2019

BUTERIN Vitalik, 2014a, « On Bitcoin Maximalism, and Currency and Platform Network Effects », <https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects>, 20 octobre 2014, consulté le 15 août 2024.

BUTERIN Vitalik, 2014b, « Ether Sale: A Statistical Overview », <https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/>, 8 août 2014, consulté le 8 octobre 2020.

BUTERIN Vitalik, 2014c, « Launching the Ether Sale », <https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/> , 22 juillet 2014, consulté le 8 octobre 2020.

BUTERIN Vitalik, 2014d, « Toward a 12-second Block Time », <https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/> , 11 juillet 2014, consulté le 11 octobre 2020.

BUTERIN Vitalik, 2014e, « On Stake », <https://blog.ethereum.org/2014/07/05/stake/>, 5 juillet 2014, consulté le 11 octobre 2020.

BUTERIN Vitalik, 2014f, « On Mining », <https://blog.ethereum.org/2014/06/19/mining/>, 19 juin 2014, consulté le 11 octobre 2020.

BUTERIN Vitalik, 2014g, « Pyethereum and Serpent Programming Guide », <https://blog.ethereum.org/2014/04/10/pyethereum-and-serpent-programming-guide/>, 10 avril 2014, consulté le 11 octobre 2020.

BUTERIN Vitalik, 2014h, « More Thoughts on Scripting and Future-Compatibility », <https://blog.ethereum.org/2014/02/05/more-thoughts-on-scripting-and-future-compatibility/>, 5 février 2014, consulté le 11 octobre 2020.

BUTERIN Vitalik, 2014i, « Introducing Ethereum Script 2.0 », <https://blog.ethereum.org/2014/02/03/introducing-ethereum-script-2-0/>, 3 février 2014, consulté le 11 octobre 2020.

BUTERIN Vitalik, 2014j, « Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform », *bitcoinnmagazine.com*, 24 janvier 2014.

BUTERIN Vitalik, 2013a, « Ethereum: The Ultimate Smart Contract and Decentralized Application Platform », <http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html> , 28 décembre 2013, consulté le 6 octobre 2020.

BUTERIN Vitalik, 2013b, « Mastercoin: A Second-Generation Protocol on the Bitcoin Blockchain », <https://bitcoinnmagazine.com/technical/mastercoin-a-second-generation-protocol-on-the-bitcoin-blockchain-1383603310> , 4 novembre 2013, consulté le 31 mai 2023.

BUTERIN Vitalik, 2013c, « The Bitcoin Gambling Diaspora », <https://bitcoinnmagazine.com/articles/the-bitcoin-gambling-diaspora-1375548799> , 3 août 2013, consulté le 5 août 2020.

BUTERIN Vitalik, 2013d, « Ethereum Whitepaper ». (trad en fr. <https://ethereum.org/fr/whitepaper/>) consulté le 21 octobre 2019.

BUTERIN Vitalik, 2013e, « Dagger: A Memory-Hard to Compute, Memory-Easy to Verify Scrypt Alternative », <http://www.hashcash.org/papers/dagger.html>, consulté le 10 septembre 2020.

BUTERIN Vitalik et SCHOEDON Afri, 2017, « EIP-649: Metropolis Difficulty Bomb Delay and Block Reward Reduction », <https://eips.ethereum.org/EIPS/eip-649>, 21 juin 2017, consulté le 16 juin 2023.

CALLON Michel, 2006, « Pour une sociologie des controverses technologiques » dans Madeleine Akrich, Michel Callon et Bruno Latour (dir.), *Sociologie de la traduction*, s.l., Presses des Mines, p. 135-157.

CALLON Michel, 1986, « Éléments pour une sociologie de la traduction : La domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc », *L'année sociologique*, 1986, vol. 36, p. 41.

CAMPBELL By Rebecca, 2016, « Robin Hood Counter Attack : DAO Is Empty , 7 Mln Ether Secured », 22 juin 2016, vol. 977, p. 2-5.

CARNEY Mark, 2019, « The Growing Challenges for Monetary Policy in the current International Monetary and Financial System », discours donné par Mark Carney, Governor de la Bank of England, Jackson Hole Symposium 2019, 23 août 2019.

CARRÉ Emmanuel, 2014, « Une histoire du ciblage de l'inflation : science des théoriciens ou arts des banquiers centraux ? », *Cahiers d'économie Politique*, 1 juin 2014, n° 66, n° 1, p. 127-171.

CARTELIER Jean, 2002, « Monnaie ou don : réflexions sur le mythe économique de la monnaie », *Journal des anthropologues*, vol. 90-91, p. 335-374.

CARTELIER Jean, 2001, « Monnaie et marché: Un point de vue critique sur les modèles de prospection », *Revue Économique*, vol. 52, n° 5, sept. 2001, p. 993-1011.

CARTELIER Jean, 1996, *La monnaie*, Dominos. Flammarion, Paris, 125 p.

CARTER Nic, 2020, « Nine Bitcoin Charts Already at All-Time Highs », [https://medium.com/@nic\\_carter/nine-bitcoin-charts-already-at-all-time-highs-78abbfe82804](https://medium.com/@nic_carter/nine-bitcoin-charts-already-at-all-time-highs-78abbfe82804), 17 novembre 2020, consulté le 4 mars 2021.

CARTER Nic et HASUFLY, 2018, « Visions of Bitcoin », [https://medium.com/@nic\\_carter/visions-of-bitcoin-4b7b7cbcd24c](https://medium.com/@nic_carter/visions-of-bitcoin-4b7b7cbcd24c), 2 août 2018, consulté le 22 novembre 2021.

CASTILLO Michael del, 2016, « The DAO: Or How A Leaderless Ethereum Project Raised \$50 Million », <https://www.coindesk.com/the-dao-just-raised-50-million-but-what-is-it>, 12 mai 2016, consulté le 15 mai 2019.

CASTILLO Michael del, 2013, « Dark Wallet: A Radical Way to Bitcoin », <https://www.newyorker.com/business/currency/dark-wallet-a-radical-way-to-bitcoin>, 24 septembre 2013, consulté le 4 août 2020.

CASTOR Amy, 2017, « In Santa Barbara, An Annual Event Brings Together Those Closest To Bitcoin's Roots », <https://www.forbes.com/sites/amycastor/2017/08/30/in-santa-barbara-an-annual-event-brings-together-those-central-to-bitcoins-roots/#7bf7f4867b60>, 30 août 2017, consulté le 18 août 2020.

CEFAI Daniel, 2009, « Codifier l'engagement ethnographique ? », *L'Engagement ethnographique*, Paris, Éditions des Hautes Études en Sciences Sociales, 2009, p. 1-27.

CHAINALYSIS TEAM, 2020, « 60% of Bitcoin is Held Long Term as Digital Gold. What About the Rest? », <https://blog.chainalysis.com/reports/bitcoin-market-data-exchanges-trading>, 18 juin 2020, consulté le 29 janvier 2021.

CHAINALYSIS TEAM, 2019, « Chainalysis Crypto Crime Report (2019) », <https://go.chainalysis.com/rs/503-FAP-074/images/2019%20Chainalysis%20Crypto%20Crime%20Report.pdf>, janvier 2019, consulté le 21 août 2020.

CHAINALYSIS TEAM, 2018, « Bitcoin's \$30 billion sell-off », <https://blog.chainalysis.com/reports/money-supply>, 8 juin 2018, consulté le 3 août 2020.

CHAMPAGNE Phil, 2014, *The Book Of Satoshi - The Collected Writings of Bitcoin Creator Satoshi Nakamoto*, s.l., e53 Publishing LLC.

CHANTEAU Jean-Pierre et LABROUSSE Agnès, 2013, « L'institutionnalisme méthodologique d'Elinor Ostrom : quelques enjeux et controverses », *Revue de la régulation*, 12 décembre 2013, n° 14.

CHANUT Guillaume, 2019, « La programmation avec Bitcoin : Les courbes elliptiques », <https://cryptostat.fr/programmation-bitcoin-courbes-elliptiques/>, 11 novembre 2019, consulté le 4 août 2020.

CHAUM David, 1996, « 05-07-96 – DigiCash\_s Ecash™ to be Issued by Deutsche Bank », [https://www.chaum.com/ecash/articles/1996/05-07-96%20-%20DigiCash\\_s%20Ecash%20to%20be%20Issued%20by%20Deutsche%20Bank.pdf](https://www.chaum.com/ecash/articles/1996/05-07-96%20-%20DigiCash_s%20Ecash%20to%20be%20Issued%20by%20Deutsche%20Bank.pdf), 7 mai 1996, consulté le 6 mai 2020.

CHAUM David, 1994, « 05-27-94 - World\_s first electronic cash payment over computer networks », <https://www.chaum.com/ecash/articles/1994/05-27-94%20->

%20World\_s%20first%20electronic%20cash%20payment%20over%20computer%20networks.pdf, 27 mai 1994, consulté le 6 mai 2020.

CHAUM David, 1985, « Security without Identification Card Computers to make Big Brother Obsolete », *Communications of the ACM*, vol 28, n° 10, p. 1030-1044.

CHAUM David, 1982, « Blind Signatures for Untraceable Payments », *Crypto*, 1982, vol. 82, p. 199-203.

CHAVANCE Bernard, 2011, « Karl Polanyi, l'économie et la société » dans *La Subsistante de l'homme. La place de l'économie dans l'histoire et la société*, Flammarion., Paris, (coll. « Bibliothèque des savoir »), p.vii-xix.

CHEN Adrian, 2011, « The Underground Website Where You Can Buy Any Drug Imaginable », <http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>, 6 janvier 2011, consulté le 30 juillet 2020.

CHIANG Christine, 2017, « Alternative Implementation Bcoin Mines First Block », <https://btcmanger.com/alternative-implementation-bcoin-mines-its-first-block/>, 14 mars 2017, consulté le 13 octobre 2021.

CHOHAN Usman W., 2017, *The Decentralized Autonomous Organization and Governance Issues*, Rochester, NY, Social Science Research Network.

CHRISTIN Nicolas, 2013, « Traveling the silk road: a measurement analysis of a large anonymous online marketplace », Rio de Janeiro Brazil, ACM.

CLASSIC Ethereum et ARVICCO (PSEUDONYME), 2016, « La déclaration d'indépendance d'Ethereum Classic », <https://ethereumclassic.org/fr/blog/2016-08-13-declaration-of-independence>, 13 août 2016, consulté le 6 août 2024.

CNET NEWS, 1997, « CyberCash, First Virtual lose big », <https://www.cnet.com/news/cybercash-first-virtual-lose-big/>, 31 janvier 1997, consulté le 20 août 2020.

COHEN Benjamin J., 2002, « Monnaie électronique : un jour nouveau ou une aube trompeuse ? », *L'Économie politique*, 2002, vol. 14, n° 2, p. 67.

COHEN Benjamin J., 1998, *The Geography of Money*, Ithaca, Cornell University Press, 229 p.

COLDEWEY David, 2014, « Dogecoin cryptocurrency donors help send Indian athletes to Sochi », <http://www.nbcnews.com/tech/tech-news/dogecoin-cryptocurrency-donors-help-send-indian-athletes-sochi-flna2D12024654>, 30 janvier 2014, consulté le 3 septembre 2020.

COLOMÉ Jordi Pérez, 2022, « Jorge Stolfi: ‘Technologically, bitcoin and blockchain technology is garbage’ », <https://english.elpais.com/science-tech/2022-07-07/jorge-stolfi-technologically-bitcoin-and-blockchain-technology-is-garbage.html>, 7 juillet 2022, consulté le 6 octobre 2022.

COMMISSION D'ENRICHISSEMENT DE LA LANGUE FRANÇAISE, 2017, *Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés)*; NOR : CTNR1713838K; Liste du 23-5-2017 - J.O. du 23-5-2017; MEN - MESRI - MC, <https://www.education.gouv.fr/bo/17/Hebdo28/CTNR1713838K.htm> , 23 mai 2017, consulté le 29 janvier 2021.

COPPOLA Frances, 2018, « The Bitcoin Standard - a critical review », <https://www.coppolacomment.com/2018/04/the-bitcoin-standard-critical-review.html>, 11 avril 2018, consulté le 3 février 2021.

CORIAT Benjamin, 2010, « La crise de l'idéologie propriétaire et le retour des communs », *Contretemps*, 27 mai 2010, p. 13.

CORIAT Benjamin et BROCA Sébastien, 2015, « Le logiciel libre et les communs », *Revue internationale de droit économique*, 2015, XXIX, n° 3, p. 265-284.

COSTEA Vlad, 2019, « Guix Makes Bitcoin Core Development More Trustless », <https://bitcoinmagazine.com/technical/guix-makes-bitcoin-core-development-trustless>, 14 août 2019, consulté le 5 octobre 2021.

COUPPEY-SOUBEYRAN Jézabel, 2021, « La monnaie légale est-elle le bien public qu'elle prétend être ? », *Le Monde*, 4 déc. 2021.

COURBIS Bernard, FROMENT Éric et SERVET Jean-Michel, 1990, « A propos du concept de monnaie », *Cahiers d'économie politique*, 1990, vol. 18, n° 1, p. 5-29.

COURS DE JUSTICE DE L'UNION EUROPÉENNE, 2015, « ARRÊT DE LA COUR (cinquième chambre) 22 octobre 2015 ; Renvoi préjudiciel – Système commun de taxe sur la valeur ajoutée (TVA) – Directive 2006/112/CE – Articles 2, paragraphe 1, sous c), et 135, paragraphe 1, sous d) à f) – Services à titre onéreux – Opérations de change de la devise virtuelle ‘bitcoin’ contre des devises traditionnelles – Exonération ».

COUTROT Thomas et REBÉRIOUX Antoine, 2005, « Gouvernance d'entreprise : quels pouvoirs pour quelles finalités ? », *Note élaborée dans le cadre du groupe de travail du Conseil scientifique d'Attac « Economie solidaire et démocratie économique »*, février 2005, p. 37.

CREATIS Claire Mouton, 2017, « Etat de l'Art des Forges Logicielles », 2017, p. 1-45.

CRYPTOAST, 2022, « « HODL » – Un signe de ralliement de la communauté Bitcoin (BTC) », <https://cryptoast.fr/hodl-signe-ralliement-communaute-bitcoin-btc/>, 27 juin 2022, consulté le 28 août 2024.

CUEN Leigh, 2020, « Cypherpunk Myths and Bitcoin in Real Life with Udi Weheimer », <https://www.coindesk.com/cypherpunk-myths-and-bitcoin-in-real-life>, 14 mars 2020, consulté le 19 mars 2020.

CVLLR Jean, 2018, « The Value Overflow Incident in the Bitcoin Blockchain — 15th August, 2010 », <https://medium.com/@jeancvllr/the-value-overflow-incident-in-the-bitcoin-blockchain-15th-august-2010-a59a516e03db>, 30 août 2018, consulté le 14 juin 2019.

D Lola, 2020, « Namecoin : la deuxième cryptomonnaie de Satoshi Nakamoto », <https://journalducoin.com/altcoins/actualites-altcoins/namecoin-la-deuxieme-cryptomonnaie-de-satoshi-nakamoto/>, 23 mai 2020, consulté le 22 juillet 2020.

DAI Wei, 1998, « B-money », <https://nakamotoinstitute.org/library/b-money/>, consulté le 12 février 2016.

DAIAN Phil, 2016, « Analysis of the DAO exploit », <http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>, 18 juin 2016, consulté le 21 juin 2016.

DAOHUB, 2016, « DAOhub Verification of 0xbb9bc244d798123fde783fcc1c72d3bb8c189413 », <https://blog.daohub.org/daohub-verification-of-0xbb9bc244d798123fde783fcc1c72d3bb8c189413-d755317ee724>, 3 mai 2016, consulté le 23 mai 2019.

DASHJR Luke, 2019, « CVE-2018–20587 Advisory and Full Disclosure (Bitcoin Core & Knots, on multiuser systems) », <https://medium.com/@lukedashjr/cve-2018-20587-advisory-and-full-disclosure-a3105551e78b>, 8 février 2019, consulté le 23 septembre 2019.

DASHJR Luke, 2014a, « [ANN][XCP] Counterparty - Pioneering Peer-to-Peer Finance - Official Thread 1/2 », <https://bitcointalk.org/index.php?topic=395761.msg5816503#msg5816503>, 21 mars 2014, consulté le 5 juin 2023.

DASHJR Luke, 2014b, « [ANN][XCP] Counterparty - Pioneering Peer-to-Peer Finance - Official Thread », <https://bitcointalk.org/index.php?topic=395761.msg5817170#msg5817170>, 21 mars 2014, consulté le 5 juin 2023.

DE FILIPPI Primavera, 2013, « Bitcoin: a regulatory nightmare to a libertarian dream », *Internet Policy Review*, 2013, vol. 3, n° 2, p. 43.

DE FILIPPI Primavera et LOVELUCK Benjamin, 2016, « The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure », *Internet Policy Review*, 2016, vol. 5, n° 3, p. 1-28.

DE TYCHEY Jérôme, 2016, « DAO Kézako - Comprendre l'Organisation Autonome Décentralisée », <https://www.ethereum-france.com/blog/dao-kezako-comprendre-lorganisation-autonome-decentralisee/>, 24 mai 2016, consulté le 10 mai 2024.

DECRYPT, 2020, « What will happen to Bitcoin after all 21 million are mined? », <https://medium.com/@decryptmedia/what-will-happen-to-bitcoin-after-all-21-million-are-mined-7a5e320d56f7>, 29 juillet 2020, consulté le 15 octobre 2022.

DEMIRGÜÇ-KUNTASLI Asli et DETRAGIACHE Enrica, 1998, *Financial Liberalization and Financial Fragility*, World Bank, Development Research Group and International Monetary Fund, Research Dept., Washington, DC, 48 p.

DENARDIS Laura et MUSIANI Francesca, 2014, « Governance by Infrastructure: Introduction, “The Turn to Infrastructure in Internet Governance” » dans *The turn to Infrastructure in Internet Governance*, Macmillian Palgrave., New York, p. 31.

DENIS David J., 2020, « Why do maintenance and repair matter? » dans Ignacio Farias, Celia Roberts et Anders Blok (dir.), *The Routledge companion to actor-network theory*, London ; New York, Routledge, Taylor & Francis Group.

DEPARTMENT OF THE TREASURY Financial Crimes Enforcement Network, 2013, « Guidance Issued: Application of FinCEN's Regulations to Persons Administering , Exchanging , or Using Virtual Currencies », 18 mars 2013, vol. 100, mm, p. 1-6.

DEQUECH David, 2013, « Is money a convention and/or a creature of the state? the convention of acceptability, the state, contracts, and taxes », *Journal of Post Keynesian Economics*, 1 janvier 2013, vol. 36, n° 2, p. 251-274.

DERMODY, 2014, « Counterparty: Enabling Decentralization with Insight - Bitcore Blog », <https://web.archive.org/web/20140428153357/https://bitcore.io/blog/articles/counterparty-enabling-decentralization-with-insight/>, 28 avril 2014, consulté le 1 juin 2023.

DESMEDT Ludovic et LAKOMSKI-LAGUERRE Odile, 2015, « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, 2015, 18 | 2e se.

DESMEDT Ludovic et PIÉGAY Pierre, 2007, « Monnaie, État et Production : apports et limites de l'approche néo-chartaliste », *Cahiers d'Économie Politique*, 2007, vol. 52, n° 1, p. 115.

DODD Nigel, 2017, « The Social Life of Bitcoin », *Theory, Culture & Society*, 2017, p. 1-27.

DODGSON Mark, GANN David, WLADAWSKY-BERGER Irving, SULTAN Naveed et GEORGE Gerard, 2015, « Managing Digital Money », *Academy of Management Journal*, avril 2015, vol. 58, n° 2, p. 325-333.

DOEPKE Matthias et SCHNEIDER Martin, 2017, « Money as a Unit of Account », *Econometrica*, 2017, vol. 85, n° 5, p. 1537-1574.

DRÉAN Gérard, 2013, « Au-delà de Bitcoin (5) : l'avenir des monnaies et systèmes de paiement », *Institut Turgot*, <https://web.archive.org/web/20130814004002/http://blog.turgot.org/index.php?post/Drean-bitcoin-fin> , 14 août 2013, consulté le 25 mai 2020.

DUCLOS Mélanie, 2014, « Que la relation d'enquête soit aussi d'amitié », *¿ Interrogations ?*, juin 2014, Implication et réflexivité, n° 18, p. 11.

DUCRÉE Jens, 2022, *Satoshi Nakamoto and the Origins of Bitcoin -- Narratio in Nomine, Datis et Numeris*, s.l.

DUFFERZAFAR, 2019, « Answer to “What is the exact « longest chain » rule implemented in the Ethereum « Homestead » protocol?” », <https://ethereum.stackexchange.com/questions/13378/what-is-the-exact-longest-chain-rule-implemented-in-the-ethereum-homestead-p>, consulté le 10 février 2020.

DUFFIELD Evan, 2014, « The Birth Of Darkcoin », <https://www.dash.org/forum/threads/the-birth-of-darkcoin.162/> , 29 mars 2014, consulté le 3 septembre 2020.

DUFY Caroline et WEBER Florence, 2007, *L'ethnographie économique*, La découverte, Paris, 122 p.

DUPONT Quinn, 2021, « Guiding Principles for Ethical Cryptocurrency, Blockchain, and DLT Research », *Cryptoeconomic Systems*, 5 avril 2021, vol. 0, n° 1.

DUPONT Quinn, 2018, « 8. Experiments in algorithmic governance: A history and ethnography of “The DAO,” a failed decentralized autonomous organization » dans Campbell-Verduyn (dir.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, Routledge, Abingdon, p. 157-177.

DUPRÉ Denis, PONSOT Jean-François et SERVET Jean-Michel, 2015, « Le bitcoin contre la révolution des communs », *5ème congrès de l'Association Française d'Economie Politique (AFEP) « L'économie politique de l'entreprise : nouveaux enjeux, nouvelles perspectives »*, juillet 2015, Lyon, France, AFEP.

EDWARDS Paul, BOWKER Geoffrey, JACKSON Steven et WILLIAMS Robin, 2009, « Introduction: An Agenda for Infrastructure Studies », *Journal of the Association for Information Systems*, mai 2009, vol. 10, n° 5, p. 364-374.

EHNTS Dirk H, 2019, « Knapp's “State Theory of Money” and its reception in German academic discourse », *Working Paper*, n° 115/2019, 2019, (coll. « Hochschule für Wirtschaft und Recht Berlin, Institute for International Political Economy (IPE), Berlin »), p. 1-32.

ELBAHRAWY Abeer, ALESSANDRETTI Laura, KANDLER Anne, PASTOR-SATORRAS Romualdo et BARONCHELLI Andrea, 2017, « Evolutionary dynamics of the cryptocurrency market », *Royal Society Open Science*, novembre 2017, vol. 4, n° 11, p. 170623.

ELECTRUM WEBSITE, 2011, « Electrum - lightweight Bitcoin client », <https://web.archive.org/web/20111109214519/http://ecdsa.org/electrum>, 9 novembre 2011, consulté le 3 mai 2023.

ELLYATT Arjun Kharpal Holly et SHILLER Robert, 2018, « Bitcoin could be here for 100 years but it's more likely to "totally collapse," Nobel laureate says », <https://www.cnbc.com/2018/01/19/bitcoin-likely-to-totally-collapse-nobel-laureate-robert-shiller-says.html>, 19 janvier 2018, consulté le 14 mai 2020.

EQUOBLEU, 2018, « CVE-2018-17144 Bitcoin... That was close. », <https://www.whitehacklabs.com/cve-2018-17144-bitcoin-that-was-close/>, 27 septembre 2018, consulté le 23 septembre 2019.

ESTEVES Ricardo, 2018, « Pigeoncoin (PGN) Hacked Due to Bitcoin Protocol Bug, Copycat Coins in Danger? », *NEWSBTC*, 2018.

ETHEREUM FOUNDATION, 2023a, « Proof-of-stake (PoS) », <https://ethereum.org> , 26 juillet 2023, consulté le 20 septembre 2023.

ETHEREUM FOUNDATION, 2023b, « Gas and fees », <https://ethereum.org> , 30 mai 2023, consulté le 14 juin 2023.

ETHEREUM FOUNDATION, 2023c, « Scaling », <https://ethereum.org> , 7 avril 2023, consulté le 20 septembre 2023.

ETHEREUM FOUNDATION, 2022, *Ethereum Foundation Report 2022*, s.l., Ethereum Foundation.

ETHEREUM FOUNDATION, 2021, « Supporting Ethereum's Client Ecosystem », <https://blog.ethereum.org/2021/03/23/supporting-ethereums-client-ecosystem/>, 23 mars 2021, consulté le 9 juin 2022.

ETHHUB, s.d., « Ethereum's Monetary Policy - EthHub », <https://docs.ethhub.io/ethereum-basics/monetary-policy/>, s.d., consulté le 11 juillet 2020.

EUROPEAN CENTRAL BANK, 2015a, *Monetary analysis*, <https://www.ecb.europa.eu/mopo/strategy/monan/html/index.en.html>, 25 juin 2015, consulté le 28 janvier 2021.

EUROPEAN CENTRAL BANK, 2015b, *Virtual Currency Schemes - A Further analysis*, Février 2015, s.l., 34 p.

EUROPEAN CENTRAL BANK, 2012, *Virtual Currency Scheme*, s.l.

FALKON Samuel, 2017, « The Story of the DAO — Its History and Consequences », *Medium*, 2017, p. 3.

FARRINGTON allen, 2021, « Random Heresies on Bitcoin and Fractional Reserve », <https://allenfarrington.medium.com/random-heresies-on-bitcoin-and-fractional-reserve-d16b9a683851>, 7 janvier 2021, consulté le 4 septembre 2023.

FAVEREAU Olivier, 2010, « La place du marché » dans Armand Hatchuel, Olivier Favereau et Franck Aggeri (dir.), *L'activité marchande sans le marché?*, Colloque de Cerisy, Presses des Mines., s.l., Presses des Mines (coll. « collection économie et gestion »), p. 111-131.

FAVEREAU Olivier, 1997, *L'incomplétude n'est pas le problème, c'est la solution*, Paris, La Découverte.

FAVIER Jacques, 2021, « Le Bitcoin, la religion du XXI<sup>e</sup> siècle née des mathématiques et d'Internet ? », *Jacques Favier - Partie I - PB16*, <https://parlonsbitcoin.com/podcasts/bitcoin-et-religion>, 14 juillet 2021, consulté le 16 novembre 2022.

FAVIER Jacques, 2017, « Tulipes », <http://blog.lavoiedubitcoin.info/post/Tulipes>, 19 septembre 2017.

FAVIER Jacques et TAKKAL BATAILLE Adli, 2017, *Bitcoin, la monnaie acéphale*, Paris, Cnrs, 280 p.

FEIERTAG Olivier et MARGAIRAZ Michel, 2012, *Les Banques centrales à l'échelle du monde. L'internationalisation des banques centrales du début du XX<sup>e</sup> siècle à nos jours / Central Banks at World Scale. The Internationalisation of Central Banks from the Early 20th Century to the Present*, Paris, Presses de Sciences Po. 276 p.

FELIXA pseudonyme, 2016a, « Updated: The next steps — part 2 — DAOhub », <https://blog.daohub.org/the-next-steps-part-2-180e58684d81>, 22 juin 2016, consulté le 27 mars 2019.

FELIXA pseudonyme, 2016b, « Update3: The DAO is under attack — but Vitalik saved us », <https://blog.daohub.org/the-dao-is-under-attack-8d18ca45011b>, 17 juin 2016, consulté le 27 mars 2019.

FIELDS Cory, 2018, « Responsible disclosure in the era of cryptocurrencies », <https://medium.com/mit-media-lab-digital-currency-initiative/http-coryfields-com-cash-48a99b85aad4>, 9 août 2018, consulté le 25 juillet 2021.

FINNEY Hal, 2009, « Bitcoin / [bitcoin-list] Crash in bitcoin 0.1.0 ».

FREECODECAMP, 2019, « The most popular programming languages used in blockchain development », <https://www.freecodecamp.org/news/the-most-popular-programming-languages-used-in-blockchain-development-5133a0a207dc/>, 18 janvier 2019, consulté le 13 octobre 2021.

FRIEDMAN Benjamin M., 2008, « Quels doivent être les objectifs de la politique monétaire. » dans Jean-Philippe Touffut (dir.), *Les banques centrales sont-elles légitimes*, Colloque du Centre Cournot, Paris, Albin Michel, p. 73-94.

FRIEDMAN Benjamin M., 1999, « The future of monetary policy: The central bank as an army with only a signal corps? », *International Finance*, 1999, vol. 2, n° 3, p. 321-338.

FRIEDMAN Milton, 1973, *The Counter-Revolution in Monetary Theory: First Wincott Memorial Lecture, Delivered at Senate House, University of London, 16 September, 1970*, London, Institute of Economic Affairs, 32 p.

FRISBY David, 1978, « Introduction to the translation » dans *The Philosophy of Money - 3rd Edition by Georg Simmel, David Frisby and Tom Bottomore, 2004*, London, Routledge, p. 1-49.

GALBRAITH JK James K, 2008, « The Collapse of Monetarism and the Irrelevance of the New Monetary Consensus », *The Levy Economics Institute of Bard College Policy Note*, 2008, vol. 1, p. 1-8.

GALBRAITH John Kenneth, 1976, *L'argent*, Paris, Gallimard . (coll. « idée, Gallimard »), collection : idées, 366 p.

GARZIK Jeff, 2014a, « [ANN][XCP] Counterparty - Pioneering Peer-to-Peer Finance - Official Thread », <https://bitcointalk.org/index.php?topic=395761.msg5796379#msg5796379>, 20 mars 2014, consulté le 5 juin 2023.

GARZIK Jeff, 2014b, « [Bitcoin-development] On OP\_RETURN in upcoming 0.9 release ».

GARZIK Jeff, 2010, « [PATCH] increase block size limit ».

GAURAV, 2019, « Bitcoin Codebase Deep Dive », <https://blog.coincodecap.com/bitcoin-development-stats>, 5 août 2019, consulté le 8 octobre 2020.

GÉNÉREUX Jacques, 1991, *Economie Politique*, Paris, Hachette, (coll. « Les fondamentaux »), vol. 3.

GERARD David, 2017, *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart contracts*, s.l., David Gerard, 184 p.

GERRING Taylor, 2016, « Cut and try: building a dream », <https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/>, 9 février 2016, consulté le 7 octobre 2020.

GERRING Taylor, 2014, « Background on the mechanics of the ether pre-sale », <https://blog.ethereum.org/2014/07/09/how-to-make-a-purchase-in-the-ether-presale/>, 9 juillet 2014, consulté le 7 octobre 2020.

GILBERT David, 2014, « \’Most Valuable Tweet in History\’ Donates \$11,000 Worth of Dogecoin to Kenyan Water Charity », <https://www.ibtimes.co.uk/most-valuable-tweet-history-donates-11000-worth-dogecoin-kenyan-water-charity-1440565>, 17 mars 2014, consulté le 3 septembre 2020.

GILBERT Emily et HELLEINER Eric, 1999, *Nation-States and Money. The past, present and future of national currencies*, Routledge., London; New York, 240 p.

GOLDBERG Sharon, HEILMAN Ethan, KENDLER Alison, ZOHAR Aviv, 2015, « Eclipse Attacks on Bitcoin’s Peer-to-Peer Network », *Proceedings of the 24<sup>th</sup> USENIX Security Symposium*, <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf>, consulté le 7 mai 2019.

GOLUMBIA David, 2015, *Bitcoin as Politics: Distributed Right-Wing Extremism*, Rochester, NY, Social Science Research Network.

GOODHART Charles, 2000, « Can Central Banking Survive Can Central Banking Survive the IT Revolution? », *Financial markets group / London School of Economic*, 2000, vol. 29, August, p. pp.1-35.

GOODHART Charles A. E., 2005, « What is the essence of money? », *Cambridge Journal of Economics*, 2005, vol. 29, n° 5, p. 817-825.

GRATSAC-LEGENDRE Valérie, 2017, « L’orfèvrerie et la monnaie au XVIII<sup>e</sup> siècle. Quelques observations autour d’une relation étrange » dans Alain Guery (dir.), *Montchrestien et Cantillon : Le commerce et l’émergence d’une pensée économique*, Lyon, ENS Éditions (coll. « Gouvernement en question(s) »), p. 305-331.

GREEN Michael W., 2021, « The Case Against Bitcoin », <https://www.thefp.com/p/the-case-against-bitcoin>, 14 mai 2021, consulté le 24 juillet 2023.

GREENBERG Andy, 2011, « Crypto Currency », <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html>, 20 avril 2011, consulté le 9 mai 2023.

GÜN SIRER Emin, 2016, « Thoughts on The DAO Hack », <http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/>, 17 juin 2016, consulté le 27 mars 2019.

GÜN SIRER Emin, KEEFER River et HESS Tjaden, 2016, « Ethereum’s DAO Wars Soft Fork is a Potential DoS Vector », <http://hackingdistributed.com/2016/06/28/ethereum-soft-Fork-dos-vector/>, 28 juin 2016, consulté le 27 mars 2019.

H Renaud, 2020, « Qui était Hal Finney, le premier à recevoir des bitcoins de Satoshi Nakamoto ? », <https://journaldulcoin.com/bitcoin/actualites-bitcoin/qui-était-hal-finney-premier-recevoir-bitcoins-satoshi-nakamoto/>, 13 janvier 2020, consulté le 13 juillet 2020.

HACKER NEWS FORUM et APO, 2018, « From the commit that fixes the issue (CVE-2018-17144), the root cause was failur... | Hacker News », <https://news.ycombinator.com/item?id=18031035>, consulté le 8 février 2022.

HAJDARBEGOVIC Nermin, 2014, « Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack », <https://www.coindesk.com/markets/2014/01/09/bitcoin-miners-ditch-ghashio-pool-over-fears-of-51-attack/>, 9 janvier 2014, consulté le 15 mai 2023.

HAJRIC Vildana, 2022, « One Bitcoin Equals One Bitcoin Becomes the Narrative as the Drop Gets ‘Too Painful’ », [Bloomberg.com](https://www.advisorperspectives.com/articles/2022/09/26/one-bitcoin-equals-one-bitcoin-becomes-the-narrative-as-the-drop-gets-too-painful), 25 sept. 2022, <https://www.advisorperspectives.com/articles/2022/09/26/one-bitcoin-equals-one-bitcoin-becomes-the-narrative-as-the-drop-gets-too-painful>, consulté le 5 avril 2023.

HARPER Colin, 2019, « Bitcoin Independence Day: How This Watershed Day Defines Community Consensus », <https://bitcoinmagazine.com/culture/bitcoin-independence-day-how-this-watershed-day-defines-community-consensus>, 1 août 2019, consulté le 5 septembre 2024.

HARRIBEY Jean-Marie, 1997, « La prise en compte des ressources naturelles et de l'environnement dans le modèle néoclassique d'équilibre générale; éléments de critique », *Économies et Sociétés. Série F, Développement, croissance et progrès*, p. 57-70.

HASDAY Antoine, 2020, « Que se passerait-il si le code informatique du bitcoin était piraté? », <https://korii.slate.fr/tech/bitcoin-scenarios-piratage-modification-code-core-blockchain-mainteneurs>, 15 décembre 2020, consulté le 6 décembre 2021.

HASU, 2018, « Ethereum Presale Dynamics Revisited », <https://medium.com/@hasufly/ethereum-presale-dynamics-revisited-c1b70ac38448>, 29 avril 2018, consulté le 6 décembre 2019.

HEARN Mike et PECK Morgan E., 2013, « Major Bug In The Bitcoin Software Tests The Community », *IEEE Spectrum*, 12 mars 2013, <https://spectrum.ieee.org/bitcoin->, consulté le 7 mars 2020.

HELD Dan et MCCORMACK Peter, 2018, « Bitcoin’s Immaculate Conception with Dan Held », *HackerNoon.com / Medium*, <https://medium.com/hackernoon/bitcoins-immaculate-conception-with-dan-held-905540eb15fa>, 1 novembre 2018, consulté le 24 novembre 2022.

HELLEINER Eric, 2003, *The making of national money: Territorial currencies in historical perspective*, Cornell Un., Ithaca, xii + 277 p.

HERTIG Alyssa, 2018a, « “Bitcoin Bug” Exploited on Crypto Fork as Attacker Prints 235 Million Pigeoncoins », <https://www.coindesk.com/bitcoin-bug-exploited-on-crypto-Fork-as-attacker-prints-235-million-pigeoncoins>, 2 octobre 2018, consulté le 14 juin 2019.

HERTIG Alyssa, 2018b, « A Long-Secret Bitcoin Key Is About to Be Revealed », <https://www.coindesk.com/markets/2018/06/26/a-long-secret-bitcoin-key-is-about-to-be-revealed/>, 26 juin 2018, consulté le 6 décembre 2021.

HESS Charlotte, 2008, « Mapping the New Commons », *SSRN Electronic Journal*, 2008.

HESS Charlotte, 2000, « Is There Anything New Under the Sun?: A Discussion and Survey of Studies on New Commons and the Internet », “*Constituting the Commons*,” the eighth biennial conference of the International Association for the Study of Common Property, 31 mai-4 juin 2000, Bloomington, Indiana.

HESS Charlotte et OSTROM Elinor, 2007, « *Understanding knowledge as a commons: From theory to practice* », The MIT Press Cambridge, Massachusetts London, England, vol.59.

HESS Charlotte et OSTROM Elinor, 2003, « Ideas, Artifacts, and Facilities: Information as a Common-pool resources », *Law and Contemporary Problems*, 2003, p. 111-145.

HINKES Andrew M, 2021, « The Limits of Code Deference », *The Journal of Corporation Law*, 19 juillet 2021, vol. 46, p. 29.

HUANG Roger, 2020, « Russia Backs Away From Total Cryptocurrency Ban », <https://www.forbes.com/sites/rogerhuang/2020/08/10/russia-backs-away-from-total-cryptocurrency-ban/>, 10 août 2020, consulté le 1 février 2021.

HUEGLI Pascal, 2022, « Bitcoin's Immaculate Conception Explained », <https://www.bitrawr.com/bitcoin/bitcoins-immaculate-conception-explained>, 14 juin 2022, consulté le 24 novembre 2022.

HUGHES Eric, 1993, « A Cypherpunk's Manifesto », <https://www.activism.net/cypherpunk/manifesto.html>, 9 mars 1993, consulté le 6 mai 2020.

HUNT Shari, 2019, « There are Two Uncle Rewards », <https://medium.com/@ShariHunt/there-are-two-uncle-rewards-a67e06fa17de>, 21 août 2019, consulté le 14 juin 2023.

I3NIKOLAI (PSEUDONYME), 2016a, « r/ethereum - From the MAKER DAO slack: "Today we discovered a vulnerability in the ETH token wrapper which would let anyone drain it." », *Reddit*, [https://www.reddit.com/r/ethereum/comments/4nmohu/from\\_the\\_maker\\_dao\\_slack\\_today\\_we\\_discovered\\_a/](https://www.reddit.com/r/ethereum/comments/4nmohu/from_the_maker_dao_slack_today_we_discovered_a/), 11 juin 2016, consulté le 27 mars 2019.

I3NIKOLAI (PSEUDONYME), 2016b, « Thanks a ton to Pete... », [www.reddit.com/r/ethereum/comments/4nmohu/from\\_the\\_maker\\_dao\\_slack\\_today\\_we\\_discovered\\_a/d45800p/](https://www.reddit.com/r/ethereum/comments/4nmohu/from_the_maker_dao_slack_today_we_discovered_a/d45800p/), *Reddit*, 11 juin 2016, consulté le 30 mars 2022.

ICHIBA HOTCHKISS Griffin, 2020, « The 1.x Files: GHOST in the Stack Machine », <https://blog.ethereum.org/2020/07/28/the-1x-files-ghost-in-the-stack-machine/>, 28 juillet 2020, consulté le 20 octobre 2020.

IMPELLIZZERI Nicolas, 2020, « Qui est Jed McCaleb, le fondateur de Ripple ? », <https://cryptost.fr/personnalite-crypto-qui-est-jed-mccaleb-fondateur-ripple/>, 12 avril 2020, consulté le 22 juillet 2020.

INGHAM Geoffrey, 2007, « The Specificity of Money », *European Journal of Sociology*, 2007, vol. 48, n° 02, p. 265-272.

INGHAM Geoffrey, 2004, *The Nature of Money*, Polity Pre., Cambridge; Malden, 254 p.

INSIDER Coin, 2021, « The story of the DAO, and how it shaped Ethereum », <https://www.coininsider.com/what-happened-to-the-dao/>, 9 juillet 2021, consulté le 9 mai 2024.

INTERNET ENGINEERING TASK FORCE, 2014, « On Consensus and Humming in the IETF », <https://datatracker.ietf.org/doc/html/rfc7282>, juin 2014, consulté le 3 janvier 2022.

JANSSENS Olivier, 2017, « Why “non-mining full nodes” are a terrible idea. », <https://medium.com/@olivierjanss/why-non-mining-full-nodes-are-a-terrible-idea-ad3c49f7a7b6>, 22 août 2017, consulté le 5 septembre 2024.

JEAN-LUC, 2018, « *Entretien avec Tim May : Aux origines du mouvement cypherpunk* », <https://bitcoin.fr/entretien-avec-tim-may-aux-origines-du-mouvement-cypherpunk/>, 20 octobre 2018, consulté le 2 juillet 2020.

JEFFREY Christopher, 2017, « *Christopher Jeffrey Consensus Pitfalls (2017-09-10)* » *Bitcoin Transcripts*, <https://btctranscripts.com/breaking-bitcoin/2017/2017-09-10-christopher-jeffrey-consensus-pitfalls/>, 10 septembre 2017, consulté le 22 juillet 2021.

JENTZSCH Christoph, 2016a, « *What an accomplishment!* », <https://web.archive.org/web/20170621071357/https://blog.slock.it/what-an-accomplishment-3e7ddea8b91d?gi=8fa1122cbd8a>, 20 juillet 2016, consulté le 17 février 2022.

JENTZSCH Christoph, 2016b, « Decentralized Autonomous Organization to Automate Governance (White paper) ».

JENTZSCH Christoph, 2016c, « The History of the DAO and Lessons Learned », *Slock.It*, 2016, p. 1-9.

JEONG Sarah, 2013, « The Bitcoin Protocol as Law, and the Politics of a Stateless Currency ».

JOHNSON Nick, 2017, « Answer to “What is the exact « longest chain » rule implemented in the Ethereum « Homestead » protocol?” »

JOURNAL OFFICIEL DE L’UNION EUROPÉENNE, 2010, « Recommandation de la Commission du 22 mars 2010 concernant l’étendue et les effets du cours légal des billets de banque et pièces en euros ».

KALLENBORN Gilbert, 2014, « Dark Wallet, le portefeuille Bitcoin qui blanchit toutes les transactions », <https://www.01net.com/actualites/dark-wallet-le-portefeuille-bitcoin-qui-blanchit-toutes-les-transactions-619144.html>, 2 mai 2014, consulté le 6 août 2020.

KANEV Alex, 2022, « 42 Bitcoin Quotes That All Investors Love », <https://coinstatics.com/bitcoin-quotes/>, 10 juin 2022, consulté le 17 avril 2024.

KARAPETSAS Lefteris, 2016a, « White Hat Siphoning has Occurred. What Now? », <https://blog.slock.it/white-hat-siphoning-has-occurred-what-now-f7ba2f8d20ef#.cs2fexc5p>, 22 juin 2016, consulté le 27 mars 2019.

KARAPETSAS Lefteris, 2016b, « White Hat Siphoning has Occurred. What Now? », <https://blog.slock.it/white-hat-siphoning-has-occurred-what-now-f7ba2f8d20ef#.p41b8kau4>, 22 juin 2016, consulté le 27 mars 2019.

KARAPETSAS Lefteris, 2016c, « It seems attacker just targeted the WhiteHatDAOs », [https://www.reddit.com/r/ethereum/comments/4p9z93/it\\_seems\\_attacker\\_just\\_targeted\\_the\\_whitehatdaos/](https://www.reddit.com/r/ethereum/comments/4p9z93/it_seems_attacker_just_targeted_the_whitehatdaos/), 22 juin 2016, consulté le 29 mai 2019.

KARAPETSAS Lefteris, 2016d, « A DAO Counter-Attack », <https://blog.slock.it/a-dao-counter-attack-613548408dd7#.icv7euyzu>, 19 juin 2016, consulté le 27 mars 2019.

KARLSTRØM Henrik, 2014, « Do libertarians dream of electric coins? The material embeddedness of bitcoin », *Distinktion*, 2014, vol. 15, n° 1, p. 23-36.

KAUSHAL Puneet Kumar, BAGGA Amadeep et SOBTI Rajeev, 2017, « Evolution of bitcoin and security risk in bitcoin wallets », Jaipur, India, IEEE.

KAVANAGH Donncha et MISCIONE Gianluca, 2017, « Infrastructures and Their Invisible Carnivalesque », *SSRN Electronic Journal*, 2017.

KEIR Andrew, 2022, « The Existence Of Bitcoin Is A Political Paradox », <https://bitcoinmagazine.com/culture/bitcoins-existence-is-a-political-paradox>, 24 août 2022, consulté le 25 août 2022.

KERNFELD Paul, 2016, « How Bitcoin Loses to the CAP Theorem - Paul Kernfeld dot com », <https://paulkernfeld.com/2016/01/15/bitcoin-cap-theorem.html>, 15 janvier 2016, consulté le 13 juillet 2020.

KESSLER Sam, 2022, « The Ethereum Merge Is Done, Opening a New Era for the Second-Biggest Blockchain », <https://www.coindesk.com/tech/2022/09/15/the-ethereum-merge-is-done-did-it-work/>, 15 septembre 2022, consulté le 20 septembre 2022.

KHARPAL Arjun, 2017, « WikiLeaks founder Assange claims he made 50,000% return on bitcoin thanks to the US government », <https://www.cnbc.com/2017/10/16/wikileaks-julian-assange-bitcoin-50000-percent-return-thanks-to-us-government.html>, 16 octobre 2017, consulté le 15 mai 2023.

KHATRI Yogita, 2021, « Swiss canton Zug now accepts bitcoin and ether for tax payments », <https://www.theblockcrypto.com/linked/95270/swiss-canton-zug-now-accepts-bitcoin-ether-tax-payments>, 18 février 2021, consulté le 4 mars 2021.

KINDELBERGER Charles, 2017, « Bitcoin is fiat money, too », <https://www.economist.com/free-exchange/2017/09/22/bitcoin-is-fiat-money-too>, 22 septembre 2017, consulté le 9 mars 2021.

KINDELBERGER Charles, 2004, *Histoire mondiale de la spéculation financière*, [1978], s.l., Valor Eds, 364 p.

KING Mervyn (Bank of England - Deputy Governor), 1999, « Challenges for monetary policy: New and old », s.l.

KING Sunny et NADAL Scott, 2012, « PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake », 19 août 2012.

KNAPP G F, 1924, « The state theory of money », *History of Economic Thought Books*, 1924.

KONING J.P., 2020, « Moneyness: The bitcoin-to-salvia divinorum trade route », <https://jpkoning.blogspot.com/2020/03/the-bitcoin-to-salvia-divinorum-trade.html>, 7 mars 2020, consulté le 13 janvier 2021.

KONING J.P., 2019a, « Moneyness: Bitcoin, 11-years in », <https://jpkoning.blogspot.com/2019/11/bitcoin-11-years-in.html>, 2 novembre 2019, consulté le 13 janvier 2021.

KONING J.P., 2019b, « The life and death of an internet monetary meme », <https://jpkoning.blogspot.com/>, 18 septembre 2019, consulté le 25 juillet 2023.

KONING J.P., 2019c, « Moneyness: Classifying cryptocurrencies », <https://jpkoning.blogspot.com/2019/07/classifying-cryptocurrencies.html>, 5 juillet 2019, consulté le 13 janvier 2021.

KONING J.P., 2018a, « Moneyness: Can lottery tickets become money? », <https://jpkoning.blogspot.com/2018/12/can-lottery-tickets-become-money.html>, 12 décembre 2018, consulté le 13 janvier 2021.

KONING J.P., 2018b, « Moneyness: Bitcoin and the bubble theory of money », <https://jpkoning.blogspot.com/2018/10/bitcoin-and-bubble-theory-of-money.html>, 13 octobre 2018, consulté le 13 janvier 2021.

KONING J.P, 2018c, « Play Bitcoin : Remember, it's just a game », <https://breakermag.com/play-bitcoin-remember-its-just-a-game/>, 7 septembre 2018, consulté le 18 janvier 2021.

KONING J.P, 2018d, « Moneyness: Tainted money », <https://jkoning.blogspot.com/2018/07/tainted-money.html>, 31 juillet 2018, consulté le 13 janvier 2021.

KONING J.P, 2018e, « Moneyness: A case for bitcoin », <https://jkoning.blogspot.com/2018/05/the-case-for-bitcoin.html>, 10 mai 2018, consulté le 13 janvier 2021.

KONING J.P, 2018f, « Moneyness: Fiatsplainin' », <https://jkoning.blogspot.com/2018/03/fiatsplainin.html>, 21 mars 2018, consulté le 13 janvier 2021.

KONING Jp, 2017, « Moneyness: The evolution of the Federal Reserve's promises as recorded on their banknotes », <https://jkoning.blogspot.com/2017/10/the-evolution-of-federal-reserves.html>, 27 octobre 2017, consulté le 9 novembre 2023.

KONING Jp, 2015, « Moneyness: The dollarization of bitcoin », <https://jkoning.blogspot.com/2015/06/the-dollarization-of-bitcoin.html>, 12 juin 2015, consulté le 18 septembre 2023.

KONING J.P, 2013, « Moneyness: Why the Fed is more likely to adopt bitcoin technology than kill it off », <https://jkoning.blogspot.com/2013/04/why-fed-is-more-likely-to-adopt-bitcoin.html>, 14 avril 2013, consulté le 1 avril 2019.

KONING J.P, 2012, « Moneyness: Bitcoin steps on the toes of a few popular monetary theories », <https://jkoning.blogspot.com/2012/10/bitcoin-steps-on-toes-of-few-popular.html>, 18 octobre 2012, consulté le 2 février 2021.

KRAKEN et SOUTHURST Jon, 2016, « Kraken to Support Direct DAO Token Trading for Fiat Currency », <https://news.bitcoin.com/kraken-dao-token-fiat/>, 27 mai 2016, consulté le 6 mai 2024.

KRANICH Nancy, 2007, « Counteracting Enclosure: Reclaiming the Knowledge Commons » dans *Understanding knowledge as a commons: From theory to practice*, The MIT Press Cambridge, Massachusetts London, England, p. 85-122.

KRUGMAN Paul, 2018a, « Opinion | Transaction Costs and Tethers: Why I'm a Crypto Skeptic », *The New York Times*, 31 juillet 2018.

KRUGMAN Paul, 2018b, « Opinion | Bubble, Bubble, Fraud and Trouble », *The New York Times*, 29 janv. 2018.

KRUGMAN Paul, 2013, « Bitcoin is Evil », [https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?\\_r=1&](https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=1&), 28 décembre 2013, consulté le 4 février 2021.

KUBÁT Max, 2015, « Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value », *Procedia Economics and Finance*, 2015, vol. 30, p. 409-416.

KUMAR JAIN Manish, 2023, « Top Programming Language for Blockchain Development », <https://www.knowledgehut.com/blog/blockchain/programming-language-for-blockchain-development>, 7 septembre 2023, consulté le 19 septembre 2023.

LACH Eric, 2011, « Feds Seeking \$7M Worth Of Privately-Minted « Liberty Dollars » », <https://talkingpointsmemo.com/muckraker/feds-seeking-7m-worth-of-privately-minted-liberty-dollars>, 4 avril 2011, consulté le 30 juin 2020.

LAGARDE Christine, 2018, « Winds of Change: The Case for New Digital Currency », *Singapore Fintech Festival*, <https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency>, 14 novembre 2018, consulté le 25 mai 2020.

LAGARDE Christine, 2017, « Fintech—A Brave New World for the Financial Sector? », <https://blogs.imf.org/2017/03/21/fintech-a-brave-new-world-for-the-financial-sector/>, 21 mars 2017, consulté le 28 octobre 2019.

LAJEUNE Gaétan, 2021, « Paymium, le précurseur français de la blockchain », <https://www.cointribune.com/analyses/personnalites/paymium-le-precurseur-francais-de-la-blockchain/>, 6 janvier 2021, consulté le 18 juillet 2022.

LARS Ludovic, 2021, « Bitcoin, quand la révolution de la monnaie vire à la religion », <https://journalducoin.com/analyses/bitcoin-revolution-monnaie-religion/>, 28 août 2021, consulté le 16 novembre 2022.

LARS Ludovic, 2020a, « Le bit gold de Nick Szabo : l'or numérique avant Bitcoin », <https://journalducoin.com/bitcoin/bit-gold-nick-szabo-or-numerique-bitcoin/>, 16 mai 2020, consulté le 2 juillet 2020.

LARS Ludovic, 2020b, « L'e-gold de Douglas Jackson : la cryptomonnaie « or » (1996) », <https://journalducoin.com/bitcoin/gold-douglas-jackson-cryptomonnaie-or-1996/>, 8 mars 2020, consulté le 2 juillet 2020.

LARS Ludovic, 2020c, « DigiCash & eCash : les cyberbucks de David Chaum (1982-90) », <https://journalducoin.com/bitcoin/digicash-ecash-cyberbucks-david-chaum-1982-90/>, 22 février 2020, consulté le 6 mai 2020.

LARS Ludovic, 2019a, « Des jetons sur Bitcoin : colored coins et autres procédés », <https://journalducoin.com/bitcoin/actualites-bitcoin/jetons-bitcoin-colored-coins-autres-procedes/>, 30 novembre 2019, consulté le 7 septembre 2020.

LARS Ludovic, 2019b, « Qu'est-ce que SegWit ? Explication technique - Bitcoin », <https://cryptoast.fr/segwit-bitcoin-explication-definition/>, 29 janvier 2019, consulté le 19 novembre 2021.

LARS Ludovic, 2018a, « Script : le langage de programmation de smart-contract Bitcoin », <https://cryptoast.fr/script-langage-programmation-bitcoin/>, 30 décembre 2018, consulté le 8 septembre 2022.

LARS Ludovic, 2018b, « Bitcoin, smart contracts et UTXO, une monnaie programmable », <https://cryptoast.fr/smart-contracts-bitcoin-monnaie-programmable-UTXO/>, 22 novembre 2018, consulté le 8 septembre 2022.

LATOUR Bruno, 2006, « Le prince : machines et machinations » dans Madeleine Akrich, Michel Callon et Bruno Latour (dir.), *Sociologie de la traduction*, s.l., Presses des Mines, p. 87-107.

LATOUR Bruno, 2000, « La fin des moyens », *Réseaux*, 2000, vol. 18, n° 100, p. 39-58.

LAYCOCK Joseph P., 2022, « Why are people calling Bitcoin a religion? », <http://theconversation.com/why-are-people-calling-bitcoin-a-religion-175717>, 3 février 2022, consulté le 1<sup>er</sup> septembre 2022.

LE CALVEZ Antoine, 2020, « Coin Metrics' State of the Network: Issue 60 - Analyzing The Early Uses of Bitcoin », <https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-25c>, 21 juillet 2020, consulté le 21 juillet 2020.

LE MAIRE Bruno, 2019, «The future of the Capital Markets Union – Towards an Investment and Savings Union », Discours lors de l'Eurofi Financial Forum 2019, <https://www.economie.gouv.fr/files/2019-09/Discours%20de%20Bruno%20Le%20Maire%20lors%20de%20l%27Eurofi%20Financial%20Forum%202019.pdf>, 13 septembre 2019.

LEE Charli, 2011, « Lite Coin White Paper », 7 octobre 2011, 6 p.

LEE Jae Hyung, 2019, *Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems*, s.l.

LÉGIFRANCE, 2019, « Article 150 VH bis - Code général des impôts - Légifrance ».

LÉGIFRANCE, 2018, « Article 150 UA - Code général des impôts - Légifrance ».

LEIGH STAR Susan et RUHLEDER Karen, 2010, « Vers une écologie de l'infrastructure : Conception et accès aux grands espaces d'information », *Revue d'anthropologie des connaissances*, 2010, Vol 4, 1, n° 1, p. 114.

LESSIG Lawrence, 2000, « Code is Law - Traduction française du célèbre article de Lawrence Lessig par Kauffmann Alexis (2010-05-22) », <https://framablog.org/2010/05/22/code-is-law-lessig/>, 2000, consulté le 12 février 2020.

LIELACHER Alex et PICKERING Andy, 2020, « Fake views: How social media bots distort the crypto narrative », *Brave New Coin*, <https://bravenewcoin.com/insights/fake-views-how-social-media-bots-are-distorting-the-crypto-narrative>, 22 septembre 2020, consulté le 9 décembre 2021.

LIGHT John, 2019, « The differences between a hard Fork, a soft Fork, and a chain split, and what they mean for the... », <https://medium.com/@lightcoin/the-differences-between-a-hard-Fork-a-soft-Fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9>, 11 mars 2019, consulté le 4 novembre 2021.

LIU Simon, 2017, « [bitcoin-dev] Responsible disclosure of bugs », <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-September/014969.html>, consulté le 13 mars 2024.

LO Stephanie et WANG J. Christina, 2014, « Bitcoin as Money? », <https://cryptochainuni.com/wp-content/uploads/Federal-Reserve-Bank-of-Boston-Current-Policy-Persepectives.pdf>, 4 septembre 2014, consulté le 22 juin 2020.

LOIBL Andreas, 2014, « Namecoin », 2014, [http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2014-08-1/NET-2014-08-1\\_14.pdf](http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2014-08-1/NET-2014-08-1_14.pdf), consulté le 23 mai 2023.

LOMBROZO Eric, 2017, « Forks, Signaling, and Activation », <https://medium.com/@elombrozo/Forks-signaling-and-activation-d60b6abda49a>, 1 juillet 2017, consulté le 6 février 2020.

LOMBROZO Eric, 2015, « BIP-0123 : BIP Classification », <https://github.com/bitcoin/bips>, 26 août 2015, consulté le 11 décembre 2019.

LOPP Jameson, 2022, « Running Bitcoin Core v0.7 and Earlier », <https://blog.lopp.net/running-bitcoin-core-v0-7-and-earlier/>, 19 mars 2022, consulté le 27 septembre 2024.

LOPP Jameson, 2021, « A History of Bitcoin Transaction Dust & Spam Storms », <https://blog.lopp.net/history-bitcoin-transaction-dust-spam-storms/>, 13 mars 2021, consulté le 8 novembre 2021.

LOPP Jameson, 2018, « Who Controls Bitcoin Core? », Medium, <https://medium.com/@lopp/who-controls-bitcoin-core-c55c0af91b8a>, 15 décembre 2018, consulté le 13 juin 2019.

LOPP Jameson, 2014, « Bitcoin Nodes: How Many is Enough? », Medium, <https://medium.com/@lopp/bitcoin-nodes-how-many-is-enough-9b8e8f6fd2cf>, 7 juin 2014, consulté le 5 septembre 2024.

LUBIN Joseph, 2014, « The Issuance Model in Ethereum », <https://blog.ethereum.org/2014/04/10/the-issuance-model-in-ethereum/>, 10 avril 2014, consulté le 23 octobre 2020.

LUSTIG Caitlin et NARDI Bonnie, 2015, « Algorithmic authority: The case of Bitcoin », *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015, vol. 2015-March, p. 743-752.

MAH-HUI LIM Michael, 2008, *Old Wine in a New Bottle: Subprime Mortgage Crisis—Causes and Consequences*, n° 532, s.l., The Levy Economics Institute.

MAJURI Yakkko, 2019, « Simply Explained: Ethereum Gas », <https://yakkomajuri.medium.com/blockchain-definition-of-the-week-ethereum-gas-2f976af774ed>, 1<sup>er</sup> avril 2019, consulté le 14 juin 2023.

MALLARD Alexandre, MÉADEL Cécile et MUSIANI Francesca, 2014, « The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin », *Journal of peer production*, 2014, p. 10.

MANGOLTE Pierre-André, 2013a, « Une innovation institutionnelle, la constitution des communs du logiciel libre », *Revue de la régulation*, 12 décembre 2013, n° 14.

MANGOLTE Pierre-André, 2013b, « Une innovation institutionnelle, la constitution des communs du logiciel libre », *Revue de la régulation*, 12 décembre 2013, n° 14.

MANNE Robert, 2011, « The Cypherpunk Revolutionary », <https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary>, 16 février 2011, consulté le 18 août 2020.

MARIANI Philippe et MARC François, 2014, *Rapport d'information fait au nom de la commission des finance sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelle*, s.l., Sénat.

MARK Dino, ZAMFIR Vlad et SIRER Emin Gün, 2016, « A Call for a Temporary Moratorium on The DAO », <https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWyS-dQ4lsBacR2dUgGTtV98C40/edit#heading=h.e437su2ytbf9>, 2016.

MASSA Annie, 2015, « Blythe Masters Says Forget Bitcoin, Embrace the Blockchain », *Bloomberg.com*, 6 oct. 2015.

MAURER Bill, NELMS Taylor C. et SWARTZ Lana, 2013, « “When perhaps the real problem is money itself!”: The practical materiality of Bitcoin », *Social Semiotics*, 2013, vol. 23, n° 2, p. 261-277.

MAUSS Marcel, 1923, *Essai sur le don. Formes et raison de l'échange dans les sociétés archaïques*, , Paris, Flammarion, rééd. 2021.

MAUSS Marcel, 1914, « Les origines de la notion de monnaie » dans *Oeuvres 2. Représentations collectives et diversité des civilisations*, Paris, Les Editions de Minuit, 1969, 106-112.

MAY Timothy C., 2018, « Enough with the ICO-Me-So-Horny-Get-Rich-Quick-Lambo Crypto », *CoinDesk*, 19 oct. 2018.

MAY Timothy C., 1994, « Tim\_may\_cyphernomicon.pdf », [https://dpya.org/en/images/9/95/Tim\\_may\\_cyphernomicon.pdf](https://dpya.org/en/images/9/95/Tim_may_cyphernomicon.pdf), 1994, consulté le 30 juin 2020.

MAY Timothy C., 1992, *The Crypto Anarchist Manifesto*, <https://www.activism.net/cypherpunk/crypto-anarchy.html>, 22 novembre 1992, consulté le 13 novembre 2016.

McCOMBIE Charlie, 2018, « New Regulations in Japan Recognise Bitcoin as a Legal Form of Payment », *Cointelegraph*, 8 mars 2018, 8 mars 2018.

MCCORMACK Peter et CORALLO Matt, 2019, « How Bitcoin Works with Matt Corallo », <https://www.whatbitcoindid.com/podcast/matt-corallo-on-how-makes-bitcoin-work>, 7 février 2019, consulté le 17 juin 2019.

MCCORMACK Peter et SONG Jimmy, 2018, « WBD037 - Jimmy Song Interview Transcription », <https://www.whatbitcoindid.com/transcription-jimmy-song>, 1 octobre 2018, consulté le 24 novembre 2021.

MCCORMACK Peter et SZABO Nick, 2019, « Nick Szabo on Cypherpunks, Money and Bitcoin », *What Bitcoin Did*, podcast, <https://www.whatbitcoindid.com/podcast/nick-szabo-on-cypherpunks-money-and-bitcoin>, consulté le 12 octobre 2020.

MCCORMACK Peter et VAN WIRDUM Aaron, 2020, « Beginner's Guide #3: Bitcoin's Pre-History and the Cypherpunks with Aaron van Wirdum », <https://soundcloud.com/what-bitcoin-did/bitcoins-pre-history-and-the-cypherpunks>, consulté le 15 octobre 2020.

MCCORMACK Peter et VOORHEES Erik, 2019, « Erik Voorhees on Understanding Libertarianism », <https://www.whatbitcoindid.com/podcast/erik-voorhees-on-understanding-libertarianism>, 24 septembre 2019, consulté le 1 février 2023.

MCCORMACK Peter et WALCH Angela, 2019, « Critiquing Bitcoin with Angela Walch », <https://medium.com/hackernoon/critiquing-bitcoin-with-angela-walch-6d3518657a92>, 24 avril 2019, consulté le 20 juillet 2022.

MCMILLAN Robert, 2012, « Lord of the Files: How GitHub Tamed Free Software (And More) », *Wired*, <https://www.wired.com/2012/02/github-2/>, 21 févr. 2012, consulté le 21 janvier 2018.

MENGER Karl, 1892, « On the Origin of Money », *the economic journal*, 1892, vol. 2, n°6, p. 1829-1841.

MÉTILLE Sylvain, 2014, « La Suisse et le bitcoin », <https://smetille.ch/2014/07/09/la-suisse-et-le-bitcoin/>, 9 juillet 2014, consulté le 4 mars 2021.

MILANO Annaliese, 2020, « About That Orange B... The History of Bitcoin's Logos », *CoinDesk*, <https://www.coindesk.com/about-that-orange-b-the-history-of-bitcoins-logos>, 20 mai 2020, consulté le 3 mars 2021.

MILES et VOORHEES Erik, 2017, « “Bitcoin — The Libertarian Introduction” — Erik Voorhees », *Medium*, <https://medium.com/lux-initiative/bitcoin-the-libertarian-introduction-c616edd8496c>, 29 janvier 2017, consulté le 1 février 2023.

MILLER Hannah, 2022, « The Merge Was a Success. Crypto Still Has Problems », *Bloomberg.com*, 19 sept. 2022.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, 2019a, « RPPM - Plus-values sur biens meubles et taxe forfaitaire sur les objets précieux - Cession d'actifs numériques à titre occasionnel - Champ d'application », *Bulletin Officiel des Finances Publiques-Impôts*, 2 septembre 2019.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, 2019b, « BNC - Champ d'application - Activités et revenus imposables - Généralités - Exploitations lucratives et sources de profits - Professions ou activités dont la classification fiscale des revenus a donné lieu à des solutions administratives ou jurisprudentielles », *Bulletin Officiel des Finances Publiques-Impôts*, 2 septembre 2019.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, 2017, *Traitemet du Renseignement et Action contre les Circuits FINanciers clandestins.*, [https://www.economie.gouv.fr/files/TRACFIN\\_Rapport\\_Analyse\\_2017\\_2018\\_Web.pdf](https://www.economie.gouv.fr/files/TRACFIN_Rapport_Analyse_2017_2018_Web.pdf), 2018 2017, consulté le 29 janvier 2021.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, 2011, *Rapport d'activité 2011, Tracfin*, s.l.

MINSKY Hyman P., 1985, « Money and the Lender of Last Resort », *Levy Economics Institute of Bard College*, 1985, paper 31, archive/ march-april 1985, p. 11-18.

MIOTTI Luis et PLIHON Dominique, 2001, « Libéralisation financière, spéculation et crises bancaires », *La Documentation Française économie internationale*, 2001, n°85, p. 3-36.

MONAHAN Taylor (aka insomniasexx), 2016, « r / TheDAO Let me repeat that one more time : we are making NO recommendation on what you should do. The community has asked for a way to split via these proposals and we have done our best to help. What you do is 100 % your choice and your », [https://www.reddit.com/r/TheDAO/comments/4oifss/myetherwallet\\_dao\\_splits\\_information/](https://www.reddit.com/r/TheDAO/comments/4oifss/myetherwallet_dao_splits_information/), consulté le 8 décembre 2022.

MOREAU Gabriel, 2019, « Les licences et Logiciels libres », [https://ecoinfo.cnrs.fr/wp-content/uploads/2019/10/ANF2019\\_LicencesLibres\\_LaurentBourges-1.pdf](https://ecoinfo.cnrs.fr/wp-content/uploads/2019/10/ANF2019_LicencesLibres_LaurentBourges-1.pdf), consulté le 16 mai 2021.

MORRIS David Z., 2023, « CoinDesk Turns 10: 2016 - How The DAO Hack Changed Ethereum and Crypto », <https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/>, 9 mai 2023, consulté le 16 avril 2024.

MORRIS Steven, 2021, « Man offers Newport council £50m if it helps find bitcoins in landfill », *The Guardian*, <http://www.theguardian.com/uk-news/2021/jan/14/man-newport-council-50m-helps-find-bitcoins-landfill-james-howells>, 14 janvier 2021, consulté le 29 janvier 2021.

MÖSER Malte et BÖHME Rainer, 2015, « Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees » dans Michael Brenner, Nicolas Christin, Benjamin Johnson et Kurt Rohloff (dir.), *Financial Cryptography and Data Security*, Berlin, Heidelberg, Springer Berlin Heidelberg (coll. « Lecture Notes in Computer Science »), vol.8976, p. 19-33.

MOW Samson, 2018, « Bitcoin's White Paper Is Not a Bible – Stop Worshipping It », *CoinDesk*, <https://www.coindesk.com/markets/2018/11/01/bitcoins-white-paper-is-not-a-bible-stop-worshipping-it/>, 1 novembre 2018, consulté le 1 septembre 2022.

MULLIN Joe, 2013, « Winklevoss twins create fund to trade Bitcoins on stock market », <https://arstechnica.com/information-technology/2013/07/winklevoss-twins-create-fund-to-trade-bitcoins-on-stock-market/>, 7 février 2013, consulté le 10 septembre 2021.

MUNIESA F, 2017, « Le marché comme solution informatique : le cas du Arizona Stock Exchange », *Papiers de recherche du CSI*, n°008, juillet 2017, p. 21.

MUNIESA Fabian, MILLO Yuval et CALLON Michel, 2007, « An introduction to market devices », *Sociological Review*, 2007, vol. 55, SUPPL. 2, p. 1-12.

MURATOV Eugene et VOGELSTELLER Fabian, 2016, « The Robin Hood Team: The DAO's Assets May Return Without a HardFork », <https://Forklog.media/the-robin-hood-team-the-daos-assets-may-return-without-a-hardFork/>, 22 juin 2016, consulté le 29 mai 2019.

MUSIANI Francesca, MALLARD Alexandre et MÉADEL Cécile, 2018, « 7 Governing what wasn't meant to be governed » dans Campbell-Verduyn Malcolm, *Bitcoin and Beyond. Cryptocurrencies, Blockchains, and Global Governance*, Routledge, Abingdon, 2017, p. 24.

NAKAMOTO Satoshi, 2011, « Dernier mail de Nakamoto Gmail - Holding coins in an unspendable state for a rolling time window », <https://plan99.net/~mike/satoshi-emails/thread5.html>, consulté le 03 août 2020.

NAKAMOTO Satoshi, 2010a, « Satoshi Nakamoto last post on Bitcointalk : Added some DoS limits, removed safe mode (0.3.19) », <https://bitcointalk.org/index.php?topic=2228.msg29479#msg29479>, consulté le 10 juillet 2020.

NAKAMOTO Satoshi, 2010b, « BitDNS and Generalizing Bitcoin », <https://bitcointalk.org/index.php?topic=1790.msg28917#msg28917>, consulté le 31 août 2020.

NAKAMOTO Satoshi, 2010c, « [PATCH] increase block size limit », <https://bitcointalk.org/index.php?topic=1347.msg15139#msg15139>, consulté le 5 septembre 2024.

NAKAMOTO Satoshi, 2010d, « They want to delete the Wikipedia article », <https://bitcointalk.org/index.php?topic=342.msg4508#msg4508>, consulté le 20 août 2020.

NAKAMOTO Satoshi, 2010e, « Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG », <https://bitcointalk.org/index.php?topic=195.msg1617#msg1617>, consulté le 27 août 2020.

NAKAMOTO Satoshi, 2010f, « Re: Wikileaks contact info? | Satoshi Nakamoto Institute », <https://bitcointalk.org/index.php?topic=1735.msg26999#msg26999>, consulté le 3 août 2020.

Nakamoto Satoshi, 2010g, « Wikileaks has kicked the hornet's nest », <https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280>, consulté le 3 août 2020.

NAKAMOTO Satoshi, 2009a, « Bitcoin open source implementation of P2P currency (old chaumian mint) », <https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/2/>, 15 février 2009, consulté le 10 octobre 2024.

NAKAMOTO Satoshi, 2009b, « Bitcoin open source implementation of P2P currency », <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>, consulté le 25 février 2020.

NAKAMOTO Satoshi, 2009c, « Bitcoin v0.1 released », <https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html>, consulté le 12 octobre 2021.

NAKAMOTO Satoshi, 2008a, « Response of Satoshi Nakamoto to a question on the impossibility to find solution in cryptography to political problems, in Mailing list », <https://satoshi.nakamotoinstitute.org/emails/cryptography/4/>, consulté le 14 juin 2020.

NAKAMOTO Satoshi, 2008b, « Bitcoin P2P e-cash paper », <https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html>, consulté le 28 août 2020.

NAKAMOTO Satoshi, 2008c, « Bitcoin: A Peer-to-Peer Electronic Cash System », <https://bitcoin.org/bitcoin.pdf>, consulté le 20 septembre 2015.

NAKAMOTO Satoshi et HEARN Mike, 2009, « Gmail - Questions about BitCoin », <https://plan99.net/~mike/satoshi-emails/thread1.html>, 12 avril 2009, consulté le 13 septembre 2023.

NARAYANAN Arvind et CLARK Jeremy, 2017, « Bitcoin's academic pedigree », *Communications of the ACM*, 2017, vol. 60, n° 12, p. 36-45.

NEWBERY John et ROCHARD Pierre, « Jnewbery-cve-2018-17144-bug », <https://diyhpl.us/wiki/transcripts/noded-podcast/jnewbery-cve-2018-17144-bug/>, consulté le 6 février 2020.

O'BRIEN Will, 2014, « How 2014 Became the Year of Multisig », <https://www.coindesk.com/2014-became-year-multisig>, 29 décembre 2014, consulté le 4 août 2020.

OCONNELL Justin, 2016, « Bitcoin Enthusiast Al Gore to Star in “An Inconvenient Truth” Follow-Up », <https://www.cnn.com/bitcoin-enthusiast-al-gore-star-inconvenient-truth-follow/>, 11 décembre 2016, consulté le 10 septembre 2021.

O'LEARY Rachel-Rose, 2018, « Ethereum ASICs Are Here: What the New Miners Mean and What's Next », <https://www.coindesk.com/markets/2018/04/03/ethereum-asics-are-here-what-the-new-miners-mean-and-whats-next/>, 3 avril 2018, consulté le 15 juin 2023.

OPTECH Bitcoin, 2021, « Soft Fork activation », <https://bitcoinops.org/en/topics/soft-Fork-activation/>, 2021, consulté le 14 décembre 2021.

ORLÉAN A, 2003, « Réflexion sur les fondements institutionnels de l'objectivité marchande », *Cahiers d'économie Politique*, 2004/1, n° 44, p. 181-196.

ORLÉAN A., 2002, « La monnaie contre la marchandise », *L'Homme*, 2002, n° 2, p. 27-48.

ORLEAN A. & AGLIETTA M., 1982, *La violence de la monnaie*, Paris, Presses Universitaires de France.

ORLÉAN André, 2019, « La communauté bitcoin », *Esprit*, 2019, Juillet-Août, n° 7, p. 47.

ORLÉAN André, 1998, « La monnaie autoréférentielle: reflexion sur les évolution monétaire contemporaine » dans *La monnaie souveraine*, Paris, Éd Odile Jacob., p. 359-386.

ORLÉAN André, 1992, « La monnaie comme lien social. Étude de Philosophie de l'argent de Georg Simmel », *Genèses*, 1992, vol. 8, n° 1, p. 86-107.

ORLÉAN André, 1989, « Pour une approche cognitive des conventions économiques », *Revue économique*, 1989, vol. 40, n°2, L'économie des conventions (Mar., 1989), p. 241-272.

OSTROM Elinor, 2005, « Governing a Commons from a Citizen's Perspective », 2005, p. 1-9.

OSTROM Elinor, 1990, *Governing the Commons*, New York, Cambridge University Press, 1990.

OSTROM Elinor et BASURTO Xavier, 2013, « Façonner des outils d'analyse pour étudier le changement institutionnel », *Revue de la régulation*, 12 décembre 2013, n° 14.

OSUNTOKUN Olaoluwa, CAMARENA Justin, CORALLO Matt et FOLKSON Michael, 2019, « Lightning security panel », Breaking Bitcoin Conference 2019, Amsterdam, <https://www.youtube.com/watch?v=orWfkDWQzo>, consulté le 9 juin 2019.

OU Elaine, 2017, « Fiatsplaining Bitcoin », <https://elaineou.com/2017/12/16/fiatsplaining-bitcoin/>, 17 décembre 2017, consulté le 3 février 2021.

PARITY TECHNOLOGIES, 2019, « Transitioning Parity Ethereum to OpenEthereum DAO | Parity Technologies », <https://www.parity.io/blog/parity-ethereum-openethereum-dao/>, 16 décembre 2019, consulté le 6 avril 2022.

PARTZ Helen, 2020a, « China Didn't Ban Bitcoin Entirely, Says Beijing Arbitration Commission », <https://cointelegraph.com/news/china-didnt-ban-bitcoin-entirely-says-beijing-arbitration-commission>, 30 juillet 2020, consulté le 1 février 2021.

PARTZ Helen, 2020b, « City of Zermatt Switzerland Now Accepts Tax Payments in Bitcoin », <https://cointelegraph.com/news/city-of-zermatt-switzerland-now-accepts-tax-payments-in-bitcoin>, 29 janvier 2020, consulté le 4 mars 2021.

PASTINELLI Madeleine, 2011, « Pour en finir avec l'ethnographie du virtuel !: Des enjeux méthodologiques de l'enquête de terrain en ligne », *Anthropologie et Sociétés*, 2011, vol. 35, n° 1-2, p. 35.

PAYE Olivier, 2005, « La gouvernance : D'une notion polysémique à un concept politologique », *Études Internationales*, 2005, vol. 36, n° 1, p. 13.

PEERCOIN, « Peercoin Docs - Documentation of Peercoin Cryptocurrency », <https://www.peercoin.net/docs/proof-of-stake>, consulté le 24 mai 2023.

PERRY BARLOW John, 2000, *Déclaration d'indépendance du cyberespace in Olivier Blondeau, Libres enfants du savoir numérique*, Paris, Ed. de l'Eclat, p. 47-54.

PFISTER Christian, 2017, « Monetary Policy and Digital Currencies: Much Ado about Nothing? », Septembre 2017, Paris, Banque de France.

PHILH, 2021, « Et voici EIP-1559 ! », <https://www.ethereum-france.com/blog/et-voici-eip-1559-the-daily-gweifr/>, 30 juillet 2021, consulté le 29 juin 2023.

PLIHON Dominique, 2008, *La monnaie et ses mécanismes*, Paris, La découverte, (coll. « Repères »).

POLANYI Karl, 2011, *La subsistance de l'homme : La place de l'économie dans l'histoire et la société [trad B Chavance]*, Paris, Flammarion.

POLANYI Karl, 1944, *La grande transformation : aux origines politiques et économiques de notre temps*, Paris, Gallimard, rééd 2004.

POLROT Simon, 2017, « Comptes, transactions, gaz et limites de gaz par bloc sur Ethereum », <https://www.ethereum-france.com/comptes-transactions-gaz-et-limites-de-gaz-par-bloc-sur-ethereum/>, 28 juin 2017, consulté le 21 octobre 2020.

POLROT Simon, 2016a, « To Fork or not to Fork, telle est la question ! », [https://www.ethereum-france.com/to-Fork\\*-or-not-to-Fork-telle-est-la-question/](https://www.ethereum-france.com/to-Fork*-or-not-to-Fork-telle-est-la-question/), 27 juin 2016, consulté le 27 juin 2019.

POLROT Simon, 2016b, « Slock.it : la promesse des objets connectés sur la blockchain », <https://www.ethereum-france.com/blog/slock-it-la-promesse-des-objets-connectes-sur-la-blockchain/>, 4 avril 2016, consulté le 29 avril 2024.

POLROT Simon, 2016c, « The DAO mortem », <https://www.ethereum-france.com/blog/the-dao-post-mortem/>, consulté le 7 mai 2021.

PONSOT Jean-François, 2021, « Monnaies numériques, confiance et souveraineté », *Banque & Stratégie*, mars 2021, n° 400, p. 4.

POPPER Nathaniel, 2016a, « Paper Points Up Flaws in Venture Fund Based on Virtual Money », *The New York Times*, 27 mai 2016.

POPPER Nathaniel, 2016b, « A Venture Fund With Plenty of Virtual Capital, but No Capitalist », *The New York Times*, 22 mai 2016.

POPPER Nathaniel, 2014, « Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58 », *The New York Times*, 30 août 2014.

POULIOT Francis, 2018, « Catallaxy: the origins of Bitcoin and innovation », <https://medium.com/@francispouliot/catallaxy-the-origins-of-bitcoin-and-innovation-93dbc3190eac>, 5 septembre 2018, consulté le 28 novembre 2022.

PRESTONBYRNE, 2018, « Whether Ether is a security », <https://prestonbyrne.com/2018/04/23/on-ethereum-security/>, 23 avril 2018, consulté le 6 décembre 2019.

PROASSETZ, 2018, « Ethereum ice age », <https://medium.com/@proassetz/ethereum-ice-age-d6e2e35df339>, 29 septembre 2018, consulté le 16 juin 2023.

QTUM, 2020, « Historical Review: Catching One of Bitcoin's Major Vulnerabilities », <https://blog.qtum.org/historical-review-catching-one-of-bitcoins-major-vulnerabilities-3fb458663177>, 20 février 2020, consulté le 7 octobre 2021.

QUENTSON Andrew, 2016, « DAO Makes History, Raises \$130 Million, Breaking All Records », <https://cointelegraph.com/news/dao-makes-history-raises-130-million-breaking-all-records>, 17 mai 2016, consulté le 23 septembre 2019.

QUÉRÉ Louis, 1989, « Les boîtes noires de Bruno Latour ou le lien social dans la machine », *Réseaux. Communication - Technologie - Société*, 1989, vol. 7, n° 36, p. 95-117.

QURESHI Haseeb, 2019, « Public-Key Cryptography », <https://nakamoto.com/public-key-cryptography/>, 29 décembre 2019, consulté le 4 août 2020.

RANDALL WRAY L, 2010, « Alternative Approaches to Money », *Theoretical Inquiries in Law*, 2010, vol. 11, n° 1, p. 29-49.

RASKIN Max et YERMACK David, 2016, « Digital currencies, decentralized ledgers, and the future of central banking », *National Bureau of Economic Research*, 2016, p. 1-18.

RAUCHS Michel, 2016, « Cryptocurrencies meeting business ecosystems : the case of bitcoin », [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3095875](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3095875), 1er septembre 2016, consulté le 21 novembre 2017.

RAUCHS Michel, GLIDDEN Andrew, GORDON Brian, PIETERS Gina, RECANATINI Martino, ROSTAND François, VAGNEUR Kathryn et ZHANG Bryan, 2018, « Distributed Ledger Systems: A Conceptual Framework », *Cambridge Centre for Alternative Finance*, août 2018, p. 110.

RAYNAL Juliette, 2017, « Zoug, la bourgade suisse devenue capitale de la Crypto Valley », <https://www.usine-digitale.fr/article/zoug-la-bourgade-suisse-devenue-capitale-de-la-crypto-valley.N587898>, 18 septembre 2017, consulté le 10 octobre 2020.

REBERIOUX Antoine, 2003, « Governance d'entreprise et théorie de la firme. Quelle(s) alternative(s) à la valeur actionnariale ? », *Revue d'économie industrielle*, 2003, vol. 104, n° 1, p. 85-110.

REDMAN Jamie, 2021, « An In Depth Look at Bitcoin's First Chain Split: Satoshi Helps Reverse the Creation of 184 Billion BTC – Featured Bitcoin News », <https://news.bitcoin.com/an-in-depth-look-at-bitcoins-first-chain-split-satoshi-helps-reverse-the-creation-of-184-billion-btc/>, 15 août 2021, consulté le 15 novembre 2021.

REDMAN Jamie, 2019a, « XRP Sentiment Manipulated by Thousands of Bots, Analyst Claims », <https://www.coininsider.org/article/64246/xrp-sentiment-manipulated-thousands-bots-analyst-claims>, 18 mars 2019, consulté le 9 décembre 2021.

REDMAN Jamie, 2019b, « The “Wrapped Bitcoin” Project Has Now Officially Launched on Ethereum », <https://news.bitcoin.com/the-wrapped-bitcoin-project-has-officially-launched-on-ethereum/>, 31 janvier 2019, consulté le 12 mai 2023.

REITWIESSNER Christian, 2016, « Smart Contract Security », <https://blog.ethereum.org/2016/06/10/smарт-contract-security>, 10 juin 2016, consulté le 13 mai 2024.

RHODES R A W, 1996, « The New Governance : Governing without Government », *Political Studies*, 1996, 44: 652-66, p. 3-4.

RIZZO Pete, 2015, « Mastercoin Seeks Second Start With Omni Reboot », <https://www.coindesk.com/mastercoin-new-beginning-omni>, 21 janvier 2015, consulté le 6 août 2020.

ROBERT BOYER ET MARIO DEHOVE, 2001, « Théories de l'intégration européenne : entre gouvernance et gouvernement », *La lettre de la régulation* 38, 2001, n° 38, p. 1-4.

ROBINSON Dan, 2020, « Ethereum is a Dark Forest », *Medium*, <https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dff>, 28 août 2020, consulté le 26 juin 2023.

RODRIGUEZ Salvador, 2014, « Jamaican bobsled team boosts value of Dogecoin, currency based on meme », <https://www.latimes.com/business/technology/la-fi-tn-jamaican-bobsled-dogecoin-currency-meme-20140120-story.html>, 20 janvier 2014, consulté le 3 septembre 2020.

RODRIK Dani, 2002, « After neoliberalism, what? », *Alternatives to Neoliberalism Conference sponsored by the New Rules for Global Finance Coalition*, 23-24 mai 2002, 12 p.

ROLLAND Maël et SLIM Assen, 2017, « Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », *Économie et institutions*, 31 décembre 2017, n° 26.

ROSENFIELD Meni, 2012, « Overview of Colored Coins », <https://allquantor.at/blockchainbib/pdf/rosenfeld2012overview.pdf>, 4 décembre 2012, consulté le 7 novembre 2021.

ROSENFIELD Meni, BUTERIN Vitalik, ASSIA Yoni et HAKIM Lior, 2013, « Colored Coins - BitcoinX », [http://bitpaper.info/serve/AMIfv94V0F8kxt1ACXga9Tc1V0jm-u-Jf2evCmcHWsZJmYSBG6JB5qA5E3J5eNToOSfOFs7LKfC6X8Y\\_nUQR-C-qQC10aruJIVDG0ueU\\_qdZ4yG5l\\_VftKoBXs1xzpZHgCTx23tErQ1glKv0XrDC07gvNNINIM-QV1pWzdqhCM1MtubSUA7fyg.pdf](http://bitpaper.info/serve/AMIfv94V0F8kxt1ACXga9Tc1V0jm-u-Jf2evCmcHWsZJmYSBG6JB5qA5E3J5eNToOSfOFs7LKfC6X8Y_nUQR-C-qQC10aruJIVDG0ueU_qdZ4yG5l_VftKoBXs1xzpZHgCTx23tErQ1glKv0XrDC07gvNNINIM-QV1pWzdqhCM1MtubSUA7fyg.pdf), 26 novembre 2013, consulté le 8 septembre 2020.

ROUBINI Nouriel, 2018, « Blockchain's Broken Promises », <https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01>, 26 janvier 2018, consulté le 8 février 2021.

ROUSSEL Alexis, 2017a, « The Whitehat Withdrawal Contract distribution period is now reaching its end », <https://blog.bity.com/2017/04/03/the-whitehat-withdrawal-contract-distribution-period-is-now-reaching-its-end/>, 3 avril 2017, consulté le 27 mars 2019.

ROUSSEL Alexis, 2017b, « The Whitehat Withdrawal Contract has been extended for 2 months », <http://blog.bity.com/2017/01/30/the-whitehat-withdrawal-contract-has-been-extended-for-2-months/>, 30 janvier 2017, consulté le 27 mars 2019.

ROUSSEL Alexis, 2016a, « Whitehat Withdrawal Contract - Final Deposit is Available », <http://blog.bity.com/2016/09/06/whitehat-withdrawal-contract-final-deposit-is-available/>, 7 septembre 2016, consulté le 27 mars 2019.

ROUSSEL Alexis, 2016b, « Whitehat Withdrawal contract - Update and Next Steps », <http://blog.bity.com/2016/08/26/whitehat-withdrawal-contract-update-and-next-steps/>, 26 août 2016, consulté le 27 mars 2019.

ROUSSEL Alexis, 2016c, « Slock.it, ou quand l'économie de partage rencontre Ethereum », <http://blog.bity.com/2016/05/03/slock-it-ou-quand-leconomie-de-partage-rencontre-ethereum/>, 3 mai 2016, consulté le 27 mars 2019.

ROUVIÈRE Simon DE LA, 2016, « (2) Simon de la Rouviere sur X : "@VladZamfir wondered the same. Not going to be pretty. :( / X » , <https://x.com/simondlr/status/731510917301735424>, 14 mai 2016, consulté le 10 juillet 2024.

RUSSO Camila, 2020, *The Infinite Machine: How an Army of Crypto-Hackers Is Building the Next Internet with Ethereum*, New York, HarperCollins Publishers, 352 pages p.

RYKWALDER Eric, 2014, « The Math Behind Bitcoin », <https://www.coindesk.com/math-behind-bitcoin>, 19 octobre 2014, consulté le 4 août 2020.

SAAD Muhammad, SPAULDING Jeffrey, NJILLA Laurent, KAMHOUA Charles, SHETTY Sachin, NYANG DaeHun et MOHAISEN Aziz, 2019, « Exploring the Attack Surface of Blockchain: A Systematic Overview », *arXiv:1904.03487 [cs]*, 6 avril 2019.

SALLE Isabelle, 2013, « Ciblage de l'inflation, transparence et anticipations – une revue de la littérature récente: », *Revue d'économie politique*, 5 novembre 2013, Vol. 123, n° 5, p. 697-736.

SAPIR Jacques, 2019, « Institutions and institutionalism: what, why and how », Paris.

SATOSHI LABS, 2019, « 7 Years of Hardware Wallets: The Success Story of Czech Crypto Enthusiasts Creating a Brand New... », <https://blog.trezor.io/7-years-of-hardware-wallets-the-success-story-of-czech-crypto-enthusiasts-creating-a-brand-new-6648769d373a>, 12 juin 2019, consulté le 21 août 2020.

SCHNEIDER Nathan, 2015, « En cavale avec le voleur de banque Enric Duran », <https://www.vice.com/fr/article/ppnxg8/devenez-la-banque-que-vous-voulez-avoir-v9n5>, 28 mai 2015, consulté le 6 octobre 2020.

SCIALOM Laurence, 2003, « Vers une société sans cash? », *Anthropolis*, 2003, vol. 1, n°2, p. 24-35.

SECURITIES AND EXCHANGES COMMISSION The Commissions, 2017, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, s.l., Securities and Exchanges Commission.

SEDGWICK Kai, 2020a, « Bitcoin History: When DDoS Attacks Made BTC's Price Drop », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-25/>, 7 mars 2020, consulté le 21 juillet 2020.

SEDGWICK Kai, 2020b, « Bitcoin History Part 24: Celebrating the First Halving in 2012 », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-24/>, 25 février 2020, consulté le 21 juillet 2020.

SEDGWICK Kai, 2020c, « Bitcoin History Part 23: The First BTC Escrow », <https://news.bitcoin.com/bitcoin-history-part-23-the-first-btc-escrow/>, 8 janvier 2020, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019a, « Bitcoin History Part 22: The New Wealthy Elite », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-22-the-new-wealthy-elite/>, 19 décembre 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019b, « Bitcoin History Part 21: Miners Pour One out for Satoshi », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-21-miners-pour-one-out-for-satoshi/>, 10 décembre 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019c, « Bitcoin History Part 20: BTC Reaches \$1 », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-20-btc-reaches-1/>, 13 novembre 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019d, « Bitcoin History Part 19: Wikileaks and the Hornet's Nest », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-19-wikileaks-and-the-hornets-nest/>, 7 novembre 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019e, « Satoshi's Final Messages Leave Tantalizing Clues to His Disappearance », *Featured Bitcoin News*, <https://news.bitcoin.com/satoshis-final-messages-leave-tantalizing-clues-to-his-disappearance/>, 30 octobre 2019, consulté le 10 juillet 2020.

SEDGWICK Kai, 2019f, « Bitcoin History Part 18: The First Bitcoin Wallet », *Wallets Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-18-the-first-bitcoin-wallet/>, 6 octobre 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019g, « Bitcoin History Part 17: That Time Mt. Gox Destroyed 2,609 BTC », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-17-that-time-mt-gox-destroyed-2609-btc/>, 21 septembre 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019h, « Bitcoin History Part 16: The First Mt. Gox Hack », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-16-the-first-mt-gox-hack/>, 25 août 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019i, « Bitcoin History Part 15: Silk Road Is Born », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-15-silk-road-is-born/>, 18 août 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019j, « Bitcoin History Part 14: The 1,000 BTC Poker Game », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-14-the-1000-btc-poker-game/>, 9 août 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019k, « Bitcoin History Part 13: The First Mining Pool », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-13-the-first-mining-pool/>, 19 mai 2019, consulté le 21 juillet

2020.

SEDGWICK Kai, 2019l, « Bitcoin History Part 12: When No One Wanted Your BTC », *News Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-12-when-no-one-wanted-your-btc/>, 12 mai 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019m, « Bitcoin History Part 11: The First Major Loss of Coins », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-11-the-first-major-loss-of-coins/>, 29 avril 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019n, « Bitcoin History Part 10: The 184 Billion BTC Bug », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/>, 28 février 2019, consulté le 23 septembre 2019.

SEDGWICK Kai, 2019o, « Bitcoin History Part 9: Mt. Gox Is Born », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-9-mt-gox-is-born/>, 26 janvier 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2019p, « Bitcoin History Part 8: When 1,500 BTC Cost Less Than \$1 », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-8-when-1500-btc-cost-less-than-1/>, 12 janvier 2019, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018a, « Bitcoin History Part 7: The First Major Hack », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-7-the-first-major-hack/>, 31 décembre 2018, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018b, « Bitcoin History Part 6: The First Bitcoin Exchange », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-6-the-first-bitcoin-exchange/>, 25 décembre 2018, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018c, « Bitcoin History Part 5: A Wild Altcoin Appears », *Altcoins Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-5-a-wild-altcoin-appears/>, 19 décembre 2018, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018d, « Bitcoin History Part 4: Casascius Creates Physical Bitcoins », *Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-4-casascius-creates-physical-bitcoins/>, 12 décembre 2018, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018e, « Bitcoin History Part 3: Turning on the Faucet », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-3-turning-on-the-faucet/>, 8 décembre 2018, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018f, « Bitcoin History Part 2: The Bitcoin Symbol », *Featured Bitcoin News*, <https://news.bitcoin.com/bitcoin-history-part-2-the-bitcoin-symbol/>, 2 décembre 2018, consulté le 21 juillet 2020.

SEDGWICK Kai, 2018g, « Eight Historic Bitcoin Transactions », *Featured Bitcoin News*, <https://news.bitcoin.com/eight-historic-bitcoin-transactions/>, 27 novembre 2018, consulté le 21 juillet 2020.

SEIBT Sébastien, 2013, « La « banque » de paiement en ligne Liberty Reserve fermée pour blanchiment », *France24*, <https://www.france24.com/fr/20130529-liberty-reserve-monnaie-virtuelle-blanchiment-argent-cyber-criminalite-arrestation-arthur-budovsky-costa-rica-internet>, 29 mai 2013, consulté le 10 octobre 2022.

SELGIN George, 2014a, « Bitcoin: Problems and Prospects », 12 novembre 2014, Hillsdale University's 2014 Free Market Forum, Indianapolis, Indiana, 23-25 octobre 2014.

SELGIN George, 2014b, « Synthetic Commodity Money », *Journal of Financial Stability*, juillet 2014, vol. 17, p. 92-99.

SELGIN George, 2013, « Quasi-Commodity Money », *SSRN Electronic Journal*, 10 avril 2013.

SERGEENKOV Andrey, 2021, « China Crypto Bans: A Complete History », <https://www.coindesk.com/learn/china-crypto-bans-a-complete-history/>, 29 septembre 2021, consulté le 11 janvier 2024.

SERVET Jean Michel et DUFRÈNE Nicolas, 2021, « Le bitcoin devient un danger pour le système monétaire et financier et pour les citoyens », *Le Monde.fr*, 3 déc. 2021.

SERVET Jean Michel, THÉRET Bruno et YILDIRIM Zeynep, 2016, « Universalité du fait monétaire et pluralité des monnaies : de la confrontation coloniale à la rencontre des sciences sociales » dans *Théories Française de la monnaie*, Pierre Alary éd., Paris, Presses Universitaires de France, (coll. « « Hors collection » »), p. 1-43.

SERVET Jean-Michel, 2001, « Le troc primitif, un mythe fondateur d'une approche économiste de la monnaie », *Revue numismatique*, 2001, vol. 6, n° 157, p. 15-32.

SERVET Jean-Michel, COURBIS Bernard et FROMENT Éric, 1991, « Enrichir l'économie politique de la monnaie par l'histoire », *Revue économique*, 1991, vol. 42, n° 2, p. 315-338.

SHAW Aaron et HILL Benjamin M., 2014, « Laboratories of Oligarchy? How the Iron Law Extends to Peer Production: Laboratories of Oligarchy », *Journal of Communication*, avril 2014, vol. 64, n° 2, p. 215-238.

SHIN Laura, 2022, *The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze*, New York, PublicAffairs, 496 p.

SHINOBI, 2022, « Why Bitcoin's Ossification Will Eventually Be Necessary », *Bitcoin Magazine*, <https://bitcoinmagazine.com/culture/why-bitcoins-ossification-will-be-necessary>, 19 mai 2022, consulté le 16 mai 2023.

SIMMEL Georg, 2009, *Philosophie de l'argent*, trad. S. Cornille et P. Ivernel, 2<sup>ème</sup> éd., Paris, PUF, 662 p.

SIMONITE Tom, 2014, « The Man Who Really Built Bitcoin », *Technology Review*, <https://www.technologyreview.com/2014/08/15/12784/the-man-who-really-built-bitcoin/>, 15 août 2014, consulté le 18 mars 2024.

SINGER Andrew, 2021, « Crypto as a “public good” in the 22nd century », *Coin Telegraph* <https://cointelegraph.com/magazine/2021/10/22/crypto-public-good-22nd-century>, 22 octobre 2021, consulté le 23 juillet 2022.

SIRER Emin Gün, MARK Dino et ZAMFIR Vlad, 2016, « A Call for a Temporary Moratorium on “The DAO” », [https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWyS-dQ4lsBacR2dUgGTtV98C40/edit?usp=embed\\_facebook](https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWyS-dQ4lsBacR2dUgGTtV98C40/edit?usp=embed_facebook), 26 mai 2016, consulté le 10 mai 2024.

SITRUK Hervé, 2008, « Monnaie électronique, monnaie fiduciaire et monnaie scripturale. Quelles substitutions ? Quelles stratégies ? », *Revue d'économie financière*, 2008, n°91, La banque solidaire. Monnaie et moyens de paiement. Les systèmes bancaires européens., p. 37-51.

SLACKNATION, 2017, « 64.1% of presale Ether accounts never accessed before », *Medium*, <https://medium.com/@slacknation/64-1-of-presale-ether-accounts-never-accessed-before-280d381056ca>, 14 mai 2017, consulté le 8 octobre 2020.

SLOCK.IT, 2016, « Decentralizing the Emerging Sharing Economy », *Slock.it*, <https://blog.slock.it/slock-it-decentralizing-the-emerging-sharing-economy-cf19ce09b957>, 1 avril 2016, consulté le 17 mars 2022.

SLOCKIT GMBH et JENTZSCH Christoph, 2015, « Slock.it DAO demo at Devcon1: IoT + Blockchain », <https://www.youtube.com/watch?v=49wHQoJxYPo>, consulté le 20 juillet 2021.

SONG Jimmy, 2019, « A Gentle Introduction to Bitcoin Core Development », <https://bitcointechtalk.com/a-gentle-introduction-to-bitcoin-core-development-fdc95eaee6b8>, 11 janvier 2019, consulté le 17 octobre 2019.

SONG Jimmy, 2018a, « Lord Keynes Would Be Proud », *Medium*, <https://medium.com/@jimmysong/lord-keynes-would-be-proud-a225fec9cf6a>, 15 octobre 2018, consulté le 13 juin 2019.

SONG Jimmy, 2018b, « Crypto-Keynesian Lunacy », *Medium*, <https://medium.com/@jimmysong/crypto-keynesian-lunacy-16bb9193a58>, 18 juin 2018, consulté le 13 juin 2019.

SONG Jimmy, 2018c, « Bitcoin Core Bug CVE-2018-17144: An Analysis », <https://hackernoon.com/bitcoin-core-bug-cve-2018-17144-an-analysis-f80d9d373362>, 2018, consulté le 20 septembre 2019.

STAR Susan Leigh, 1999, « Ethnography of infrastructure », *American Behavioral Scientist*, 1999, vol. 43, p. 377-391.

STAY Ronald J, 1997, « Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann », *Georgia State University Law Review*, 1997, vol. 13, p. 25.

STEINER Philippe, 2007, « Karl Polanyi, Viviana Zelizer et la relation marchés-société », *Revue du MAUSS*, 2007, vol. 29, n° 1, p. 257.

STEWART Daniel, 2005, « Social Status in an Open-Source Community », *American Sociological Review*, 2005, vol. 70, n° 5, p. 823-842.

STRAW HAT Guido D., 2019, « Looking back on exploiting CVE-2018-17144 », <https://bitcoindev.network/looking-back-on-exploiting-cve-2018-17144/>, 5 mars 2019, consulté le 17 mars 2021.

SWANSON Tim, 2021, « Bitcoin and other PoW coins are an ESG nightmare », <https://www.ofnumbers.com/2021/02/14/bitcoin-and-other-PoW-coins-are-an-esg-nightmare/>, 14 février 2021, consulté le 4 mars 2021.

SWISSINFO.CH, 2016, « Zug first to accept bitcoin for government services », [https://www.swissinfo.ch/eng/crypto-valley\\_zug-first-to-accept-bitcoin-for-government-services/42143908](https://www.swissinfo.ch/eng/crypto-valley_zug-first-to-accept-bitcoin-for-government-services/42143908), 10 mai 2016, consulté le 4 mars 2021.

SZABO Nick, 2008a, « Unenumerated: Bit gold », <https://unenumerated.blogspot.com/2005/12/bit-gold.html>, 27 décembre 2008, consulté le 6 mai 2020.

SZABO Nick, 2008b, « Unenumerated: Wet code and dry », <https://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html>, 24 août 2008, consulté le 25 octobre 2022.

SZABO Nick, 2005, « Unenumerated: Bit gold », <https://web.archive.org/web/20060329122942/http://unenumerated.blogspot.com/2005/12/bit-gold.html>, 29 décembre 2005, consulté le 6 mai 2020.

SZABO Nick, 1996, « Nick Szabo -- Smart contracts: Building Blocks for Digital Markets », [https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smarts\\_contracts\\_2.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smarts_contracts_2.html), 1996, consulté le 13 juin 2023.

SZILÀGYI Péter, 2016, « DAO Wars: Your voice on the soft-Fork dilemma - Ethereum Blog », <http://archive.fo/7UUrY>, 24 juin 2016, consulté le 20 mai 2019.

TAAKI Amir, 2011, « bitcoin/bips-0001 », <https://github.com/bitcoin/bips/blob/274fa400d630ba757bec0c03b35ebe2345197108/bip-0001.mediawiki>, consulté le 7 avril 2017.

TANZARIAN Armand, 2014, « Ethereum Raises 3,700 BTC in First 12 Hours of Ether Presale », <https://cointelegraph.com/news/ethereum-raises-3700-btc-in-first-12-hours-of-ether-presale>, 23 juillet 2014, consulté le 7 octobre 2020.

TASCA Paolo et LIU Shaowen, 2018, « The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships », *SSRN Electronic Journal*, 2018, vol. 19, n° 2, p. 94-126.

TERUZZI David, 2016a, « DAO: Contractors et Curators », *blogchain café*, <http://blogchaincafe.com/dao-contractors-et-curators>, 27 avril 2016, consulté le 24 mai 2019.

TERUZZI David, 2016b, « Les consensus: Proof of work vs Proof of stake », *blogchain café*, <https://blogchaincafe.com/les-consensus-proof-of-work-vs-proof-of-stake>, 14 mars 2016, consulté le 13 juillet 2020.

THE INTERNAL REVENUE SERVICE (IRS), 2014, « Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies », 2014, p. 1-6.

THÉRET Bruno, 2012, « Du keynésianisme au libertarianisme.La place de la monnaie dans les transformations du savoir économique autorisé », *Revue de la régulation*, 2012, vol. 10.

THÉRET Bruno, 2009, « Monnaie et dettes de vie », *L'Homme*, 30 avril 2009, n° 190, n° 2, p. 153-179.

THÉRET Bruno, 2008, « Les trois états de la monnaie », *Revue économique*, 2008, vol. 59, n° 4, p.813-840.

THÉVENOT Laurent, 1986, « Les Investissement de forme », *Presses Universitaires de France*, 1986 p. 21-71.

THEYMOS, 2018, « The duplicate input vulnerability shouldn't be forgotten », <https://bitcointalk.org/index.php?topic=5035144.0>, 22 septembre 2018, consulté le 31 mai 2021.

TIMÓN Jorge, 2015, « BIP-0099 : Motivation and deployment of consensus rule changes ([soft/hard]Forks) », <https://github.com/bitcoin/bips>, 20 juin 2015, consulté le 11 décembre 2019.

TIROLE Jean, 2017, « There are many reasons to be cautious about bitcoin », <https://www.ft.com/content/1c034898-d50f-11e7-a303-9060cb1e5f44>, 30 novembre 2017, consulté le 14 mai 2020.

TORPEY Kyle, 2016, « The Checks and Balances of Bitcoin Governance », *Bitcoin Magazine*, <https://bitcoinmagazine.com/technical/the-checks-and-balances-of-bitcoin-governance-1454695089>, 5 février 2016, consulté le 8 février 2022.

TROMBLY Maria, 2001, « CyberCash files for bankruptcy, has new deal with Network 1 », <https://www.computerworld.com/article/2591382/cybercash-files-for-bankruptcy--has-new-deal-with-network-1.html>, 6 mars 2001, consulté le 20 août 2020.

TROMPETTE Pascale et VINCK Dominique, 2009, « Retour sur la notion d'objet-frontière », *Revue d'anthropologie des connaissances*, 2009, vol. 3, 1, n° 1, p. 5-27.

TUAL Stephan, 2016a, « The DAO Creation is now Live », *Slock.it Blog*, <https://archive.is/wOjUZ>, 30 avril 2016, consulté le 3 mai 2024.

TUAL Stephan, 2016b, « Daohub.org gets a facelift, full scope of The DAO is revealed », *Medium*, <https://medium.com/ursium-blog/daohub-org-gets-a-facelift-full-scope-of-the-dao-is-revealed-4d4c43eaf7b>, 21 avril 2016, consulté le 29 avril 2024.

TUAL Stephan, 2016c, « A Primer to Decentralized Autonomous Organizations (DAOs) », <https://blog.slock.it/a-primer-to-the-decentralized-autonomous-organization-dao-69fb125bd3cd>, 3 mars 2016, consulté le 27 mars 2019.

TUAL Stephan, 2016d, « Vitalik Buterin, Gavin Wood, Alex van De Sande, Vlad Zamfir announced amongst exceptional DAO Curators », *Medium*, 25 avril 2016, <https://medium.com/ursium-blog/vitalik-buterin-gavin-wood-alex-van-de-sande-vlad-zamfir-announced-amongst-stellar-dao-curators-44be4d12dd6e>, consulté le 20 juin 2016.

TUAL Stephan, 2016e, « Announcing DAO.LINK, the bridge between blockchain and brick-and-mortar companies », *Slock.it Blog*, <https://blog.slock.it/announcing-dao-link-the-bridge-between-blockchain-and-brick-and-mortar-companies-9510ba04d236#.fg2c41d3k>, consulté le 20 juin 2016.

TUAL Stephan, 2016f, « No DAO funds at risk following the Ethereum smart contract ‘recursive call’ bug discovery », *Slock.it Blog*, <https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b>, consulté le 20 juin 2016.

TUTIN Christian, 2009, *Une histoire des théories monétaires par les textes*, Flammarion., Paris, Champs classiques, 508 p.

VAN DE SANDE Alex, 2016a, « (2) Alex Van de Sande (avsa.eth) sur X : « @SlackCryptoAlex @lambdamat because it's not official. This is a collective action by individuals not representing any of their employers » », *X*, <https://x.com/avsa/status/745370293502251009>, 21 juin 2016, consulté le 11 juillet 2024.

VAN DE SANDE Alex, 2016b, « (1) Alex Van de Sande (avsa.eth) sur X : « DAO IS BEING SECURELY DRAINED. DO NOT PANIC. », *X*, <https://x.com/avsa/status/745313647514226688>, 21 juin 2016, consulté le 11 juillet 2024.

VAN WIRDUM Aaron, 2018, « The Genesis Files: How David Chaum’s eCash Spawned a Cypherpunk Dream », *Bitcoin Magazine*, <https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream>, 24 avril 2018, consulté le 2 juillet 2020.

VAROUFAKIS Yanis, 2020, « Why Bitcoin is not a socialist's ally – Reply to Ben Arc – Yanis Varoufakis », <https://www.yanisvaroufakis.eu/2020/07/27/why-bitcoin-is-the-not-socialists-alley-reply-to-ben-arc/>, 27 juillet 2020, consulté le 8 février 2021.

VAROUFAKIS Yanis, 2013, « Bitcoin and the dangerous fantasy of 'apolitical' money », <https://www.yanisvaroufakis.eu/2013/04/22/bitcoin-and-the-dangerous-fantasy-of-apolitical-money/>, 22 avril 2013, consulté le 12 mai 2020.

VAUPLANE Hubert DE, 2018, « Bitcoin : Fantasme-ou-croyance », *Revue Banque*, janvier 2018, n° 815-816, p. 2.

VELDE François R., 2013, « Bitcoin a primer », *The Federal Bank of Chicago*, décembre 2013, n° 317, p. 1-4.

VERGNE Jean Philippe et SWAIN Gautam, 2017, « Categorical Anarchy in the U.K. The British Media's Classification of Bitcoin and the Limits of Categorization », *Research in the Sociology of Organisation*, 2017, vol. 51, p. 187-222.

VESSENES Peter, 2016a, « Deconstructing the DAO Attack : A Brief Code Tour Some Background And Where To Look », <https://vessenes.com/deconstructing-thedao-attack-a-brief-code-tour/>, 18 juin 2016, consulté le 12 octobre 2019.

VESSENES Peter, 2016b, « More Ethereum Attacks: Race-To-Empty is the Real Deal », <https://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/>, 9 juin 2016, consulté le 27 mars 2019.

VOELL Zack, 2020, « Ethereum Classic Attacker Successfully Double-Spends \$1.68M in Second Attack: Report », *Coin Desk*, <https://www.coindesk.com/markets/2020/08/07/ethereum-classic-attacker-successfully-double-spends-168m-in-second-attack-report/>, 7 août 2020, consulté le 4 octobre 2022.

VON MISES Ludwig, 1912, *The theory of money and credit*, New Haven, Yale University Press, 1953, Auburn, Alabama, Ludwig von Mises Institute, 505 p.

VOORHEES Erik, 2013, « SatoshiDice Sold for \$12.4 Million », *Bitcoin Magazine*, <https://bitcoinmagazine.com/articles/satoshidice-sold-12-4-million>, 28 juillet 2013, consulté le 28 juillet 2020.

WALCH Angela, 2019, « Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems », 30 janvier 2019, p. 36.

WALCH Angela, 2017a, « The Path of the Blockchain Lexicon (and the Law) », *36 Rev. Banking & Fin. L.*, 2017, vol. 191, n° 2016, p. 1-13.

WALCH Angela, 2017b, « Open Source Operational Risk : Should Public Blockchains Serve as Financial Market Infrastructures ? » dans David Lee Kuo Chuen & Robert H. DengElsevier (dir.), *Handbook of Digital Banking & Internet Finance*, s.l., vol.2, p. 1-23.

WALKER, GREG, 2017, « Coinbase Transaction », <https://learnmeabitcoin.com/technical/coinbase-transaction>, 10 mars 2017, consulté le 12 janvier 2023.

WATERS Richard, 2016, « Automated company raises equivalent of \$120m in digital currency », <https://www.ft.com/content/600e137a-1ba6-11e6-b286-cddde55ca122>, 16 mai 2016, consulté le 23 septembre 2019.

WEBER Beat, 2014a, « Bitcoin and the legitimacy crisis of money », *Cambridge Journal of Economics*, décembre 2014, vol. 40, n° 1, p. 1-25.

WEBER Beat, 2014b, « Can Bitcoin compete with money? », *Journal of Peer Production*, n° 4 (2014), <http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoincompete-with-money/>, consulté le 22 juin 2020.

WEBER Florence et ZELIZER Viviana A., 2006, « Viviana zelizer, « l'argent social » », *Genèses*, 2006, n° 65, p. 126-137.

WEINSTEIN Olivier, 2013, « Comment comprendre les « communs » : Elinor Ostrom, la propriété et la nouvelle économie institutionnelle », *Revue de la régulation*, 12 décembre 2013, n° 14.

WHALEPANDA, 2016, « Ethereum: Chain of liars & thieves », Medium, <https://medium.com/@WhalePanda/ethereum-chain-of-liars-thieves-b04aaa0762cb>, 16 août 2016, consulté le 4 février 2020.

WHITE Lawrence H., 2020, « Has Bitcoin Succeeded? », *Cato Institute Blog*, <https://www.cato.org/blog/has-bitcoin-succeeded>, 28 décembre 2020, consulté le 19 février 2021.

WHITE Lawrence H., 2018, « How a Bitcoin System is Like and Unlike a Gold Standard », <https://fee.org/articles/how-a-bitcoin-system-is-like-and-unlike-a-gold-standard/>, 12 janvier 2018, consulté le 4 septembre 2023.

WHITERABBIT1111, 2022, « The origin digital antiquities market (NFTs) », <https://whiterabbit1111.medium.com/the-origin-digital-antiquities-market-nfts-1ea9b69c03f9>, 1 juin 2022, consulté le 23 mai 2023.

WILCKE Jeffrey, 2016, « To Fork or not to Fork », <https://blog.ethereum.org/2016/07/15/to-Fork-or-not-to-Fork/>, 15 juillet 2016, consulté le 27 mars 2019.

WILLETT JR, 2012, « 2ndBitcoinWhitepaper vs 0.5 20120106 », [https://drive.google.com/file/d/18iRKDmZy44YDd3jyEtafouT1PA7dEi5e/view?usp=sharing&usp=embed\\_facebook](https://drive.google.com/file/d/18iRKDmZy44YDd3jyEtafouT1PA7dEi5e/view?usp=sharing&usp=embed_facebook), 6 janvier 2012, consulté le 31 mai 2023.

WILLIAMS Mandy, 2022, « Ethereum's History: From Whitepaper to HardForks and the ETH Merge », <https://cryptopotato.com/ethereums-history-from-whitepaper-to-hardForks-and-the-eth-merge/>, 25 décembre 2022, consulté le 16 juin 2023.

WIRDUM Aaron van, 2019, « Stratum V2 Could Overhaul Pooled Bitcoin Mining », *Bitcoin Magazine*, <https://bitcoinmagazine.com/articles/with-stratum-v2-braiins-plans-big-overhaul-in-pooled-bitcoin-mining>, 5 août 2019, consulté le 19 mars 2020.

WIRDUM Aaron van, 2018, « What Is Gitian Building? How Bitcoin's Security Processes Became a Model for the Open Source Community », *Bitcoin Magazine*, <https://bitcoinmagazine.com/technical/what-is-gitian-building-how-bitcoin-s-security-processes-became-a-model-for-the-open-source-community-1461862937>, 28 avril 2018, consulté le 1 octobre 2021.

WIRDUM Aaron van, 2017, « How Bitcoin Extension Blocks Are Backward Compatible — and How They're Not », *Bitcoin Magazine*, <https://bitcoinmagazine.com/technical/how-extension-blocks-are-backward-compatible-and-how-theyre-not>, 20 avril 2017, consulté le 25 novembre 2021.

WIRDUM Aaron van, 2016, « Rejecting Today's Hard Fork, the Ethereum Classic Project Continues on the Original Chain: Here's Why », *Bitcoin Magazine*, <https://bitcoinmagazine.com/culture/rejecting>

today-s-hard-Fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808, 20 juillet 2016, consulté le 6 août 2024.

WIRDUM Aaron van, 2014, « Why Bitcoin Really Does Represent the Democratization of Money », *Bitcoin Magazine*, <https://bitcoinmagazine.com/culture/bitcoin-really-represent-democratization-money-1395137137>, 18 mars 2014, consulté le 26 juillet 2022.

WOOD Gavin, 2016, « Why I've Resigned as a Curator of the DAO », *Medium*, <https://medium.com/@gavofyork/why-i've-resigned-as-a-curator-of-the-dao-238528fbd447#.ikzzqv33z>, 13 mai 2016, consulté le 15 mai 2019.

WOOD Gavin, 2014a, « Gav's Ethereum DEX Update II », *Blog Ethereum*, <https://blog.ethereum.org/2014/11/01/gavs-ethereum-d%ce%bev-update-ii/>, 1 novembre 2014, consulté le 11 octobre 2020.

WOOD Gavin, 2014b, « “Yellow paper” : Ethereum: A Secure Decentralised Generalised Transaction Ledger (Version 2020-09-05) », 2014, p. 39.

WOODFORD Michael, 2000, « Monetary Policy in a World Without Money », *International Finance*, 2000, vol. 3, June, p. 229-260.

WRAY L. Randall, 2004, « The Credit Money and State Money Approaches », *SSRN Electronic Journal*, avril 2004.

YERMACK David, 2013, « Is bitcoin a real currency? An economic appraisal », *National Bureau of Economic Research*, 2013, p. 1-22.

YOUNG Joseph, 2017, « Vitalik Buterin: Early Versions of Ethereum Were Supposed to Launch on Bitcoin », *Coin Journal*, <https://coinjournal.net/news/vitalik-buterin-early-versions-ethereum-supposed-launch-bitcoin/>, 14 novembre 2017, consulté le 7 octobre 2020.

ZAMFIR Vlad, 2019, « Against Szabo's Law, For A New Crypto Legal System », *Medium*, <https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827>, 26 janvier 2019, consulté le 20 mai 2019.

ZAMFIR Vlad, 2017, « Against on-chain governance », *Medium*, [https://medium.com/@Vlad\\_Zamfir/against-on-chain-governance-a4ceacd040ca](https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca), 3 décembre 2017, consulté le 29 mars 2022.

ZAMFIR Vlad, 2016, « (2) Vlad Zamfir sur X : « @simondlr would the community hard Fork ethereum if there was a critical bug in the DAO? :p », X, <https://x.com/VladZamfir/status/731510468695756800>, 14 mai 2016, consulté le 10 juillet 2024.

ZELIZER Viviana, 2005, « Argent, circuits, relations intimes », *Enfances, Familles, Générations*, 2005, n° 2.

ZELIZER Viviana A., 2000, « The Purchase of Intimacy », *Law and Social Inquiry*, juillet 2000, vol. 25, n° 3, p. 817-848.

ZELIZER Viviana A., 1999, « Chapitre 5. Official standardisation vs social differentiation in american's use of money » dans *Introduction- Nation-states and money, The past the present and the future of national currencies* (Gilbert, Emily & Helleiner, Eric), Routledge., London; New York, p. 82-96.

ZELIZER Viviana A., 2005, *La signification sociale de l'argent*, traduit de l'américain par Christian Cler, Seuil., Paris, 348 p.

ZELIZER Viviana A ., 1989, « The Social Meaning of Money : “Special Monies” », *The American Journal of Sociology*, 1989, vol. 95, n° 2, p. 342-377.

ZHAO Gloria, 2020, « Map of the Bitcoin Network. A beginner-friendly “map” to help you... », *Medium*, <https://medium.com/@gloriazhao/map-of-the-bitcoin-network-c6f2619a76f3>, 13 juillet 2020, consulté le 5 janvier 2021.

ZHAO Xiangfu, CHEN Zhongyu, CHEN Xin, WANG Yanxia et TANG Changbing, 2017, « The DAO attack paradoxes in propositional logic », Hangzhou, IEEE.

ZOLESIO Emmanuelle, 2011, « Anonymiser les enquêtés », *Revue pluridisciplinaire de sciences humaines et sociales*, 2011, (coll. « Interrogation? »), p. 174-183.

« Griff Green and the DAO / Layer Zero, 2021, <https://www.youtube.com/watch?v=cVC9SbTmfSg>, consulté le 25 avril 2024.

« Le point de la Banque de France sur le bitcoin et autres crypto-actifs », 2018, <https://publications.banque-france.fr/lemergence-du-bitcoin-et-autres-crypto-actifs-enjeux-risques-et-perspectives>, consulté le 13 mai 2020.

« Bitcoin ‘Ought to Be Outlawed,’ Nobel Prize Winner Stiglitz Says - Bloomberg », 29 novembre 2017, <https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd>, consulté le 14 mai 2020.

« THE FILTER: “Griff Green & Slock.it” », 12 mai 2016, <https://www.youtube.com/watch?v=J2MIjN3gmhg>, consulté le 26 avril 2024.

« Milton Friedman, Land value tax and internet currencies », 1999, [https://www.youtube.com/watch?v=j2mdYX1nF\\_Y](https://www.youtube.com/watch?v=j2mdYX1nF_Y), consulté le 26 mai 2020

Ecole doctorale de l'EHESS

Centre d'Étude des Mouvements Sociaux (CEMS)

Discipline : Économie et Sciences sociales

**ROLLAND MAËL**

**LIVRET 2 : GLOSSAIRE & ANNEXES**

## GLOSSAIRE : CRYPTOMONNAIE ET PROTOCOLE DE REGISTRE DISTRIBUÉ

Les termes explicités dans le glossaire se trouvent présentés en italique, suivis d'un astérisque (\*) et explicités brièvement pour leur première occurrence dans le manuscrit. Après, ils ne seront plus suivis que d'un astérisque (\*). Sources principales : Rauchs et al, 2018 ; Bano et al, 2017 ; Seibold et Samman, 2016 ; adaptations et compléments de l'auteur.

**[Français | Anglais : définition]** : les termes en français sont accompagnés de leurs équivalents en anglais, qui prédominent dans le domaine étudié, imposant certains concepts et notions sous leur forme anglaise comme points de référence et de connaissance commune. Ce sont ces termes que nous utiliserons par la suite (par exemple, *Fork*\*, *smart contract*).

### Actif digital | Digital Asset :

L'appellation « actif digital\* » est le terme le plus englobant, ne se limitant pas aux technologies de registre\* distribué. Elle inclut également toutes les formes d'actifs et monnaies sous forme numérique, comme les points de fidélité, les accessoires et skin dans un jeu, etc., qui sont aussi des actifs de ce type. Voir encadré Chap.II.3.

### Administrateur | Administrator :

Parmi les « Core Développeurs\* », correspond à l'ensemble des acteurs disposant de droits privilégiés au sein du répertoire de dépôt du code source du logiciel référent, hébergé sur une *forge logicielle*\*. Suivant les niveaux de priviléges, les administrateurs peuvent ajouter, supprimer et modifier le code source.

### Algorithmme de consensus | Consensus Algorithm :

Correspond à l'ensemble de règles et processus utilisés par les participants afin de vérifier, traiter et parvenir à un accord sur un enregistrement canonique\*, gage du maintien dynamique de la cohérence\* des données endogènes\*. Il en existe différentes familles - Preuve de travail\* (PoW\*), Preuve d'enjeu\* (PoS), Preuve d'enjeu déléguée (DPoS), etc. Ce terme renvoie d'abord à l'algorithme utilisé au sein de la famille *PoW*\* pour valider un nouvel enregistrement candidat\* (Sha 256, Scrypt, etc.).

### Altcoin | Altcoin :

La dénomination indigène Altcoin regroupe et qualifie péjorativement toutes les cryptomonnaies\*, actifs numériques et monnaies digitales\*, à l'exception du Bitcoin, pris comme idéal-type. Certains termes utilisés par des figures communautaires dites Maximalistes\* sont encore plus péjoratifs (scamcoin ; shitcoin, etc...) et mettent en évidence les différences et les critiques philosophiques et pratiques qui structurent ces communautés.

### Archivage partagé | Shared recordkeeping :

Désigne la capacité du système à permettre à plusieurs parties de créer, entretenir et mettre à jour collectivement un ensemble d'enregistrements partagés.

### Arbre de Merkle (ou de Hachage) | Merkle tree (or Hash Tree) :

Correspond à une méthode cryptographique permettant de structurer des données d'un volume souvent important, via des *empreintes numériques*\*. Elle permet d'accéder à un ensemble de données et d'en vérifier l'intégrité, réduites à des *Hash*\* sans avoir à les posséder elles-mêmes dans leur totalité. Un arbre de hachage est constitué par un ensemble d'empreintes numériques interdépendantes où les feuilles sont le *hash*\* de chacun des blocs de données initiales, et qui, concaténés deux à deux, permettent de calculer un *hash*\* parent. Ces *hash*\* parents sont eux-mêmes concaténés deux à deux jusqu'à l'obtention d'un *hash*\* unique qui correspond au *hash*-sommel ou racine (« *Merkle root* »). Ce dernier est donc une empreinte liée cryptographiquement à toutes les empreintes des données initiales. Dans le cas d'une cryptomonnaie\*, cette racine, intégrant la totalité des *hash*\* des transactions\* contenues dans un *enregistrement*\*, se trouvera dans l'*en-tête du bloc*\*. Voir Annexes n°V.4.

### Au sein du protocole | On Chain :

Interactions, transactions\*, processus qui se produisent au sein des frontières formelles du protocole de registre\* distribué et qui se retrouvent représentées dans la couche de données du système.

### Authentification cryptographique | Cryptographic authentication :

Processus permettant de prouver l'identité des contreparties, l'existence et la possession d'actifs digitaux *via* des couples de clefs publiques et

privées (voir aussi *signature cryptographique*). Voir Annexes n°V.1 et V.2.

#### **Chaîne de blocs | Blockchain :**

L'usage du terme Blockchain est une synecdoque particularisante réduisant le tout à une de ses parties, en l'espèce à la structure de données. Ce concept, popularisé par des slogans comme « Forget Bitcoin, embrace Blockchain » émanant d'acteurs de la finance traditionnelle (en l'espèce Blythe Master de JP Morgan), reste discutable, car il invisibilise l'essentiel, à savoir le protocole qui le soutient et le rôle incitatif du monnayage et de l'unité de compte native émise dans la production d'un consensus. D'ailleurs, certains protocoles de registre\* distribué reposent sur des familles de structure de données différente, très éloignée de cette structure en enregistrements\* ou Blocs (les DAG pour « Directed Acyclic Graph », par exemple).

#### **Cible de difficulté | Difficulty target :**

Dans un consensus basé sur la *preuve de travail*\*, il s'agit d'un seuil à atteindre pour que l'*empreinte numérique* de l'*en-tête d'un enregistrement candidat*\* soit considérée comme valide (être inférieur ou égal). Cette cible de difficulté est programmée pour augmenter ou diminuer afin de maintenir un *temps d'enregistrement*\*

#### **Code Source Ouvert | Open Source Code :**

Le code source de l'implémentation logicielle est accessible au public et ouvre, suivant les droits accordés, à des modifications et à des copies, contrairement au code propriétaire, non accessible au public et couvert par des droits de propriété intellectuelle.

#### **Cohérence | Consistency :**

Propriété recherchée par tout système informatique de calcul distribué permettant que tous les nœuds\* du système accèdent exactement aux mêmes *données endogènes*\*. Aucune cryptomonnaie n'est cohérente à un instant T et cette propriété renvoie à la probabilité (forte ou faible) que le système parvienne à un consensus sur une valeur proposée. C'est l'*algorithme de consensus*\* qui lève à court terme l'ambiguïté, forçant l'ensemble des nœuds\* du réseau\* à converger sur une histoire commune qu'ils dupliquent et sur laquelle ils continuent à enregistrer les changements d'état.

#### **No Coiners vs Coiners | No Coiners vs Coiners :**

Termes indigènes servant à caractériser les acteurs relativement à leurs possessions ou non de CM et crypto-actifs\*. Le terme No Coiner fut premier : il sert à qualifier péjorativement les personnes ne

possédant pas de Bitcoin ou d'Altcoin\* et qui, dans le même temps, expriment scepticisme et critique à leur encontre. À l'opposé et en symétrie, le terme « Coiners\* » ou « crypto bro » est venu qualifier ceux qui possèdent des CM, les défendent à tout prix.

#### **Confirmation | Confirmation :**

Correspond au nombre d'enregistrements successifs « minés » au-dessus du bloc d'une transaction\* considérée. Ce nombre indique également combien d'enregistrements doivent être inversés ou écrasés pour supprimer une transaction\* du registre. La finalité d'une transaction\* renvoie à un nombre de confirmations considéré comme suffisant pour s'assurer d'un règlement irréversible. Sur Bitcoin, c'est généralement 6 confirmations qui sont attendues aujourd'hui.

#### **Contrat intelligent | Smart-contract (SC) :**

Voir script à exécution programmatique.

#### **Consensus multi-parties | Multi-party Consensus :**

Désigne la capacité d'un système de protocole de registre\* distribué à arriver à un accord entre différentes parties prenantes sur un ensemble partagé d'enregistrements faisant autorité et ce, en l'absence d'une autorité centrale.

#### **Cryptographie (ou chiffrement) | Cryptography :**

Correspond à une discipline qui s'intéresse à un ensemble de techniques et d'algorithmes permettant de chiffrer/déchiffrer des informations. Loin de ne faire que « cacher », les outils cryptographiques permettent, par chiffrement, la certification et l'authentification de données (signature par clef privée, déchiffrement/vérification par clef publique), comme des voies de structuration des données (les *fonctions de hash*\*, *arbre de Merkle*\*).

#### **Crypto-actifs | Crypto Assets :**

Les crypto-actifs\* sont des objets numériques dont la matérialité, bien qu'inscrite dans un protocole de registre\* distribué, repose sur un ou plusieurs centre(s) établi(s), reconnu(s) et disposant de droits exorbitants. Comme tout actif financier, ces formes suivent une logique contractuelle de signature et, en cela, se rapprochent des titres financiers. Voir encadré Chap.II.3.

#### **Cryptomonnaie (CM) | Cryptocurrency :**

Les CM recouvrent les UCN\* émises et administrées par des protocoles de registre\* distribué publics et s'apparentent à une nouvelle catégorie de monnaie, suivant leur gouvernance

singulière qui les voit reposer ni sur la logique de signature propre à la finance, ni sur la logique de sceau propre aux monnaies nationales. Bien que collective, cette logique de co-monnaage distribué est fondée sur un consensus entre l'ensemble des participants d'où une transparence, une sécurité et une intégrité du système qui ne reposent pas sur une autorité centrale, mais sont polycentriques. Voir encadré Chap.II.3.

#### Débit | Throughput :

Le débit représente le taux maximum auquel un protocole de registre\* distribué peut traiter des transactions\*, généralement mesuré en transactions\* par seconde (TPS). Il dépend de divers facteurs, tels que le type d'algorithme de consensus\* ou la taille des blocs de données. Un débit élevé est crucial pour la scalabilité et la performance des systèmes de registre\* distribué.

#### Développeurs | Developers :

Correspond à l'ensemble des acteurs qui, suivant leurs compétences spécifiques, peuvent écrire et relire les codes informatiques qui sous-tendent les éléments technologiques constitutifs des systèmes de protocoles de registre\* distribué (couche protocolaire) et/ou de leurs systèmes connectés (couche applicative). Ils peuvent être professionnels ou participer comme contributeurs bénévoles.

#### Disponibilité | Availability :

Correspond à une propriété recherchée par tout protocole de registre\* distribué permettant de garantir que toutes les requêtes soient satisfaites et que les *données endogènes\** soient toujours disponibles.

#### Données endogènes | Endogenous references :

Correspondent aux données pouvant être créées et transférées uniquement par le biais du protocole de registre\* distribué et qui, par leur format, leur sémantique, etc., ont un sens en son sein. Essentielles à son fonctionnement, elles garantissent la cohérence et l'intégrité des transactions\* et des enregistrements. Par exemple, pour Bitcoin et Ethereum, les données endogènes incluent les transactions\*, les blocs et les contrats intelligents.

#### Empreinte numérique | Hash :

Voir fonction de hachage.

#### Enregistrement candidat | Candidate Record :

Correspond à un enregistrement fraîchement propagé au réseau\* et donc, qui ne fait pas encore l'objet d'un consensus en son sein. C'est lorsqu'une majorité de nœuds\* l'ont reçu, vérifié et intégré dans leur registre\* transactionnel qu'il s'érite en *enregistrement canonique\**.

#### Enregistrement canonique | Record :

Un enregistrement - pour Bitcoin et Ethereum, il est d'usage de le nommer « Bloc » - représente un ensemble de données de transaction\* conteneurisé, reconnu par l'ensemble des nœuds\* comme canonique, après que chacun en a vérifié la validité. Un enregistrement est composé d'un *en-tête de bloc\** et de la liste des transactions\* qu'il contient, c'est-à-dire des transactions\* traitées et validées depuis le bloc précédent, à laquelle s'ajoute la plupart du temps une transaction\* attribuant une récompense au créateur de cet enregistrement.

#### Enregistrement de genèse | Genesis Record (or Genesis Block) :

Il correspond au premier enregistrement émis et diffusé au sein d'un protocole de registre\* distribué. Il a un statut particulier puisqu'il ne peut faire référence à un enregistrement précédent, contrairement aux autres enregistrements, ni à aucune transaction\* lui ayant précédé. Le bloc de genèse est codé dans les logiciels originaux et lance le protocole.

#### En-tête d'enregistrement (ou de bloc) | Record header (or block header) :

Un en-tête d'enregistrement est unique et sert à identifier un enregistrement particulier sur un *registre\**. C'est cet en-tête d'enregistrement qui est haché lors du processus de *preuve de travail\**. Sous le protocole Bitcoin, les *enregistrements\** ou blocs sont composés d'un en-tête de taille fixe contenant les informations uniquement nécessaires pour l'assemblage du registre\* (ou *blockchain*). Bien que cette taille très limitée ne permette pas de stocker l'ensemble des transactions\*, l'en-tête contient néanmoins la racine d'un *Arbre de Merkle\**, ce qui permet de vérifier la présence d'une transaction\* spécifique dans le *registre\** sans avoir à en télécharger l'intégralité.

#### Évolutivité ou Mise à l'échelle | Scalability :

Capacité d'un système de protocole de registre\* distribué à gérer un nombre croissant d'interactions de manière efficace sans compromettre ses performances.

#### Explorateur de registre | Ledger explorer :

Correspond à un outil offrant une interface utilisateur pour visualiser les données en temps réel d'un protocole de registre distribué. Facilitant la transparence et la vérification des transactions\*, il s'agit d'un outil *off chain* essentiel pour les utilisateurs et les développeurs\* qui souhaitent suivre l'activité et la santé du réseau\*.

### Frais de transaction au sein de la chaîne | On chain transaction fees finality :

Ce sont des frais exprimés et payés en *unité de compte native*\*, que définit l'utilisateur lorsqu'il produit une transaction\* afin d'interagir au *sein de la chaîne*\*. Généralement, et par-delà les différences entre les CM et leurs mécanismes de frais, la quantité de frais de transaction\* payée relativement aux autres usagers détermine la rapidité avec laquelle cette transaction\* sera traitée : les *opérateurs de transaction*\* ont tendance à choisir de traiter les transactions\* ayant les frais les plus élevés, de fait les plus rentables, puisque ces frais de transaction\* s'ajoutent à la *récompense d'enregistrement* pour constituer le revenu d'activité des *opérateurs de traitement des transactions*\*. L'utilisation de *passerelles*\* (bourse d'échange, etc.) peut induire, en plus de frais de transaction\* au sein de la chaîne, des frais de transaction\* en dehors de la chaîne, définis par les conditions générales de vente de la passerelle\*.

### Finalité de la transaction | Transaction finality :

Désigne le moment où un enregistrement confirmé peut être considéré comme définitif et irréversible. Elle peut être probabiliste, comme avec la PoW\* de Bitcoin, où la réversibilité devient computationnellement impossible après quelques blocs. Elle peut aussi être explicite, avec des protocoles intégrant des points de contrôle. En général, ce sont les acteurs économiques acceptant les unités de compte natives (UCN\*) qui définissent le nombre de confirmations nécessaires pour considérer une transaction\* comme réglée de leur côté.

### Fonction de hachage | Hash fonction :

Correspond à une fonction cryptographique qui, appliquée à des données brutes entrantes, les chiffre sous la forme d'une empreinte numérique\* unique et partielle (un *Hash*\*), de taille définie, et qui permet d'identifier facilement les données initiales. Voir Annexe n°V.3.

### Forge logicielle | Software Forge (conventionally referred to « code base repo » or « GitHub repo ») :

Une forge est une plateforme d'hébergement de projets logiciels, correspondant à un environnement web regroupant un ensemble d'outils qui permettent le développement collaboratif et distribué de logiciels. Elle offre un portail communautaire et l'accès à un site internet, un ensemble d'outils de gestion de projet et un environnement de développement collaboratif.

Les services disponibles vont de la fourniture d'un système de gestion des versions à des trackers permettant de faire remonter des demandes de fonctionnalité, réaliser le suivi des bogues, de la gestion de tâches ; la livraison des paquets et fichiers ; une intégration continue ; la gestion de documents (wiki) ; et d'autres services (forums, listes de discussion, sondages, etc.).

### Fork | Fork :

Peut-être traduit par *bifurcation*, mais, même en français, cet anglicisme s'est imposé. Suivant la situation, il peut qualifier un événement (volontaire ou non) qui voit un réseau\* se scinder en deux ou plusieurs réseaux\* (*Fork*\* de chaîne), avec autant de registres\* différents de transaction\*. Il sert aussi généralement à qualifier les modifications protocolaires considérées comme importantes, pour les faire évoluer dans une direction souhaitée (ajout/suppression de fonctionnalités, changement d'architecture, etc.). On distingue alors les *Soft Forks*\* des *Hard Forks*\*, comme leur dimension plus ou moins contentieuse. Un Fork\* de chaîne peut se produire suivant un bug logiciel, qui induit alors une perte de la *consistance*\* des *données endogènes*\* puisque des clients logiciels différents ne suivent plus les mêmes règles protocolaires ; ou quand une modification du protocole de registre\* distribué est entreprise et non suivie par l'ensemble des acteurs, donnant lieu à un *Hard Fork*\* contentieux. Ces deux branches de programmes devenues non compatibles donnent naissance à deux protocoles de registre\* distribué différents qui existent de manière autonome, le Fork\* devenant un moyen politique d'émancipation et de recomposition d'acteurs autour de valeurs et d'intérêts différenciés.

### Horodatage | Timestamp :

Processus d'enregistrement de la date et de l'heure exactes auxquelles un événement se produit. Il est couramment utilisé dans les fichiers journaux, les bases de données, les documents numériques et les systèmes de suivi pour assurer la traçabilité et l'intégrité des données.

### Hors-protocole | Off chain :

Interactions, transactions\*, processus qui se produisent en dehors des frontières formelles du protocole de registre\* distribué.

### Journal local | Journal :

Correspond à un ensemble d'enregistrements consignés localement dans un nœud, qui n'est pas nécessairement conforme au consensus des autres

nœuds\*. Les Journaux locaux sont partiels, provisoires et hétérogènes.

#### **Unité(s) de Compte Native(s) (UCN) | Native currency(ies) :**

La/les unités de compte émises et administrées au sein du protocole et utilisées typiquement pour réguler la production d'enregistrement\*, payer les frais de transaction\* d'usage du réseau\*, conduire la politique monétaire en vue d'aligner les intérêts des parties prenantes. Leurs formes scripturales suivent la logique et le(s) format(s) du protocole considéré.

#### **Langage de programmation | Programming language :**

Notation formelle utilisée pour définir des codes informatiques et les faire exécuter par un programme. Il comprend un ensemble d'instructions produisant divers types de résultats. La description d'un langage de programmation\* se divise généralement en deux : la syntaxe (forme) et la sémantique (signification). Elles peuvent être définies par un document de spécification ou ne relever que d'une implémentation dominante traitée comme une référence. Les développeurs\* peuvent utiliser de nombreux langages de programmation aux caractéristiques différentes pour réaliser des codes sources qui doivent encore être compilés pour être traduits en langage machine de bas de niveau. Ce langage machine, le langage natif d'un processeur, ne correspond qu'à des instructions codées en binaire. Par ex. : C++, Python, JavaScript, Solidity, Bytecode, etc.

#### **Livre Blanc | White Paper (WP) :**

Appellation qui tire son origine de la vie politique anglaise, où des documents imprimés sur un papier blanc servaient à présenter des politiques gouvernementales, et les soumettre à l'avis de la population. Ce terme a été utilisé par les entreprises pour décrire certains projets ou politiques commerciales. Désigne, dans notre champ, une publication plus ou moins longue, qui vise à donner une somme d'informations sur un projet donné. Le Livre Blanc sert à exposer un objectif comme les moyens proposés pour le résoudre. Publié par le/les instigateur(s) du projet, il peut aussi contenir des informations sur le financement du projet, un plan de route, un budget indicatif et une description de l'équipe qui travaille au développement. Un WP n'entre pas forcément profondément dans les détails techniques ; aussi, des Yellow Papers peuvent être publiés. Ces derniers correspondent à une version plus technique du WP, où sont présentés les détails technologiques, voire scientifiques, du projet.

#### **Maximaliste (Bitcoiner) | Maximalist (Bitcoiner) :**

Terme apparu en 2014, souvent attribué à Vitalik Buterin (2014a). Il désigne les *bitcoiners*\* pour qui Bitcoin devrait dominer toutes les autres CM (qualifiées d' « altcoins\* » ou de « shitcoins »), considérées comme inférieures ou inutiles. Ils considèrent qu'un environnement d'une multiplicité de CM concurrentes n'est pas souhaitable et que toutes les innovations, le développement dans le domaine crypto devraient se faire exclusivement sur Bitcoin. Par extension, le terme *maximaliste* peut également désigner les fervents défenseurs d'une cryptomonnaie\* spécifique et rejetant toutes les autres.

#### **Monnaies digitales | Digital Money :**

Catégorie générique recouvrant les monnaies basées sur une technologie de registre\* distribué, mais ne se limitant pas aux cryptomonnaies\* (CM). Elle englobe de nombreux objets relevant des logiques de signature ou de sceau, en fonction de l'existence d'acteurs centraux disposant de droits exorbitants sur le protocole, les données et le réseau\*. On peut distinguer en son sein, en plus des CM, les unités de compte émises par des entités privées, comme Tether, qui sont des monnaies numériques privées, et des monnaies publiques, avec l'arrivée des monnaies digitales\* de banque centrale (CBDC), dont la confiance repose sur une autorité émettrice publique. Voir encadré Chap.II.3.

#### **Nœud | Node :**

De manière générale, ce terme recouvre les acteurs non humains et leurs opérateurs humains participant du réseau\*, communiquant avec leurs pairs en suivant les règles canoniques du protocole de registre\* distribué considéré. Ils peuvent revêtir différentes formes et, suivant celles-ci, prendre part à tout ou partie des processus liés au traitement des transactions\* et à la production d'enregistrements ou à leur vérification : nœuds\* mineurs, nœuds\* complets, etc.

#### **Nonce | Nonce :**

Correspond en cryptographie\* à un nombre arbitraire (aléatoire ou pseudo-aléatoire) destiné à être utilisé une seule fois. Pour ce qui est des fonctions de *preuve de travail*\*, certains processus demandent de fournir un nonce qui, combiné au bloc de données mis en entrée d'une fonction de hachage\*, fournit un résultat ayant certaines caractéristiques recherchées, rendant beaucoup plus difficile de créer un résultat cible que de le vérifier. Pour Bitcoin, c'est ce nonce qui est modifié par les opérateurs de transaction\* à

chaque tentative de *preuve de travail*\*, jusqu'à l'obtention d'une *empreinte numérique*\* d'enregistrement inférieure ou égale à la *cible de difficulté*\*. Aussi, l'activité des opérateurs de transaction\* est de trouver en premier le *nonce* qui, combiné aux données initiales de l'*enregistrement candidat*\*, permet d'obtenir une empreinte numérique\* valide. Le *nonce* peut prendre un sens différent pour ce qui a trait à Ethereum, car, en plus du sens précédent, il correspond aussi à la numérotation des transactions\* effectuées et traitées par un compte de portefeuille.

#### **Passerelle | Gateway :**

Contient l'ensemble des acteurs qui fournissent une interface entre le système de protocole de registre\* distribué et le monde extérieur. On retrouve ici les bourses d'échange crypto fiat qui offrent une passerelle monétaire, mais aussi de nombreux autres services comme les explorateurs de registre\*, par exemple.

#### **Preuve de travail\* | Proof of Work (PoW\*) :**

Correspond à un processus nécessitant de résoudre un défi cryptographique : obtenir une empreinte cryptographique d'un niveau de difficulté donné. Pour les protocoles de registre\* dont le consensus repose sur une Proof of Work, ce processus est appelé « mining », et les opérateurs qui s'en chargent sont les « mineurs ».

#### **Portefeuille | Wallet :**

Correspond à un logiciel client capable de générer, stocker et administrer des couples de clefs cryptographiques afin de conserver et transférer ses CM et actifs digitaux.

#### **Protocole informatique | Protocol :**

Ensemble de règles et de procédures standardisées permettant à des machines en réseau\* de communiquer entre elles. Il détermine, pour un système donné, les modalités de son fonctionnement.

#### **Problème de double dépense | Double spending problem :**

Problème auquel fait face toute monnaie numérique. Il correspond à un acte frauduleux par lequel une unité de compte, du fait de son caractère numérique, est falsifiable et duplicable, et peut être dépensé plus d'une fois. Comme pour la fausse monnaie, une telle pratique peut faire augmenter la masse monétaire et éroder la confiance des utilisateurs dans le système de paiement.

#### **Récompense d'enregistrement | Block reward :**

Correspond à une récompense en *unité de compte native*\* perçue par un opérateur de transaction\* dont l'*enregistrement candidat*\* devient canonique en étant intégré au *registre*\*. Elle tient le rôle de création monétaire, rémunérant les acteurs en contrepartie du travail de traitement et de sécurisation des transactions\* et du *registre*.

#### **Registre | Ledger :**

Correspond, à tout moment, à l'ensemble des enregistrements faisant autorité, consignés dans une portion substantielle des nœuds\* participant au réseau\*. Un *registre* se compose d'une série de différents enregistrements stockant des informations relatives aux transactions\* qui ont lieu sur le réseau\*. Les enregistrements intégrés dans un tel registre sont peu susceptibles d'être effacés ou modifiés, et sont considérés comme finaux. Voir *finalité de paiement*\*

#### **Réorganisation d'enregistrement | Record reorganisation :**

Il s'agit d'un événement normal de tout protocole de registre\* distribué où un nœud du réseau\* découvre qu'un autre enregistrement valide existe en parallèle de celui qu'il suit. Par l'algorithme de consensus et à la suite d'un nouveau cycle de production d'enregistrement, cette version alternative du registre\* est devenue canonique pour tous, excluant un ou plusieurs enregistrement(s) auparavant inclus, dit(s) « orphelin(s) ». L'attaque 51% dont parle extensivement Nakamoto se rapporte à un cas critique de ce phénomène où une entité disposant de plus de 51% de la puissance de calcul va pouvoir préparer en secret un historique concurrent valide et plus lourd que celui actuellement considéré comme canonique, afin de tirer profit de l'annulation de transactions\* effectuées au sein de l'historique rendu orphelin. Voir Annexe n°V.5.

#### **Réseau\* | Network :**

Correspond à l'ensemble des acteurs - humains ou non - et des processus interconnectés qui mettent en œuvre un protocole de communication entre différentes machines ou *nœuds*\* leur permettant d'échanger des informations. Les réseaux les plus répandus fonctionnent sur le mode de communication dit « client/serveur », où un ordinateur et son utilisateur - le client - demandent des informations par l'émission d'une requête à un serveur central qui en dispose et lui transmet en retour. C'est le cas des navigateurs et d'une grande majorité de sites Internet, par exemple. D'autres formes existent comme les *réseaux*\* *pair-à-pair*\*

#### **Réseau pair-à-pair | Peer-to-peer Network :**

Correspond à un réseau\* où les nœuds\* qui participent à l'échange d'information sont, contrairement au mode « client/serveur », tour à tour client et serveur, demandeur et donneur. Chaque nœud\* est sur un pied d'égalité avec les autres nœuds\* constituant le réseau\*, et ils sont donc des pairs. Il n'y a plus un acteur qui dispose des informations auxquelles souhaite accéder une multitude d'utilisateurs, car les informations sont répliquées sur une multitude de nœuds\*.

#### Résistance à la censure | Censorship

##### Resistance :

Correspond à l'impossibilité pour un acteur ou un cartel d'effectuer unilatéralement et arbitrairement : (i) une modification des règles du protocole ; (ii) de bloquer ou de censurer des transactions\* ; et (iii) de saisir un compte ou de geler des avoirs.

#### Script à exécution programmatique |

##### Programmatically-executed scrypt :

Script informatique qui, lorsqu'il est déclenché par un message particulier, est exécuté par le protocole de registre\* distribué. Lorsque le code est capable de fonctionner suivant les attentes des parties engagées, le caractère déterministe de l'exécution réduit le niveau de confiance nécessaire aux participants individuels dans leurs interactions réciproques. Ils sont communément appelés « Smart contracts\* » en raison de la capacité des scripts à remplacer certaines relations contractuelles ou fiduciaires, comme la conservation ou le séquestre, par du code. En revanche, ils ne sont ni autonomes, ni adaptatifs (« intelligents »), et encore moins un contrat au sens juridique du terme.

#### Signature cryptographique | Cryptographic signature :

Reposant sur la cryptographie\* asymétrique, ce type de signature permet de vérifier mathématiquement la possession d'un ensemble de données, si tant est que l'utilisateur conserve secrète sa clef privée pour signer ses transactions\*. Voir Annexe n°V.1.

#### Sortie de transaction non dépensée | UTXO :

Forme prise par les unités de compte reçues mais non encore dépensées pour les systèmes de protocole de registre\* distribué qui, comme Bitcoin, fonctionnent sur ce type d'architecture : ici, l'état de la structure des *données endogènes\**, contenues dans le *registre\** à un instant T, représente la collection de toutes les UTXO\* existantes. Ainsi, une transaction\* correspond à une cession authentifiée d'une ou plusieurs

UTXO\* (qui sont à l'*output* de la transaction\*) et qui donnera lieu, en sortie, à une UTXO\* reçue par le receveur (pour lui en *input*). D'autres architectures peuvent être choisies quant au suivi de l'état de la structure de donnée, comme avec Ethereum et son *modèle basé sur compte\**.

#### Modèle basé sur compte | Account based

##### Model :

Le modèle basé sur compte, comme pour le modèle basé sur UTXO\*, sert en premier lieu au suivi de l'état de la structure de donnée. Mais ici, comme pour un compte bancaire traditionnel, à un instant T, le système de protocole de registre\* distribué renseigne des soldes pour chaque compte. Une transaction\* authentifiée correspond alors à une cession qui réduit le solde de l'envoyeur d'autant que ce que le receveur reçoit sur son compte. Ce choix d'Ethereum s'explique par le fait que, en plus des comptes personnels - ou comptes de détenteur externe ou EOA - contrôlés par une clé privée, il existe des comptes contrôlés par une commande/code de contrat (les smart contracts\*, SC). Le modèle basé sur compte répond alors à des besoins spécifiques et permet d'augmenter la capacité d'exécution des smart contracts\* du protocole de registre\* distribué qui fait ce choix (plus grande simplicité, gain de place, fongibilité accrue).

#### Système de protocole de registre distribué |

##### DLT system :

Système d'enregistrement électronique qui permet à un réseau\* de participants indépendants d'établir un consensus autour d'un ordonnancement de transactions\* validées cryptographiquement qui fait autorité. Les enregistrements sont rendus persistants par fait de réPLICATION des données sur une multitude de nœuds\*, et sont témoins de violabilité /d'intégrité (temper-evident) par les liens cryptographiques qui les relient (les hash\*). Le résultat partagé du processus de réconciliation/consensus constitue un registre\* transactionnel canonique faisant autorité.

#### Système de protocole de registre fermé (ou avec autorisation) | Permissioned System :

Protocole de registre\* distribué de type « Classique », car premier à avoir été développé. Ce système correspond à la définition générale des DLT ; l'archivage partagé\* n'est pas ouvert à tous et seuls les participants formellement reconnus et autorisés peuvent participer. Cette sélection est effectuée par l'/les autorité(s) compétente(s) – entité(s) qui conçoit(ven)t et déploie(n)t le système – et inscrite dans le code logiciel fourni par les administrateurs.

### **Système de protocole de registre ouvert (ou sans autorisation) | Permissionless System :**

Protocole de registre\* distribué qui sous-tend ce que nous considérons et qualifions de CM. Dans ce type de système, l'archivage partagé\* est ouvert à tous sans qu'une entité ou un groupe ne se voie reconnaître protocolairement de privilège quelconque.

### **Temps d'enregistrement | Block time :**

Le temps d'enregistrement ou de bloc fait référence au temps moyen nécessaire pour créer (ou miner) un nouveau bloc sur la blockchain et conclure un cycle de traitement des transactions\*. Pour Bitcoin, le temps d'enregistrement moyen est d'environ 10 minutes.

### **Tolérance à la partition | Partitioning Tolerance :**

Correspond à une propriété recherchée par tout système informatique de calcul distribué permettant qu'aucune défaillance - à l'exception d'une panne totale du réseau\* - d'un ou plusieurs nœud(s) n'empêche le système de répondre correctement.

### **Traitement des transactions | Transaction processing :**

Correspond à l'ensemble des processus qui spécifient les mécanismes de mise à jour du registre. Il définit : (i) quels participants ont le droit de mettre à jour l'ensemble d'enregistrements partagés faisant autorité (sans autorisation pour les systèmes ouverts et avec autorisation formelle pour les systèmes privés ou de consortium), et (ii) comment les participants parviennent à un accord consensuel sur la mise en place de cette mise à jour. Appelé aussi « mining ».

### **Transaction | Transaction :**

Renvoie à toute modification proposée au registre ; elle n'est pas nécessairement de nature économique (transfert de valeur). Une transaction\* peut être soit non confirmée (non incluse dans le registre, elle se trouve encore seulement dans la mempool), soit confirmée (inclusa dans le registre). Une même transaction\* peut contenir une multitude de transactions\* différentes : différents receveurs ; différentes modifications de registre, etc.

### **Validation | Validation :**

Correspond à l'ensemble des processus requis afin d'assurer que les acteurs arrivent indépendamment à la même conclusion en ce qui concerne l'état du registre. Cela inclut la vérification de la validité des transactions\* non confirmées, la vérification des enregistrements,

qu'ils soient confirmés ou non, et l'audit de l'état du système.

### **Validation indépendante | Independent Validation :**

Désigne la capacité du système de protocole de registre\* distribué à permettre à chaque participant la vérification indépendante de l'état des transactions\* et de l'intégrité du système.

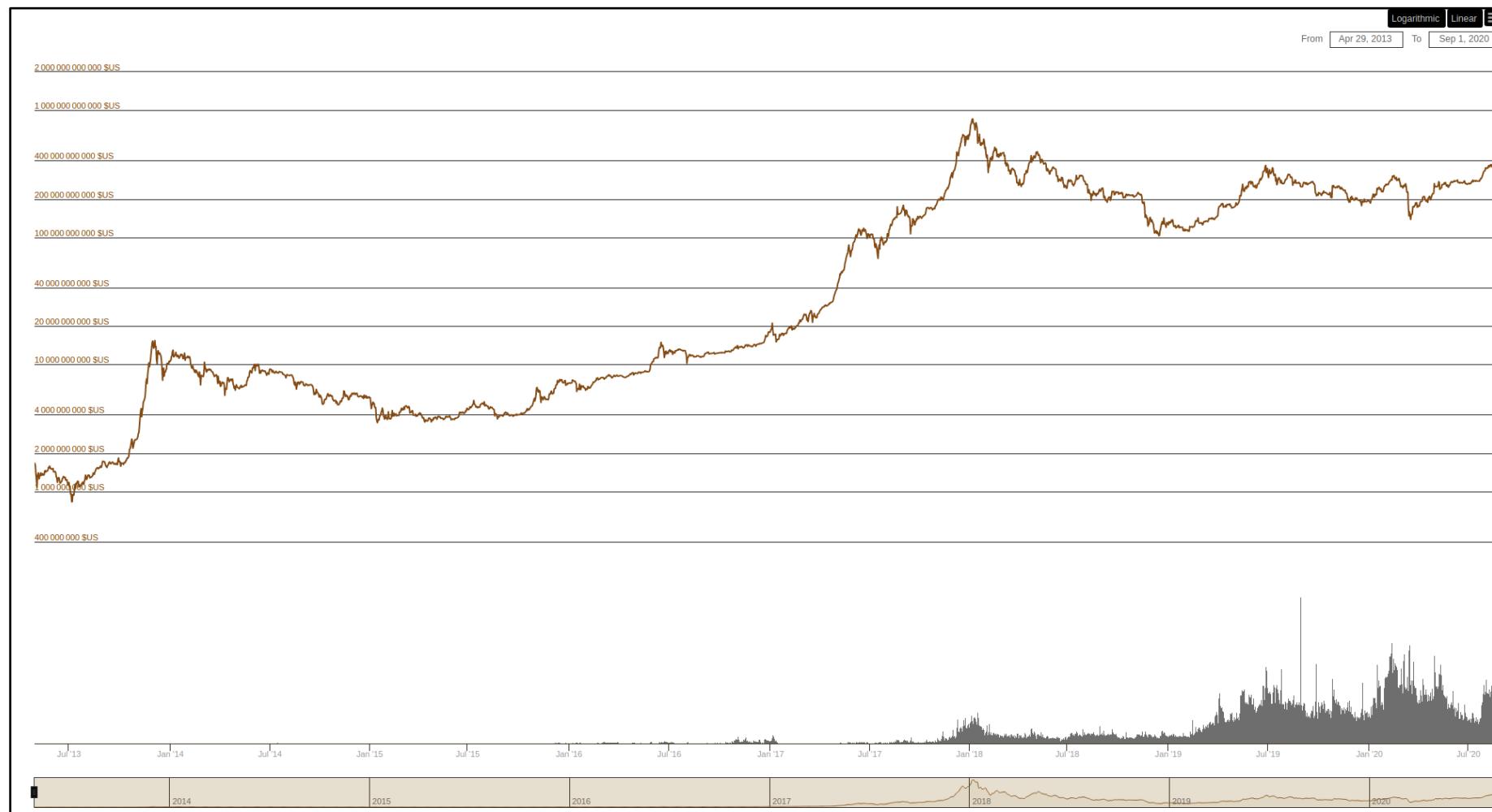
## ANNEXES

|  |              |
|--|--------------|
| <b>ANNEXE I : DONNÉES SYNTHÉTIQUES RELATIVES À L'ÉCOSYSTÈME DES CM PRIS DANS SON ENSEMBLE .....</b>  | <b>XII</b>   |
| ANNEXE I.1 : CAPITALISATION TOTALE ET TAUX DE DOMINANCE SUR LE MARCHÉ DES CRYPTO-ACTIFS (~5868 ACTIFS LISTÉS SUR COINGECKO), AU 01/09/2020 ..... | XII          |
| ANNEXE I.2 : CAPITALISATION TOTALE ET TAUX DE DOMINANCE DE MARCHÉ DES CRYPTO-ACTIFS (~5868 ACTIFS LISTÉS), AU 01/09/2020 .....                   | XIV          |
| ANNEXE I.3 : ÉVOLUTION DU NOMBRE D'UTILISATEURS DE LA PLATEFORME COINBASE .....  | XVI          |
| ANNEXE I.4 : CHRONOLOGIES CIRCONSTANCIÉES DU PHÉNOMÈNE DES INITIAL COIN OFFERING (ICO), DE JUILLET 2013 À JUIN 2017 .....                        | XVII         |
| <b>ANNEXE II : DONNÉES SYNTHÉTIQUES RELATIVES À L'ÉCOSYSTÈME DE BITCOIN .....</b>  | <b>XVIII</b> |
| ANNEXE II.1 : L'UCN BITCOIN ET SA DÉCIMALISATION (MATÉRIELLE ET SYMBOLIQUE) .....  | XVIII        |
| ANNEXE II.2 : UNE OFFRE MONÉTAIRE PROGRAMMATIQUE : ENTRE ÉMISSION ANTICIPÉE ET EFFECTIVE .....   | XIX          |
| ANNEXE II.3 : CAPITALISATION DE MARCHÉ DU BTC, EN PRIX DE MARCHÉ ET RÉALISÉE, EN USD .....   | XX           |
| ANNEXE II.4 : NOMBRE D'ADRESSES ACTIVES ET TAILLE MOYENNE DES ENREGISTREMENTS (EN BYTES), QUOTIDIEN  | XXI          |
| ANNEXE II.5 : NOMBRE DE TRANSACTIONS ET TRANSFERTS QUOTIDIENS .....  | XXI          |
| ANNEXE II.6 : TAILLE GLOBALE DE TOUS LES TRANSFERTS QUOTIDIENS, BTC ET USD .....   | XXII         |
| ANNEXE II.7 : TAILLE MOYENNE DES TRANSFERTS, EN BTC ET USD, QUOTIDIEN .....  | XXII         |
| ANNEXE II.8 : TAILLE MÉDIANE DES TRANSFERTS, EN BTC ET USD, QUOTIDIEN .....  | XXIII        |
| ANNEXE II.9 : SOMME DES FRAIS DE TRANSACTION, EN BTC ET USD, QUOTIDIEN .....   | XXIII        |
| ANNEXE II.10 : FRAIS DE TRANSACTION, MOYEN ET MÉDIAN, EN BTC ET USD, QUOTIDIEN .....   | XXIV         |
| ANNEXE II.11 : REVENU CUMULÉ DES .....   | XXIV         |
| ANNEXE II.12 : QUANTITÉ HASH/S CUMULÉE ET PRIX DU BTC, EN USD, QUOTIDIEN .....   | XXV          |
| ANNEXE II.13 : ÉVOLUTION DE L'INDEX DE CONSOMMATION ÉLECTRIQUE DE BITCOIN, EN TWH ANNUALISÉ .....  | XXV          |
| ANNEXE II.14 : VOLATILITÉ DE L'UCN BTC, EN USD SUR 30, 60 ET 180 JOURS .....   | XXVI         |
| <b>ANNEXE III : DONNÉES SYNTHÉTIQUES RELATIVES À L'ÉCOSYSTÈME D'ETHEREUM .....</b>   | <b>XXVII</b> |
| TABLEAU III.1: L'UCN ETHER ET SA DÉCIMALISATION (MATÉRIELLE ET SYMBOLIQUE) .....   | XXVII        |
| ANNEXE III.2 : L'OFFRE MONÉTAIRE PROGRAMMATIQUE D'ETHEREUM : ENTRE ÉMISSION ANTICIPÉE ET EFFECTIVE .....   | XXIX         |
| FIGURE III.3 : CAPITALISATION DE MARCHÉ DE L'ETH EN PRIX DE MARCHÉ, EN USD .....   | XXX          |
| ANNEXE III.4 : NOMBRE D'ADRESSES ACTIVES ET TAILLE MOYENNE DES ENREGISTREMENTS (EN BYTES), QUOTIDIEN .....                                       | XXXI         |
| ANNEXE III.5 : NOMBRE DE TRANSACTIONS ET TRANSFERTS .....  | XXXI         |
| ANNEXE III.6 : TAILLE GLOBALE DE TOUS LES TRANSFERTS QUOTIDIENS, ETH ET USD .....  | XXXII        |
| ANNEXE III.7 : TAILLE MOYENNE DES TRANSFERTS, EN ETH ET USD, QUOTIDIEN .....   | XXXII        |
| ANNEXE III.8 : TAILLE MÉDIANE DES TRANSFERTS, EN ETH ET USD, QUOTIDIEN .....   | XXXIII       |
| ANNEXE III.9 : SOMME DES FRAIS DE TRANSACTION, EN ETH ET USD, QUOTIDIEN .....  | XXXIII       |
| ANNEXE III.10 : FRAIS DE TRANSACTION, MOYEN ET MÉDIAN, EN ETH ET USD, QUOTIDIEN .....  | XXXIV        |
| ANNEXE III.11 : REVENU CUMULÉ DES .....  | XXXIV        |
| ANNEXE III.12 : QUANTITÉ HASH/S CUMULÉE ET PRIX DE L'ETH EN USD, QUOTIDIEN .....   | XXXV         |
| ANNEXE III.13 : VOLATILITÉ DE L'UCN ETH, EN USD SUR 30, 60 ET 180 JOURS .....  | XXXV         |
| ANNEXE III.14 : LES COFONDATEURS D'ETHEREUM .....  | XXXVI        |
| ANNEXE III.15 ETHEREUM VERSUS ETHEREUM CLASSIC .....   | XL           |
| <i>Annexe III.15.1 : Répartition du taux de Hash moyen entre ETH et ETC, quotidien .....</i>   | <i>XLI</i>   |
| <i>Annexe III.15.2 : Miner de l'ETH ou de l'ETC : un dilemme philosophique et économique .....</i>   | <i>XLI</i>   |
| <i>Annexe III.15.3 : Evolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum Classic .....</i>                          | <i>XLII</i>  |
| <i>Annexe III.15.4 : Evolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum .....</i>                                  | <i>XLII</i>  |
| <b>ANNEXE IV: DONNÉES SYNTHÉTIQUES RELATIVES À NOS STRATÉGIES ET DISPOSITIFS D'ACCÈS AU TERRAIN .....</b>  | <b>XLIII</b> |
| ANNEXE IV.1 : DÉTAILS DES IMMERSIONS PARTICIPANTES .....   | XLIII        |

|  |              |
|--|--------------|
| ANNEXE IV.2 : DÉTAILS DES OBSERVATIONS PARTICIPANTES.....  | L            |
| ANNEXE IV.3 : STATUT(S) ET RÔLE(S) COUVERT(S) PAR LES ACTEURS DE NOS ENTRETIENS .....                    | LIII         |
| ANNEXE IV.4 : LISTE DES ENTRETIENS MENÉS ET NOTICE BIOGRAPHIQUE SUCCINCTE DES ENQUÊTÉS .....             | LVI          |
| <b>ANNEXE V: RETOURS CIRCONSTANCIÉS SUR LES COMPOSANTS CLEFS ET LE FONCTIONNEMENT<br/>D'UNE CM .....</b> | <b>LXVII</b> |
| ANNEXE V.1 : CRYPTOGRAPHIE ASYMÉTRIQUE ET SOUVERAINETÉ INDIVIDUELLE .....                                | LXVII        |
| ANNEXE V.2 : CLEFS PRIVÉES, CLEFS PUBLIQUES ET ADRESSES BITCOIN .....                                    | LXVII        |
| ANNEXE V.3 : LA FONCTION DE HACHAGE SHA 256 .....  | LXVIII       |
| ANNEXE V.4 : L'ARBRE DE MERKLE.....  | LXVIII       |
| ANNEXE V.5 : CAS D'UNE RÉORGANISATION MALICIEUSE DE TYPE .....   | LXX          |
| ANNEXE V.6 : RELATIONS HIÉRARCHIQUES ENTRE LES TROIS COUCHES D'UN PROTOCOLE DE REGISTRE DISTRIBUÉ.       | LXXI         |

## Annexe I : Données synthétiques relatives à l'écosystème des CM pris dans son ensemble

### Annexe I.1 : Capitalisation totale et taux de dominance sur le marché des crypto-actifs (~5868 actifs listés sur Coingecko), au 01/09/2020



Source : <https://www.coingecko.com/fr>



Source : <https://www.coingecko.com/fr>

Annexe I.2 : Capitalisation totale et taux de dominance de marché des crypto-actifs (~5868 actifs listés), au 01/09/2020

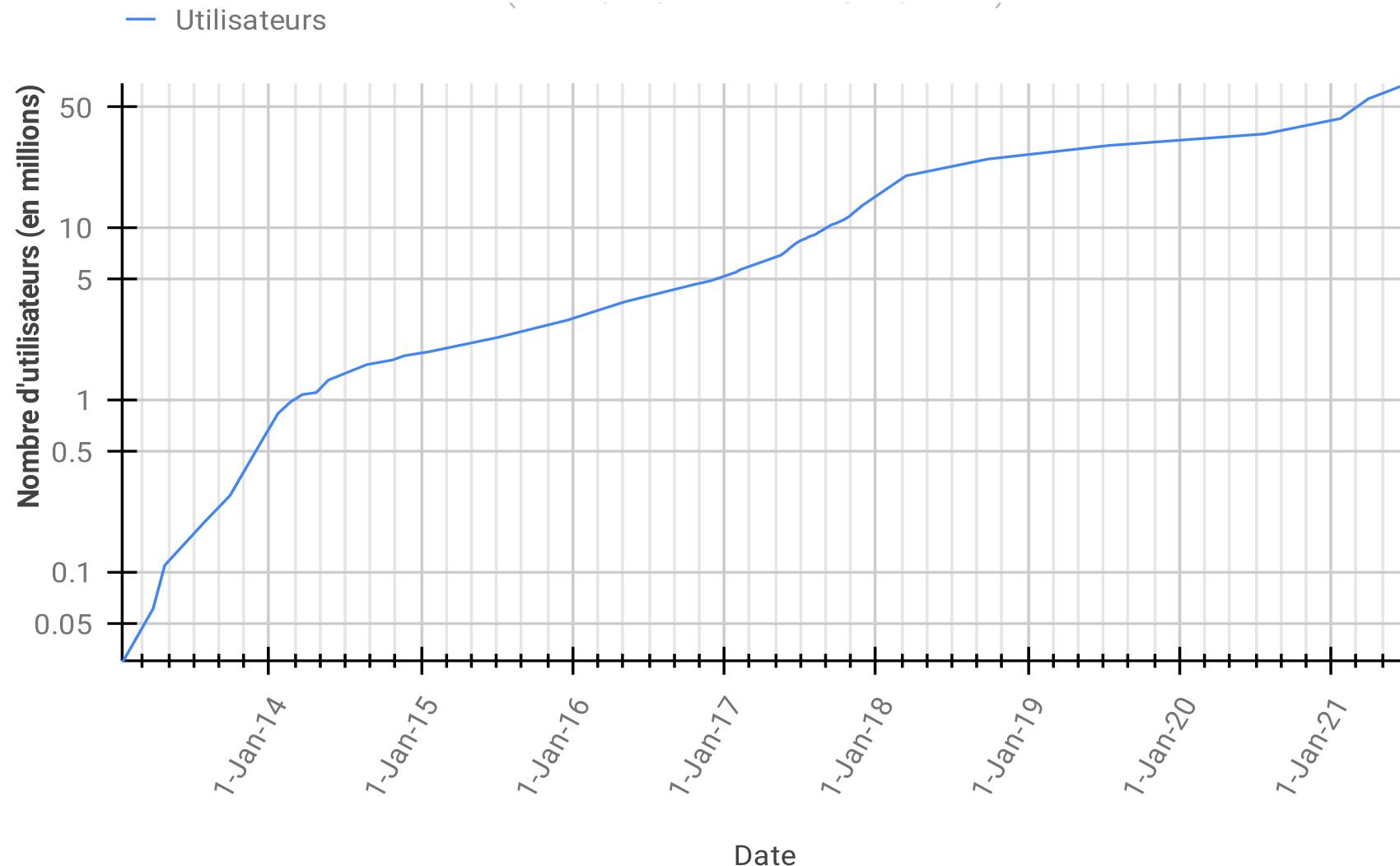
| Rang | CM ou crypto-actif   | Ticker | Cours (\$) | Volume 24h (en \$) | Capitalisation totale (en \$) | Dominance (en %) |
|------|--|--------|------------|--------------------|-------------------------------|------------------|
| 1    |  Bitcoin        | BTC    | 11 909,63  | 23 529 258 593     | 220 049 317 281               | 54,89 %          |
| 2    |  Ethereum       | ETH    | 460,92     | 17 249 915 593     | 51 787 809 789                | 12,91 %          |
| 3    |  Tether         | USDT   | 1          | 39 137 093 048     | 13 442 100 350                | 3,35 %           |
| 4    |  XRP            | XRP    | 0,29       | 1 906 782 832      | 13 155 811 083                | 3,28 %           |
| 5    |  ChainLink      | LINK   | 16,21      | 1 099 639 778      | 6 240 933 623                 | 1,55 %           |
| 6    |  Polkadot      | DOT    | 6,72       | 555 583 850        | 6 092 040 460                 | 1,51 %           |
| 7    |  Bitcoin Cash | BCH    | 280,63     | 2 493 105 816      | 5 198 817 899                 | 1,29 %           |
| 8    |  Litecoin     | LTC    | 62,75      | 2 472 163 202      | 4 102 489 879                 | 1,02 %           |

|   |  |            |               |                       |                        |                |
|---|--|------------|---------------|-----------------------|------------------------|----------------|
| <b>9</b>                                    |  Cardano    | <b>ADA</b> | <b>0,1242</b> | <b>528 551 176</b>    | <b>3 867 875 994</b>   | <b>0,96 %</b>  |
| <b>10</b>                                   |  Bitcoin SV | <b>BSV</b> | <b>199,14</b> | <b>758 820 514</b>    | <b>3 688 194 961</b>   | <b>0,92 %</b>  |
| <b>25 premières</b>                         |  |            |               |                       | <b>357 540 681 324</b> | <b>89,19 %</b> |
| <b>50 premières</b>                         |  |            |               |                       | <b>374 229 952 997</b> | <b>93,35 %</b> |
| <b>Effectif Total (5868 crypto-actifs*)</b> |  |            |               | <b>94 529 688 590</b> | <b>400 851 587 974</b> | <b>100%</b>    |

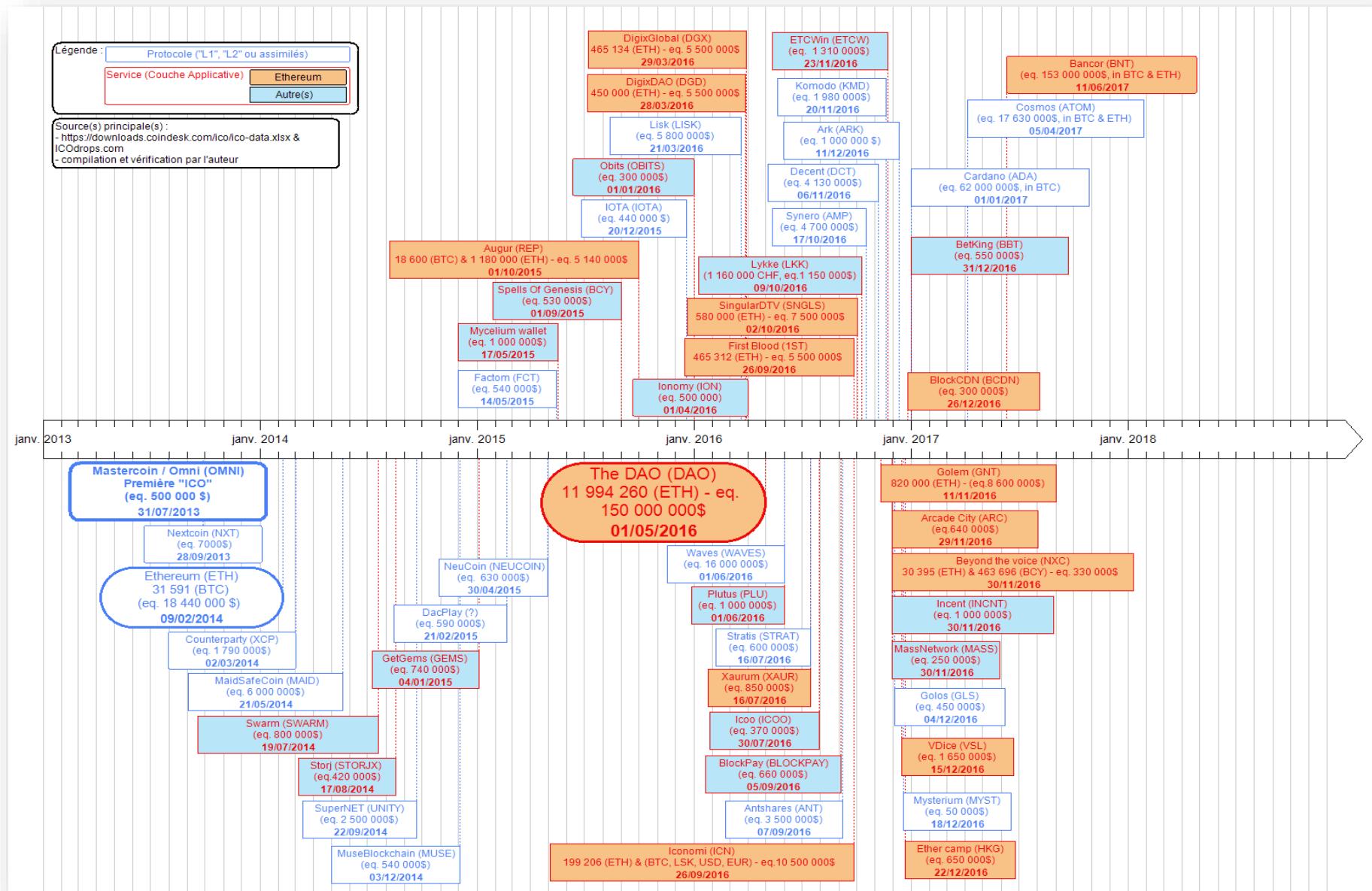
Source : <https://www.coingecko.com/fr>, traitement de l'auteur.

### Annexe I.3 : Évolution du nombre d'utilisateurs de la plateforme Coinbase

(Du 13/01/2013 au 30/06/2021)



## Annexe I.4 : Chronologies circonstanciées du phénomène des Initial Coin Offering (ICO), de juillet 2013 à juin 2017



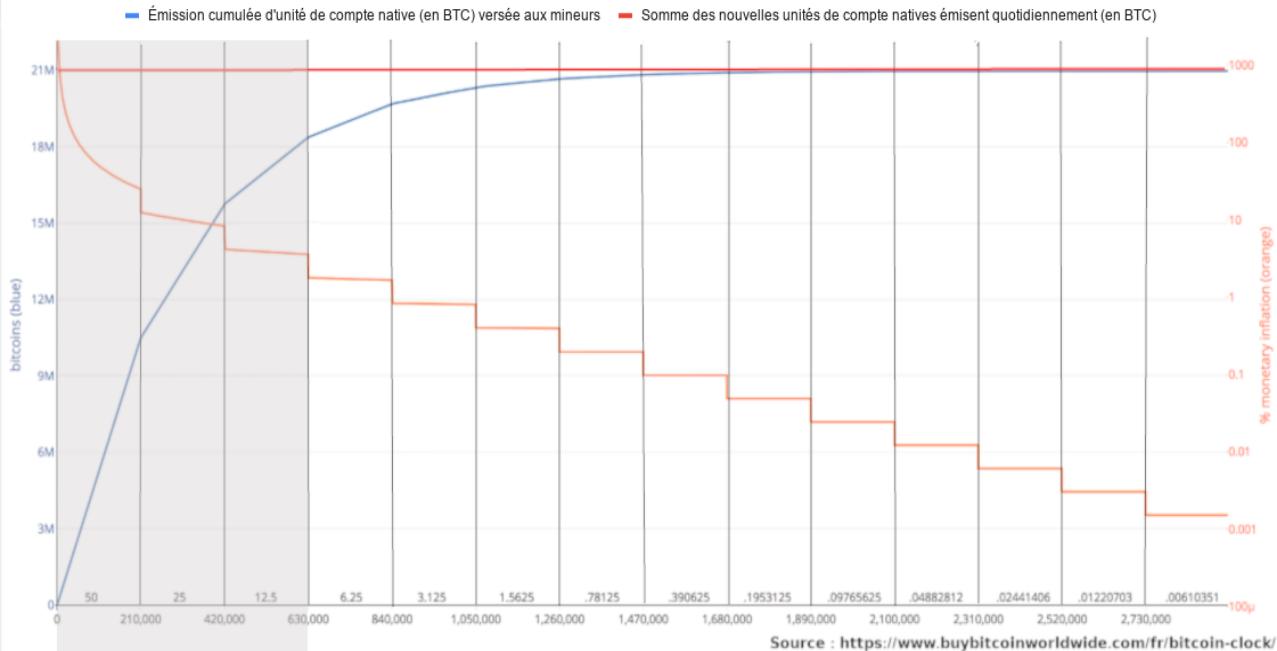
## Annexe II : Données synthétiques relatives à l'écosystème de Bitcoin

### Annexe II.1 : L'UCN bitcoin et sa décimalisation (matérielle et symbolique)

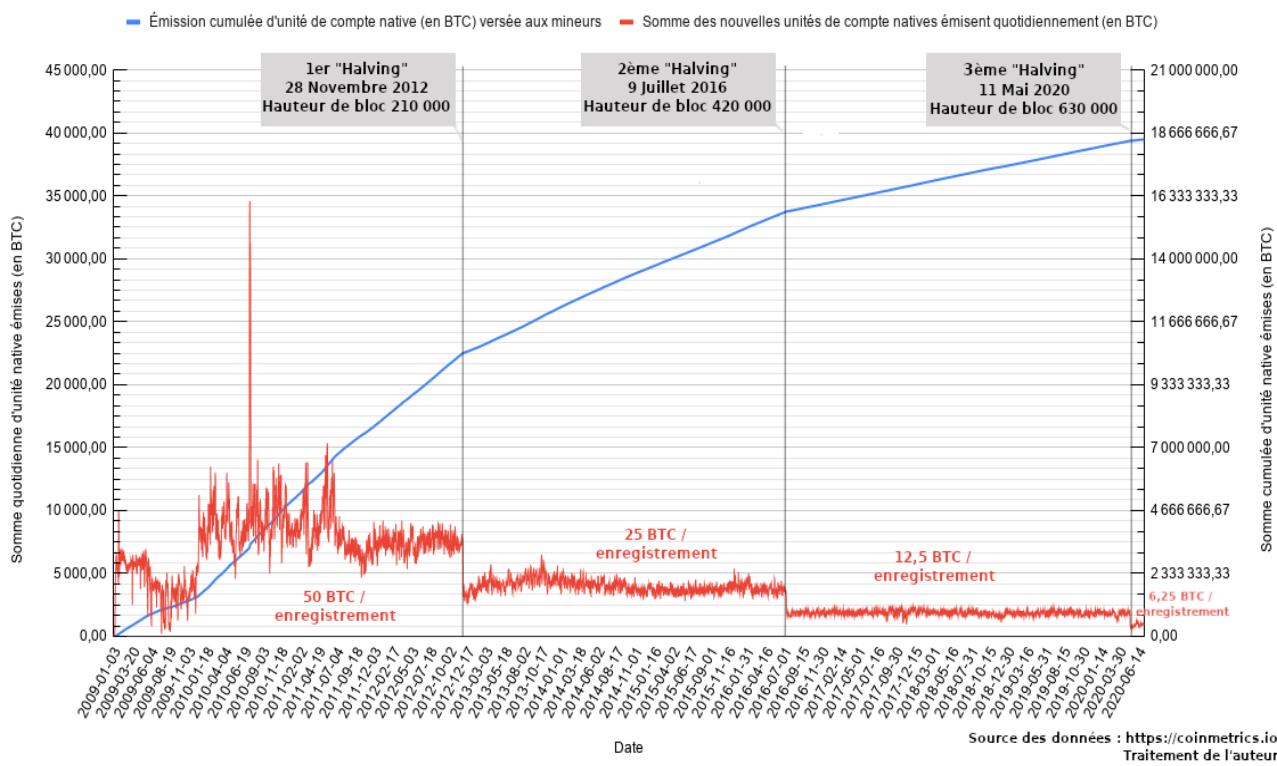
| Bitcoin et son UCN* bitcoin  |   |  |                             |
|--|---|--|-----------------------------|
| Représentation symbolique des UCN*   |   |  |                             |
| « Ticker » boursier & symbole  | <b>BTC (ou XBT)</b><br><b>฿</b>   |  |                             |
| Décomposition fractionnaire des UCN* et leur valeur de conversion en UCN* principale | <b>Unité(s) fractionnaire(s) conventionnelle(s)</b>   |  | <b>Valeur en UCN* (BTC)</b> |
|  | Le « <i>bitcoin</i> » (ou BTC)  |  | 1                           |
|  | Le « <i>Cent-bitcoin</i> »   le « <i>cBTC</i> »   ou le « <i>bitcent</i> »  |  | 0.01                        |
|  | Le « <i>Milli-Bitcoin</i> »   le « <i>mBTC</i> »   ou le « <i>millibit</i> »  |  | 0.001                       |
|  | Le « <i>Micro-Bitcoin</i> »   le « <i>μBTC</i> »   ou le « <i>bit</i> »   |  | 0.000001                    |
|  | Le « <i>Finney</i> »  |  | 0.0000001                   |
|  | Le « <i>Satochi</i> »   |  | 0.00000001                  |
| Source :   | <a href="https://atozmarkets.com/news/simple-guide-to-bitcoin-units-of-measurement/">https://atozmarkets.com/news/simple-guide-to-bitcoin-units-of-measurement/</a> |  |                             |

## Annexe II.2 : Une offre monétaire programmatique : entre émission anticipée et effective

**Figure n°2.1. Emission anticipée d'unité de compte BTC (cumulée et quotidienne)**  
 du 03-01-2009 au 07-07-2020

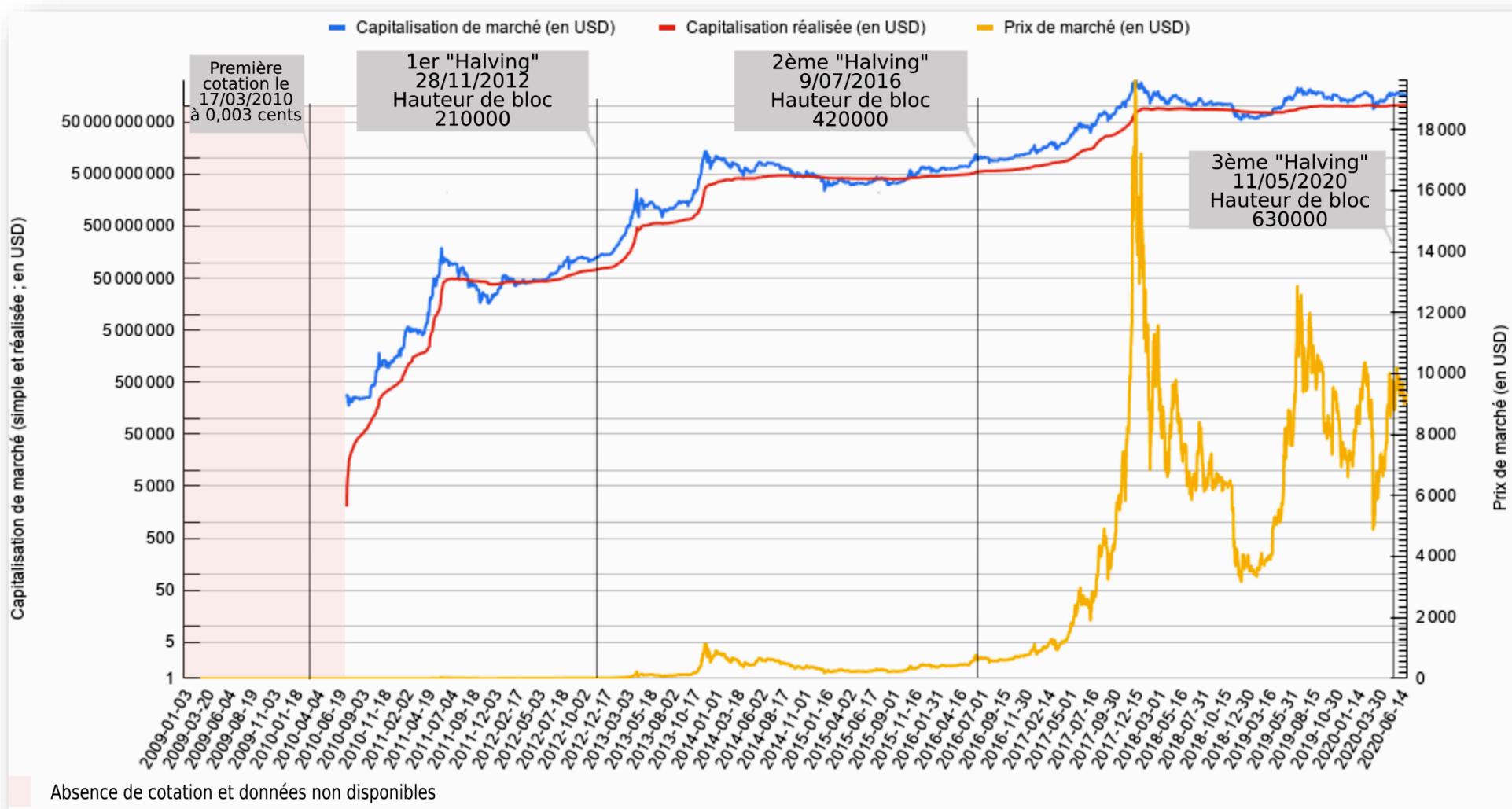


**Figure n°2.2. Emission effective d'unité de compte BTC (cumulée et quotidienne)**  
 (Du 03/01/2009 au 07/07/2020)



## Annexe II.3 : Capitalisation de marché du BTC, en prix de marché<sup>(1)</sup> et réalisée<sup>(2)</sup>, en USD

(du 18 Juillet 2010 au 07 Juillet 2020)



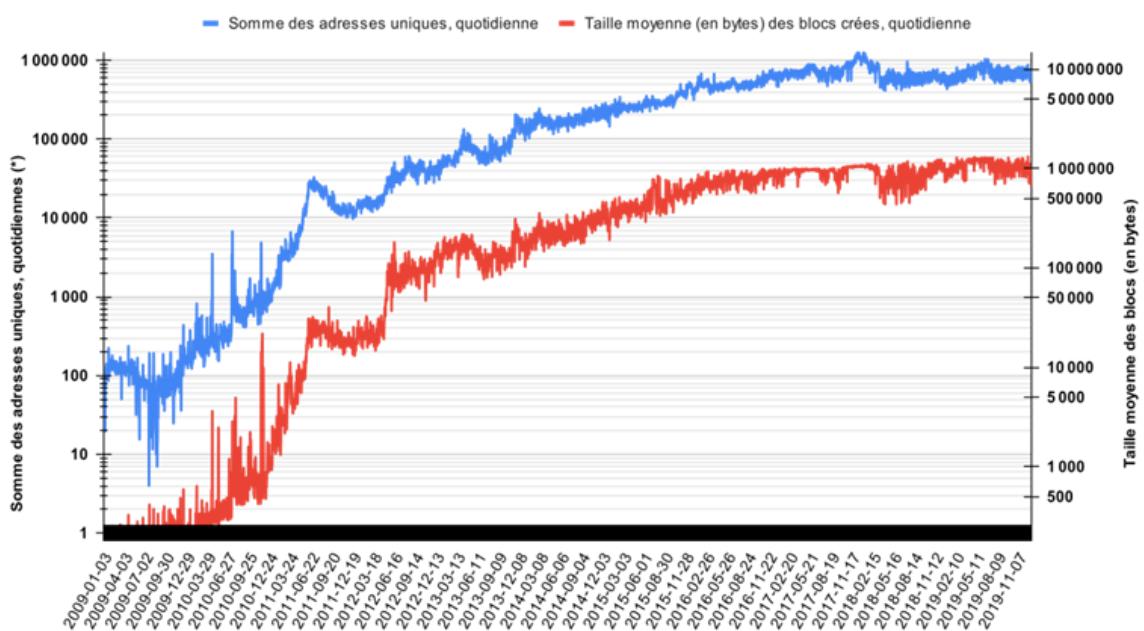
**Source des données :** <https://www.coinmetrics.io>; (cf. Chapitre 1 pour la 1<sup>ère</sup> cotation) ; traitement de l'auteur.

<sup>(1)</sup> Valeur agrégée en USD de l'offre actuelle, également appelée valeur du réseau ou capitalisation du marché.

<sup>(2)</sup> Valeur agrégée en USD basée sur le prix de clôture du BTC le jour de la dernière transaction impliquant chacune d'elles (leurs UTXO) : cette mesure est plus précise en ce qu'elle tient

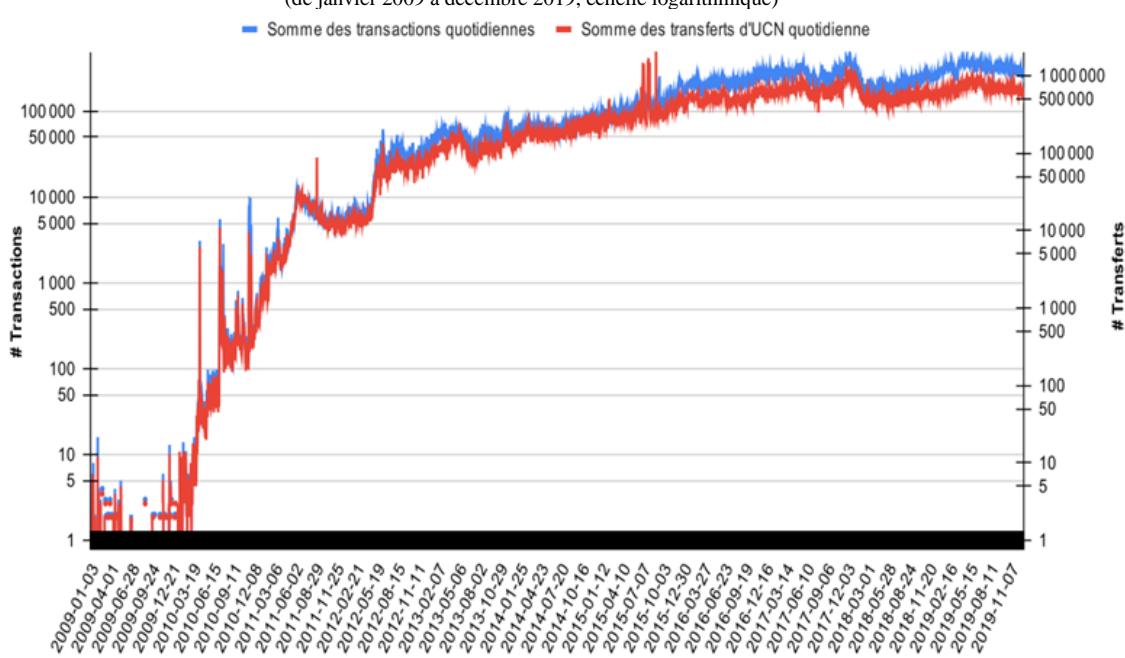
## Annexe II.4 : Nombre d'adresses actives<sup>(1)</sup> et taille moyenne des enregistrements (en bytes), quotidien

(de janvier 2009 à décembre 2019, échelle logarithmique)



## Annexe II.5 : Nombre de transactions<sup>(2)</sup> et transferts<sup>(3)</sup> quotidiens

(de janvier 2009 à décembre 2019, échelle logarithmique)



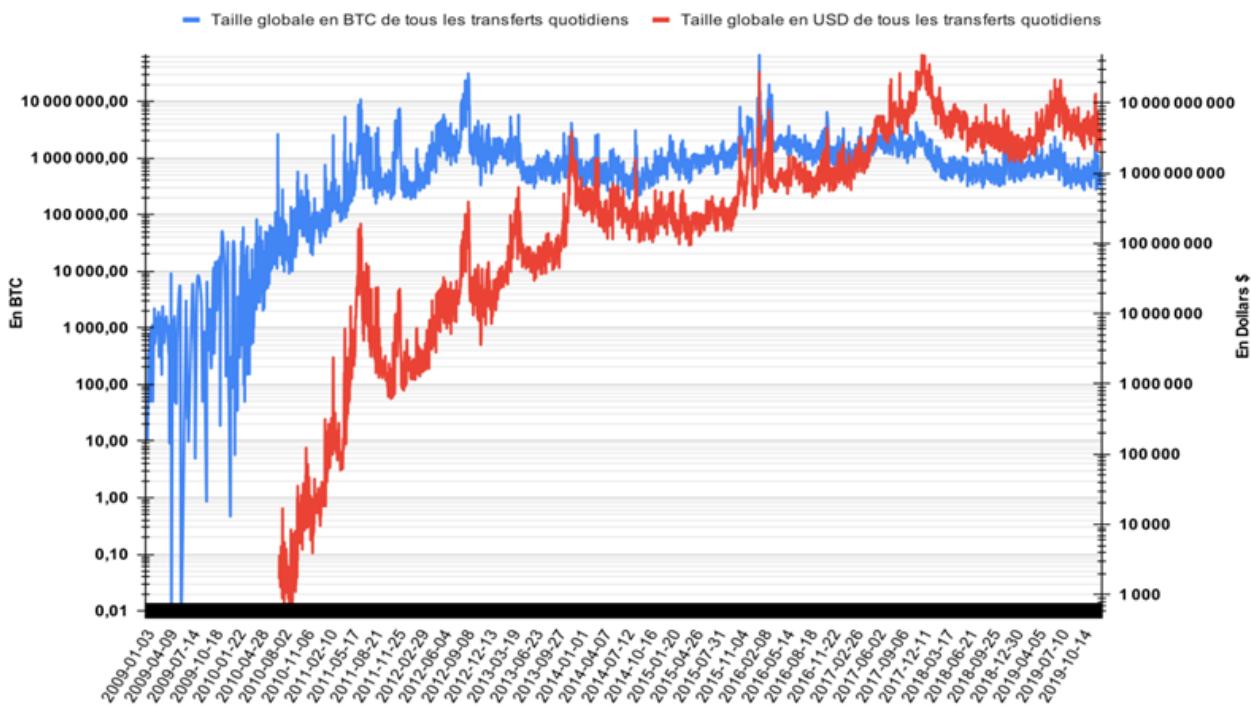
**Source des données :** <https://www.coinmetrics.io>; traitement de l'auteur.

<sup>(1)</sup> Somme des adresses uniques actives quotidiennes (destinataires et envoyeurs, chaque adresse n'est comptée qu'une fois).

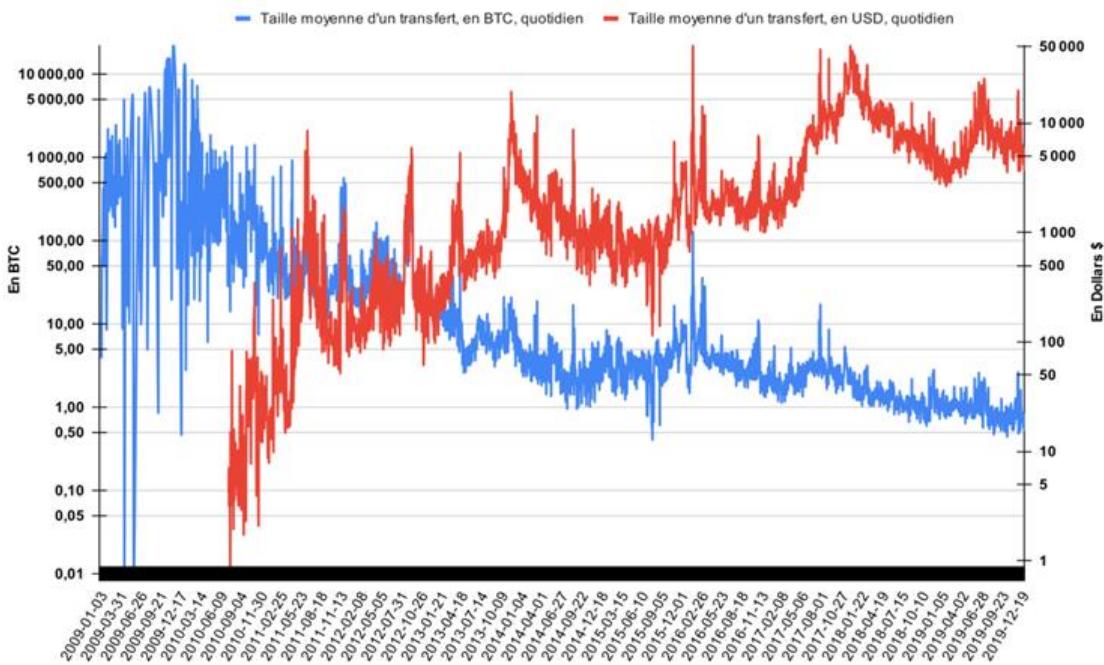
<sup>(2)</sup> Somme des transactions quotidiennes (exécutées ou non et avec transfert d'UCN ou non), hors transactions protocolaires (cf. *coinbase transaction*).

<sup>(3)</sup> Somme des transferts quotidiens : mouvements d'UCN d'une adresse à une autre, résultants d'une transaction et qui ont une valeur positive.

**Annexe II.6 : Taille globale de tous les transferts quotidiens, BTC et USD<sup>(1)</sup>**  
 (de janvier 2009 à décembre 2019, échelle logarithmique)



**Annexe II.7 : Taille moyenne des transferts, en BTC et USD, quotidien<sup>(2)</sup>**  
 (de janvier 2009 à mars 2019, échelle logarithmique)



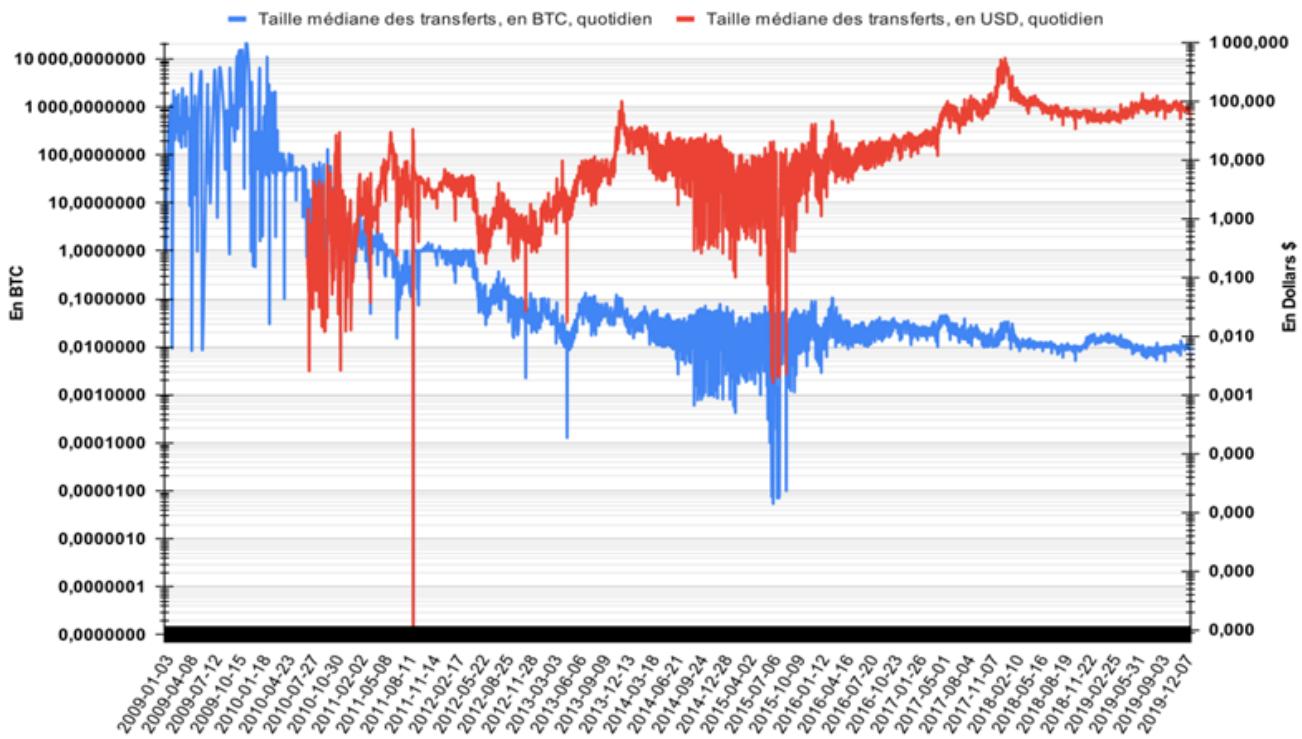
Source des données : <https://www.coinmetrics.io>; traitement de l'auteur.

<sup>(1)</sup> Quantité totale d'UCN transférées (en BTC) et valeur agrégée des transferts (en USD), quotidienne.

<sup>(2)</sup> Quantité moyenne d'UCN transférée (en BTC) et valeur moyenne des transferts (en USD), quotidienne.

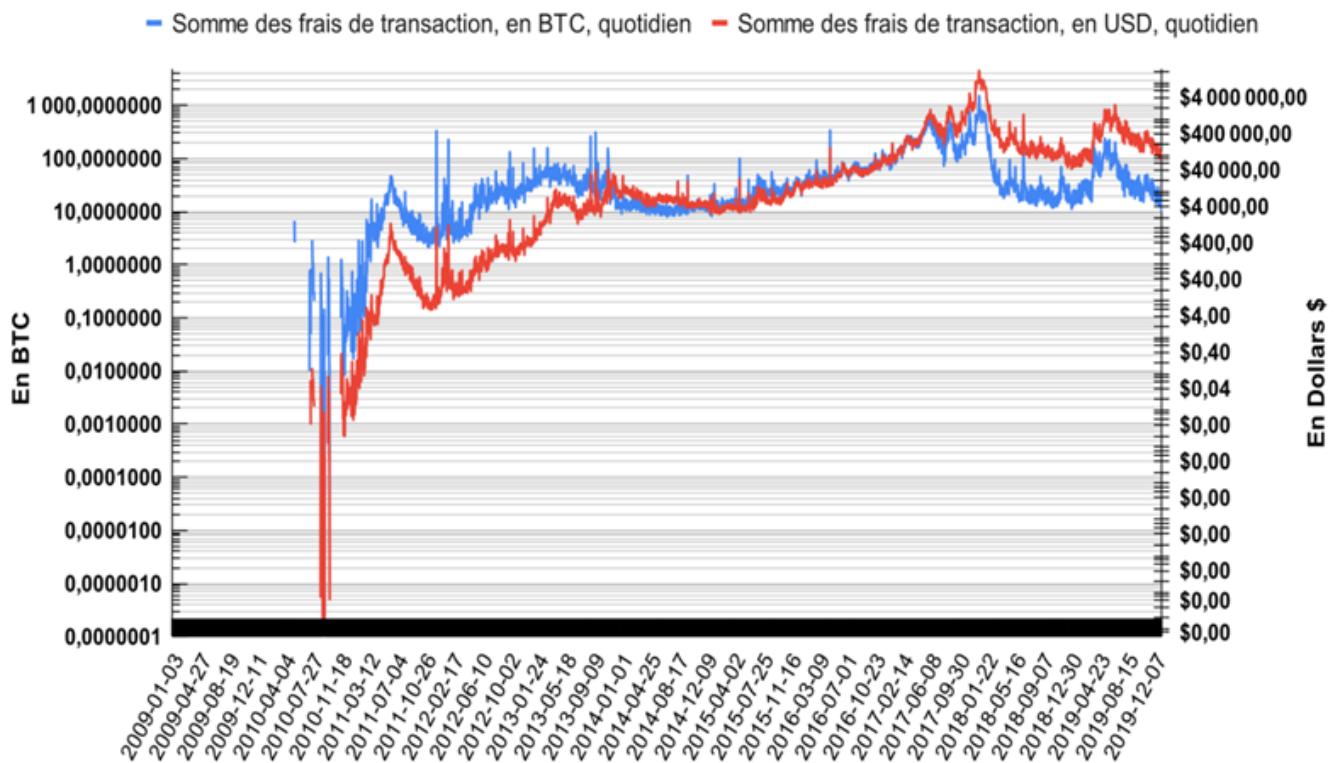
## Annexe II.8 : Taille médiane des transferts, en BTC et USD, quotidien<sup>(1)</sup>

(de janvier 2009 à mars 2019, échelle logarithmique)



## Annexe II.9 : Somme des frais de transaction, en BTC et USD, quotidien<sup>(2)</sup>

(de janvier 2009 à décembre 2019, échelle logarithmique)



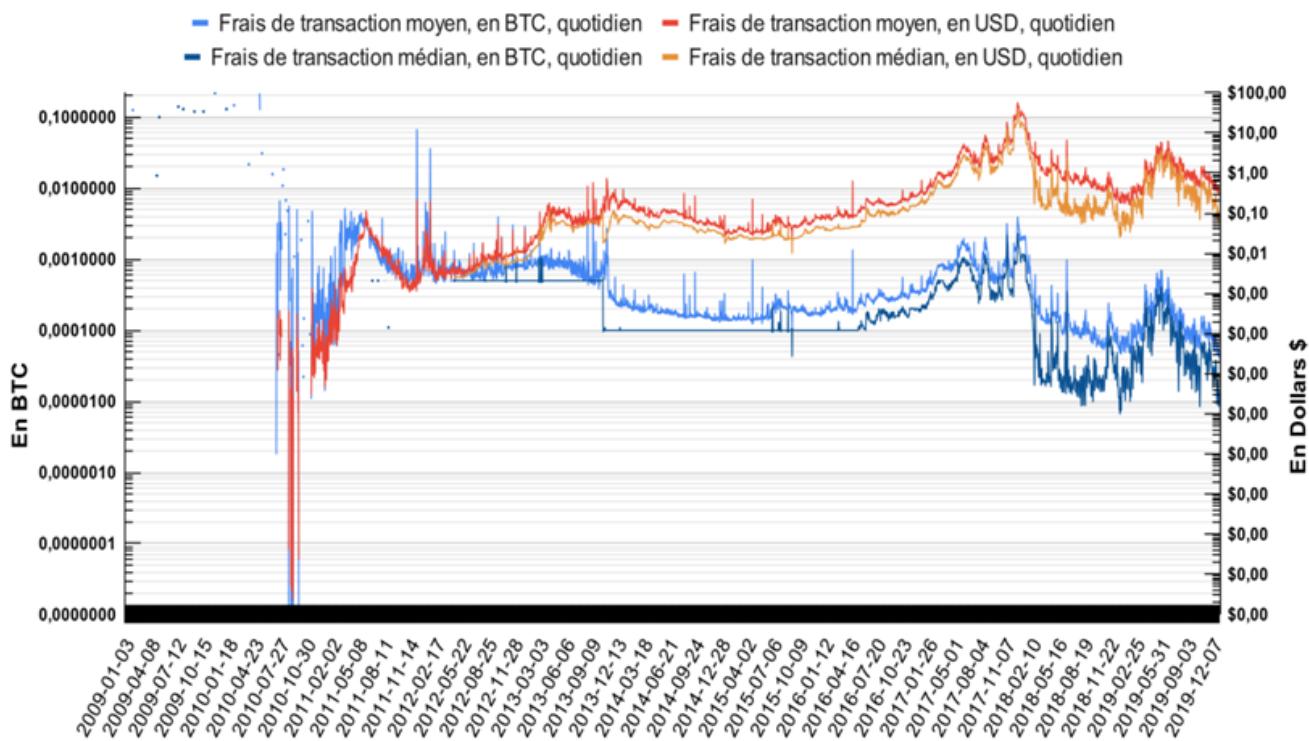
Source des données : <https://www.coinmetrics.io>; traitement de l'auteur.

<sup>(1)</sup> Quantité médiane d'UCN transférée (en BTC) et valeur médiane des transferts (en USD), quotidienne.

<sup>(2)</sup> Somme des frais de transaction reçus par les mineurs, en BTC et USD, quotidien (hors récompenses d'émission monétaire).

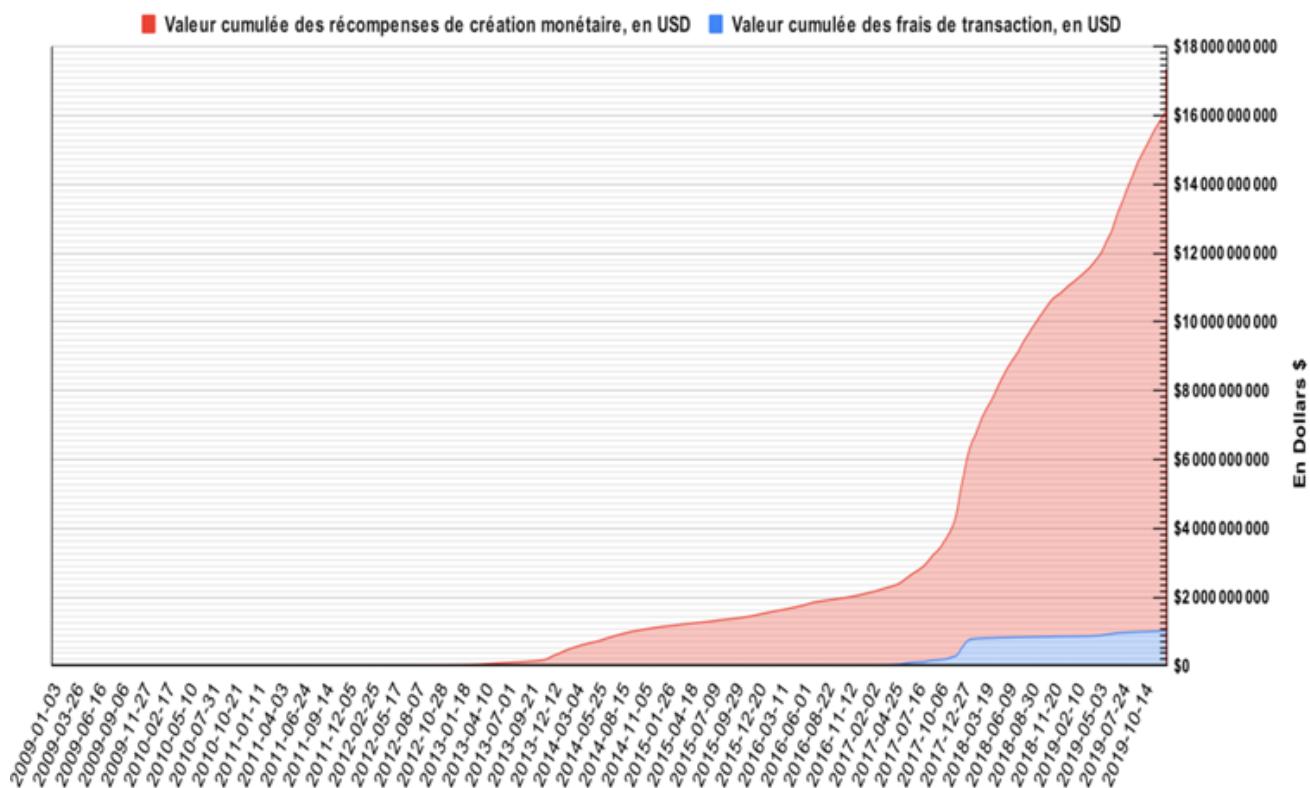
## Annexe II.10 : Frais de transaction, moyen et médian, en BTC et USD, quotidien<sup>(1)</sup>

(de janvier 2009 à décembre 2019, échelle logarithmique)



## Annexe II.11 : Revenu cumulé des « mineurs » en USD<sup>(2)</sup>

(de janvier 2009 à décembre 2019)

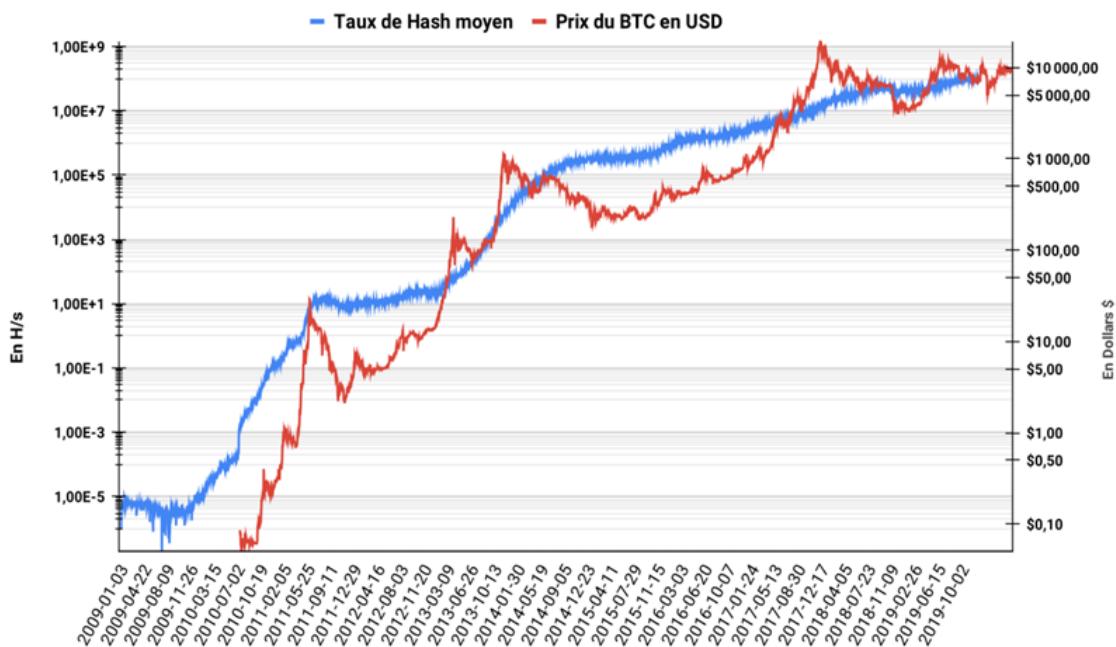


Source des données : <https://www.coinmetrics.io>; traitement de l'auteur.

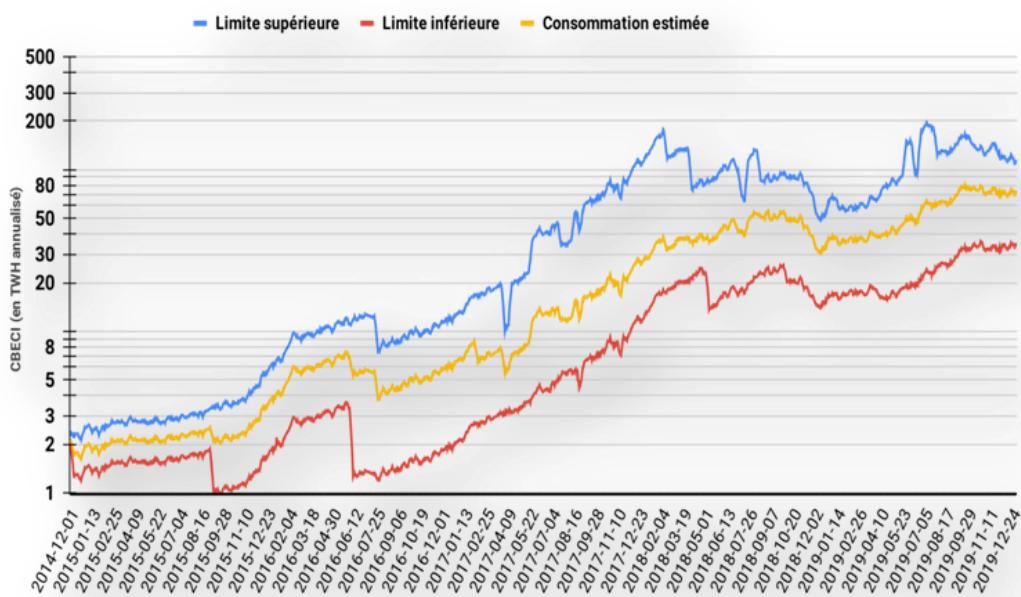
<sup>(1)</sup> Frais de transaction, moyen et médian, en BTC et en USD, quotidien.

<sup>(2)</sup> Valeur cumulée, en USD, des récompenses d'émission monétaire et des frais de transaction perçus par les « mineurs ».

**Annexe II.12 : Quantité Hash/s cumulée<sup>(1)</sup> et prix du BTC, en USD, quotidien**  
 (de janvier 2009 à décembre 2019, échelle logarithmique)



**Annexe II.13 : Évolution de l'index de consommation électrique de Bitcoin, en TWH annualisé<sup>(2)</sup>**  
 (de janvier 2009 à décembre 2019, échelle logarithmique)

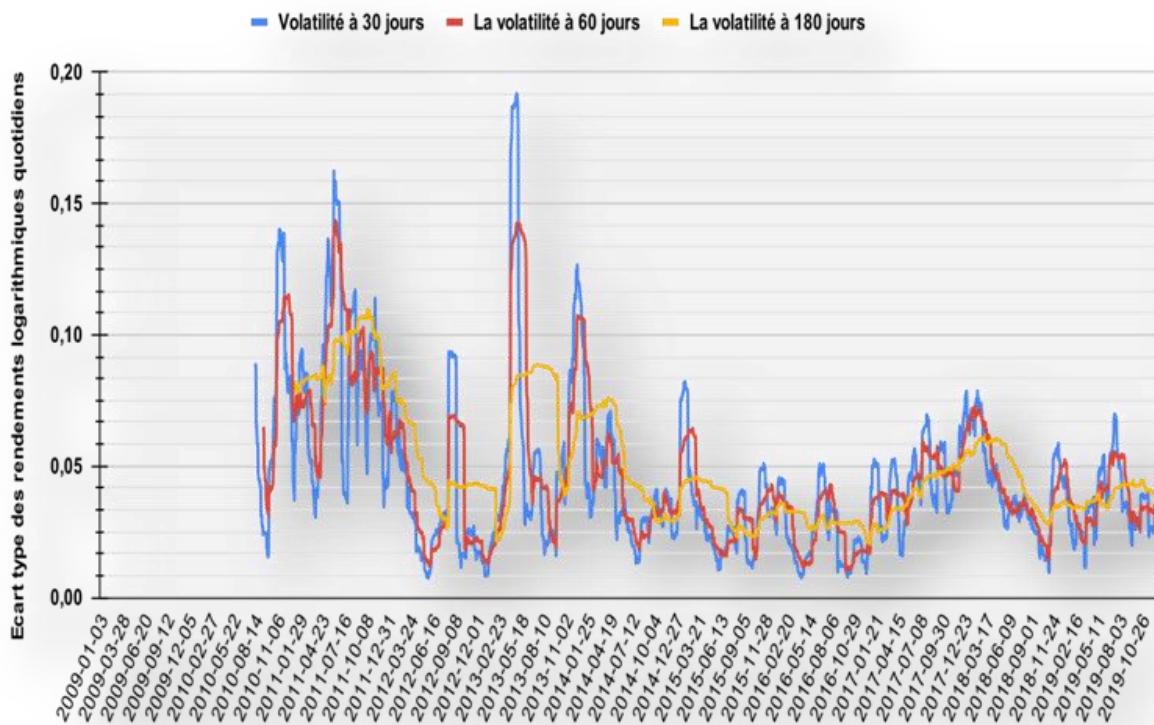


**Source des données :** <https://www.coinmetrics.io>; <https://www.cbeci.org/>; traitement de l'auteur.

<sup>(1)</sup> Taux de Hash moyen et quotidien déployé dans Bitcoin, exprimé en H/s.

<sup>(2)</sup> L'index de consommation électrique de Bitcoin (CBECI publié par Cambridge) : est un indicateur hybride combinant une liste d'équipements de minage type et des hypothèses concernant les seuils de rentabilité déterminant les équipements profitables en fonction du coût de l'électricité. Cela donne trois scénarios : (i) un optimiste (« limite inférieure » ou « *lower bound* »), représentant la limite inférieure, elle correspond au minimum de dépense électrique suivant l'hypothèse que tous les mineurs utilisent l'équipement le plus efficace ; (ii) un pessimiste (« limite supérieure » ou « *upper bound* ») correspondant à la dépense maximale de Bitcoin, suivant l'hypothèse que tous les mineurs utilisent le matériel le moins efficace énergétiquement, tant que l'exploitation de ce matériel reste rentable ; enfin, (iii) un scénario intermédiaire (« consommation estimée » ou « *best guess* »), reposant sur l'hypothèse que les mineurs utilisent un panier de matériel rentable plutôt qu'un modèle unique.

**Annexe II.14 : Volatilité de l'UCN BTC, en USD  
sur 30, 60 et 180 jours<sup>(1)</sup>**  
(de janvier 2009 à mars 2021)



**Source des données :** <https://www.coinmetrics.io>; <https://www.cbeci.org/>; traitement de l'auteur.  
<sup>(1)</sup> Volatilité de l'UCN BTC, en Dollars, calculée comme écart type des rendements logarithmiques naturels quotidiens sur 30, 60 et 180 jours.

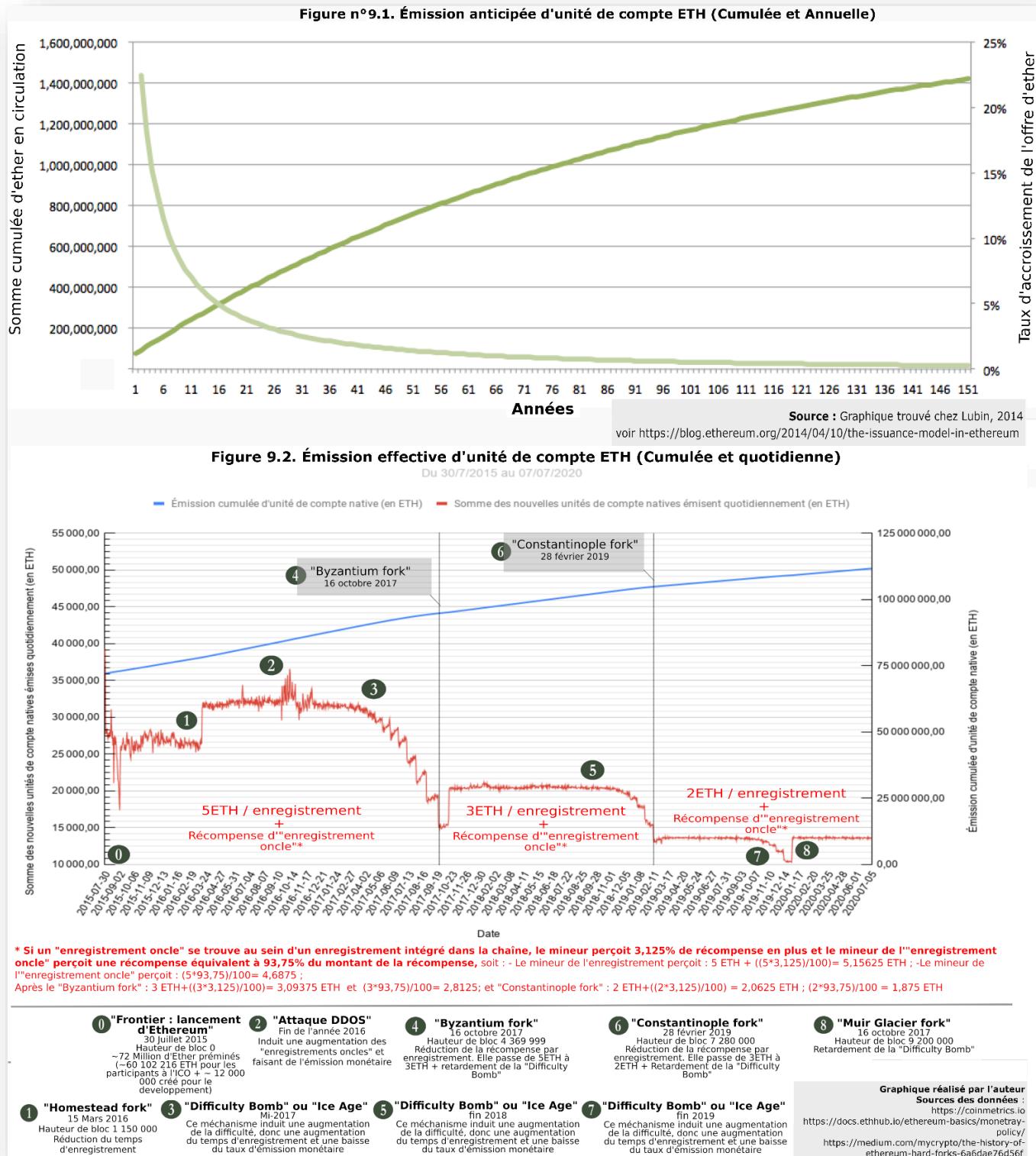
### Annexe III : Données synthétiques relatives à l'écosystème d'Ethereum

Tableau III.1: L'UCN Ether et sa décimalisation (matérielle et symbolique)

| Ethereum et son UCN* Ether  |   |
|---|---|
|   |                 |
|   | <b>ETH</b><br> |
| Unité(s) fractionnaire(s) conventionnelle(s)                            | Valeur en UCN* (ETH)  |
| L'« <i>ether</i> »   l'« <i>ETH</i> »   ou le « <i>Buterin</i> »        | 1<br>(Ou $10^{18}$ Wei)   |
| Le « <i>Milliether</i> »   ou le « <i>Finney</i> »                      | 0.001<br>(Ou $10^{15}$ Wei)   |
| Le « <i>Microether</i> »   ou le « <i>Szabo</i> »                       | 0.000001<br>(Ou $10^{12}$ Wei)  |
| Le « <b>Gwei</b> »   le « <i>Shannon</i> »   ou le « <i>Nanoether</i> » | 0.000000001<br>(Ou $10^9$ Wei)  |

|   |  |
|---|--|
| Le « <b><i>Mwei</i></b> »   le « <i>Lovelace</i> »   ou le « <i>Picoether</i> »   | 0.000000000001<br>(Ou $10^6$ Wei)            |
| Le « <b><i>Kwei</i></b> »   le « <i>Babbage</i> »   ou « <i>Femoether</i> »   | 0.0000000000000001<br>(Ou $10^3$ Wei)        |
| Le « <b><i>Wei</i></b> »   le « <i>Attoether</i> »  | 0.0000000000000000000000000001<br>(Ou 1 Wei) |
| Compilation de l'auteur ; <a href="https://gwei.io/">https://gwei.io/</a> + <a href="https://coinguides.org/ethereum-unit-converter-gwei-ether/">https://coinguides.org/ethereum-unit-converter-gwei-ether/</a> |  |

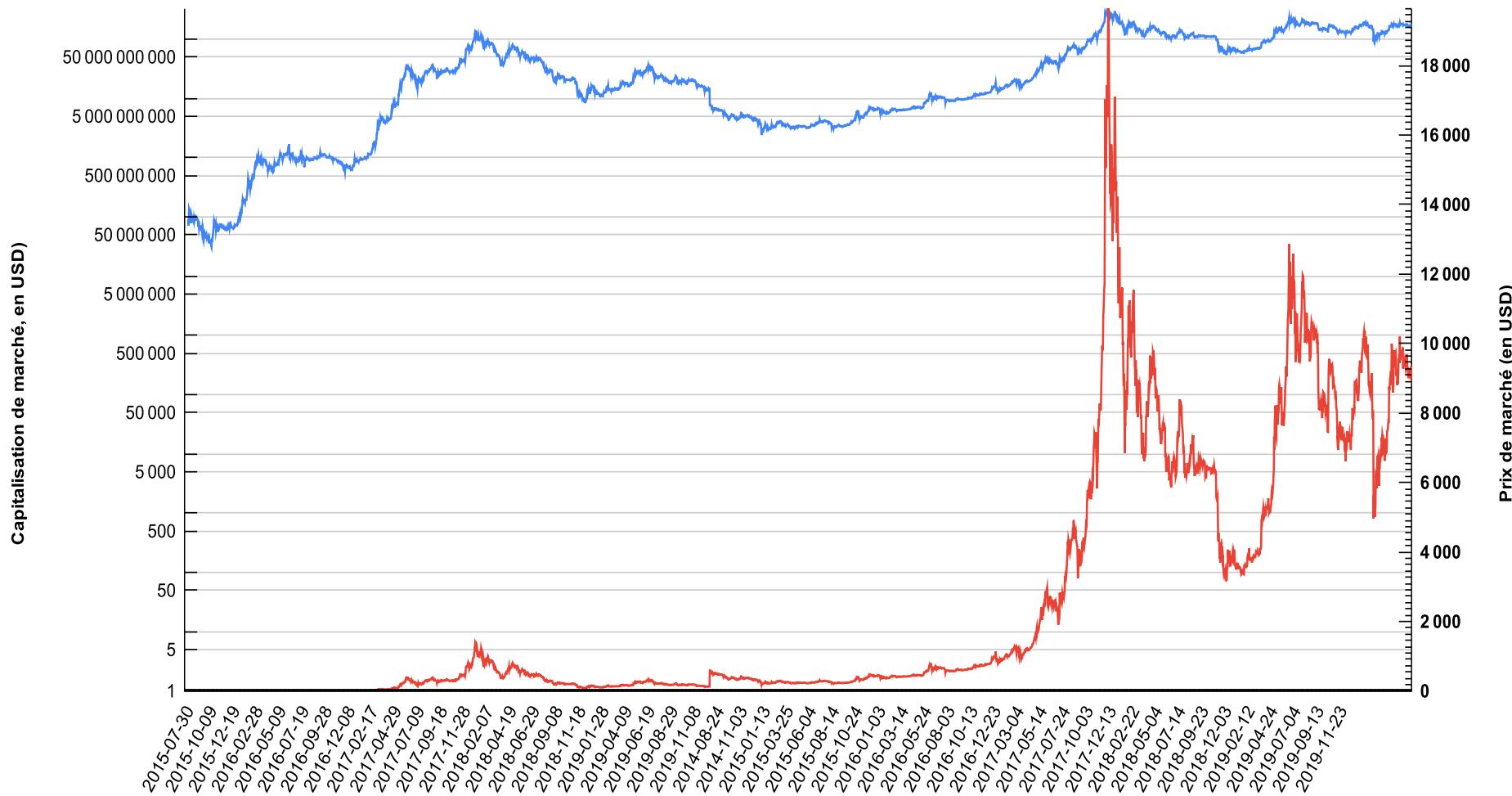
## Annexe III.2 : l'offre monétaire programmatique d'Ethereum : entre émission anticipée et effective



**Figure III.3 : Capitalisation de marché de l'ETH en prix de marché (1), en USD**

(du 30 juillet 2015 au 01 janvier 2020)

— Capitalisation de marché (en USD) — Prix de marché (en USD)



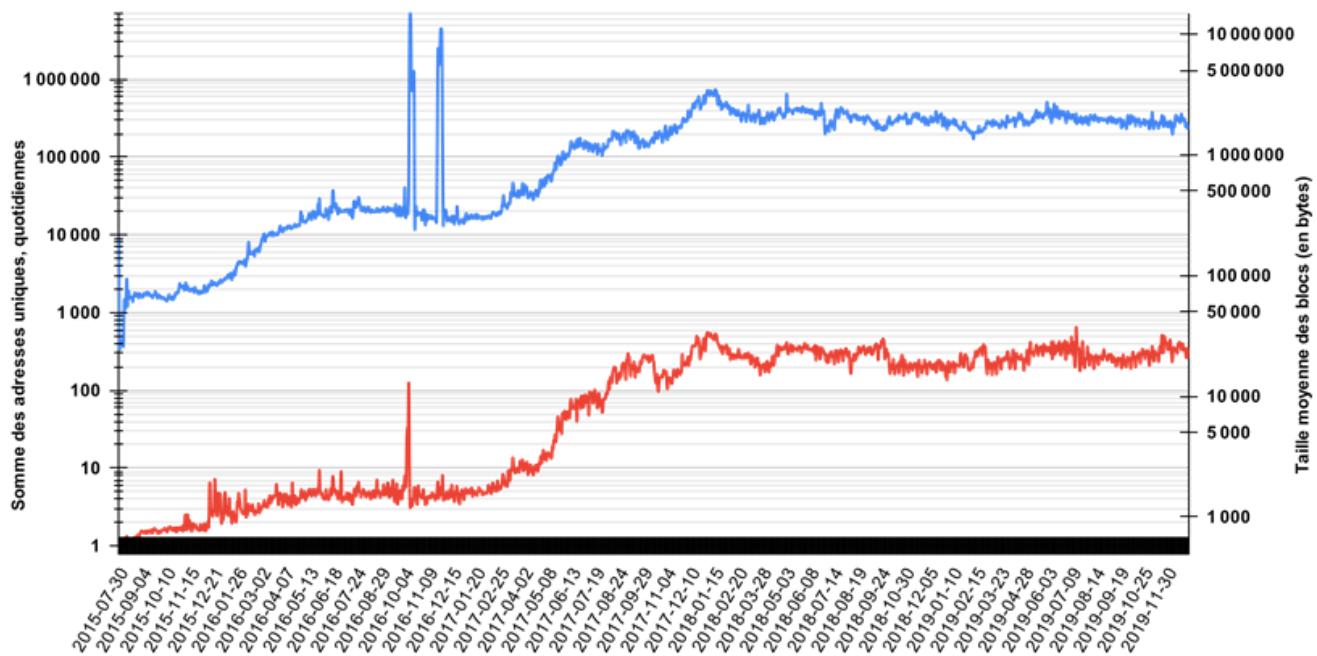
Source des données : <https://www.coinmetrics.io>; (Chapitre 1 pour la 1<sup>ère</sup> cotation) ; traitement de l'auteur.

<sup>(1)</sup> Capitalisation boursière « simple » : valeur agrégée en USD de l'offre actuelle, également appelée « valeur du réseau » ou « capitalisation du marché ».

## Annexe III.4 : Nombre d'adresses actives<sup>(1)</sup> et taille moyenne des enregistrements (en bytes), quotidien

(de juillet 2015 à décembre 2019, échelle logarithmique)

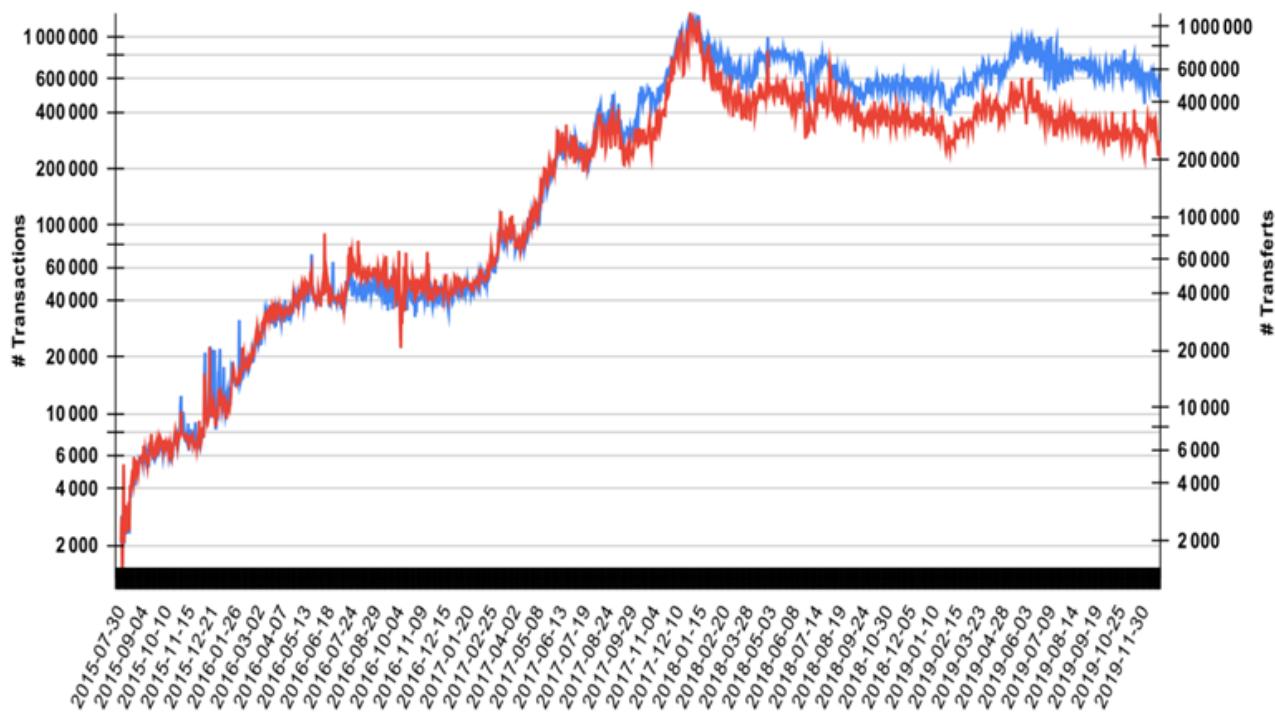
— Somme des adresses uniques, quotidienne — Taille moyenne (en bytes) des blocs créés, quotidienne



## Annexe III.5 : Nombre de transactions<sup>(2)</sup> et transferts<sup>(3)</sup> quotidiens

(de juillet 2015 à décembre 2019, échelle logarithmique)

— Somme des transactions quotidiennes — Somme des transferts d'UCN quotidienne



Source des données : <https://www.coinmetrics.io>; traitement de l'auteur.

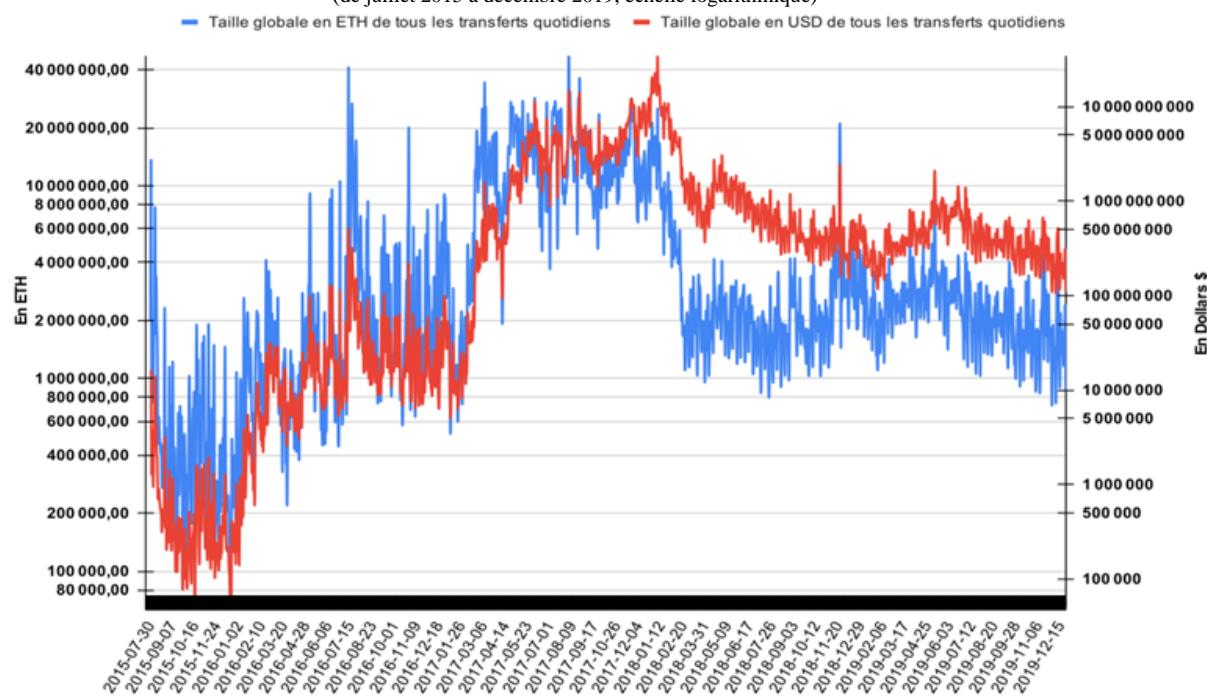
<sup>(1)</sup> Somme des adresses uniques actives quotidiennes (destinataires et envoyeurs, chaque adresse n'est comptée qu'une fois).

<sup>(2)</sup> Somme des transactions quotidiennes (exécutées ou non et avec transfert d'UCN ou non), hors transactions protocolaires.

<sup>(3)</sup> Somme des transferts quotidiens : mouvements d'UCN d'une adresse à une autre, résultants d'une transaction et qui ont une valeur positive.

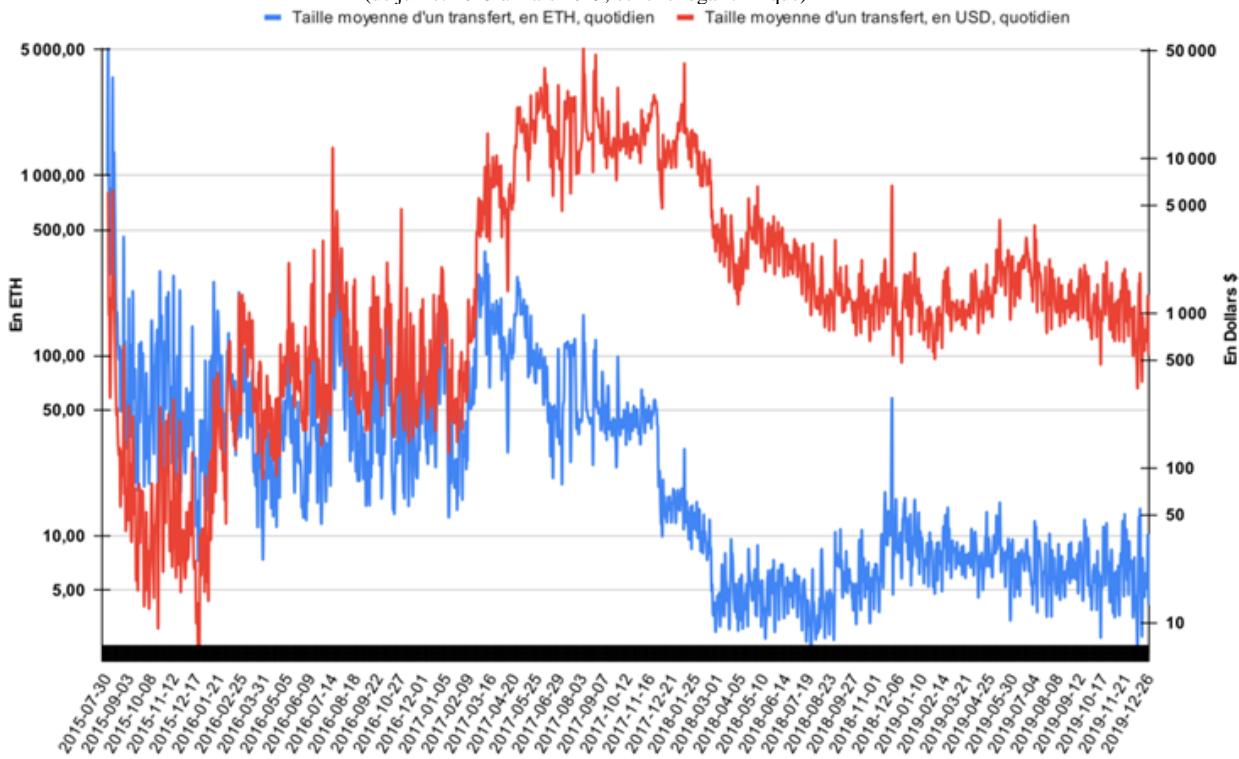
### Annexe III.6 : Taille globale de tous les transferts quotidiens, ETH et USD<sup>(1)</sup>

(de juillet 2015 à décembre 2019, échelle logarithmique)



### Annexe III.7 : Taille moyenne des transferts, en ETH et USD, quotidien<sup>(2)</sup>

(de juillet 2015 à mars 2019, échelle logarithmique)



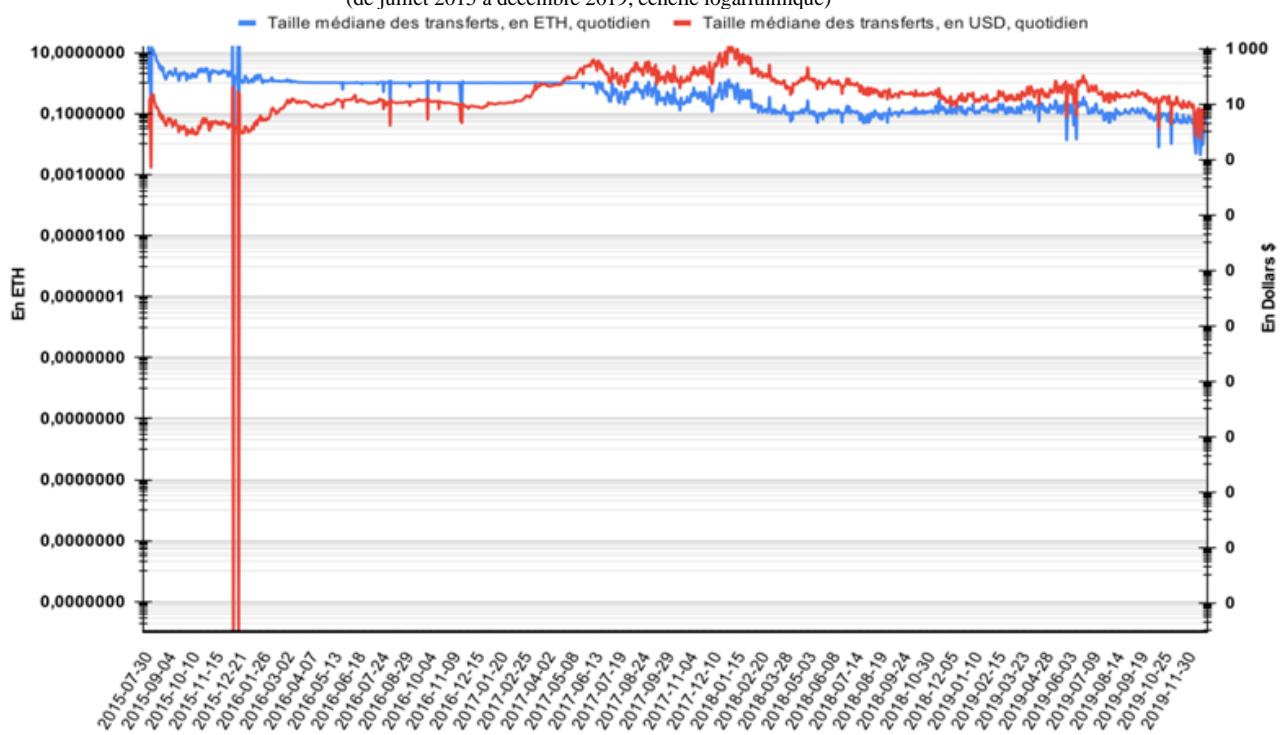
Source des données : <https://www.coinmetrics.io>; traitement de l'auteur.

<sup>(1)</sup> Quantité totale d'UCN transférées (en ETH) et valeur agrégée des transferts (en USD), quotidienne.

<sup>(2)</sup> Quantité moyenne d'UCN transférée (en ETH) et valeur moyenne des transferts (en USD), quotidienne.

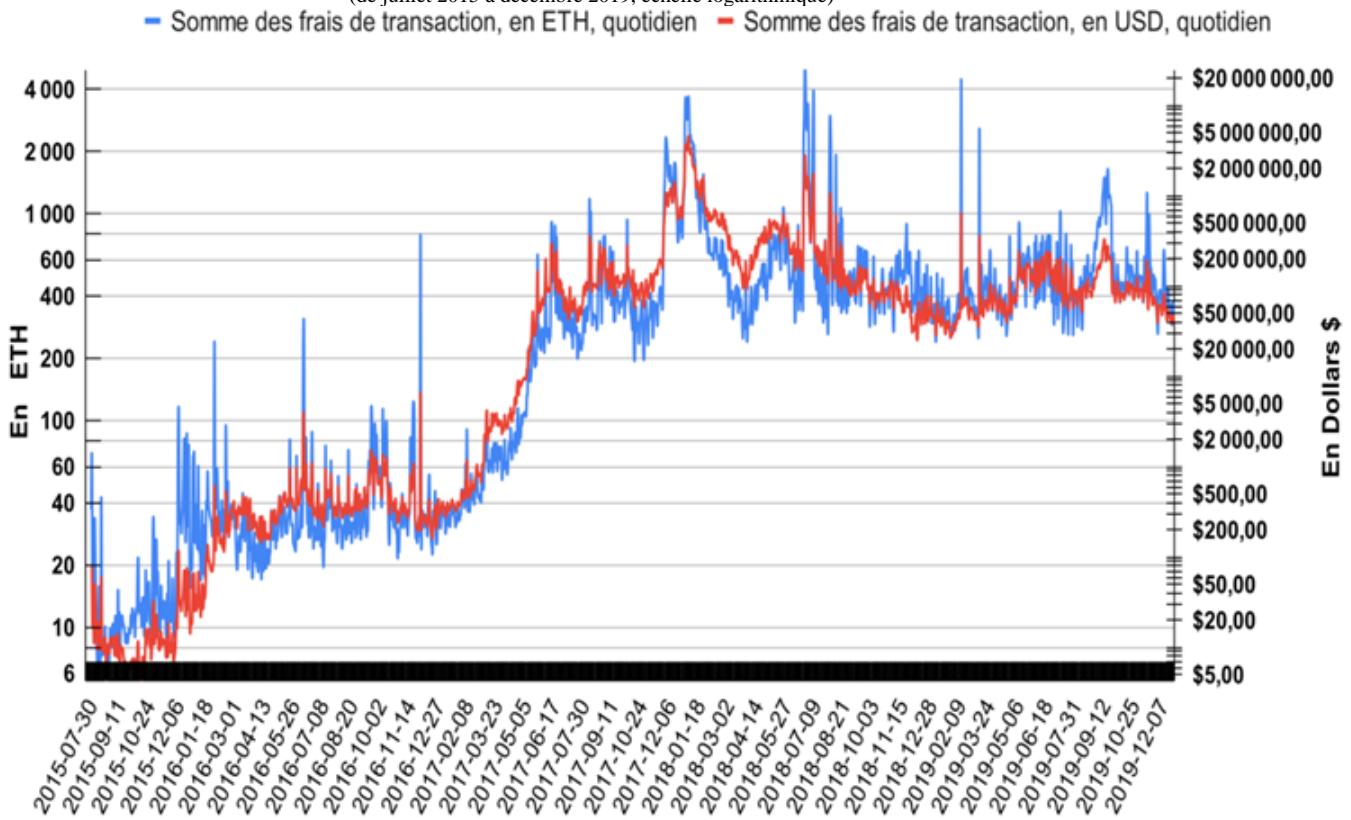
### Annexe III.8 : Taille médiane des transferts, en ETH et USD, quotidien<sup>(1)</sup>

(de juillet 2015 à décembre 2019, échelle logarithmique)



### Annexe III.9 : Somme des frais de transaction, en ETH et USD, quotidien<sup>(2)</sup>

(de juillet 2015 à décembre 2019, échelle logarithmique)



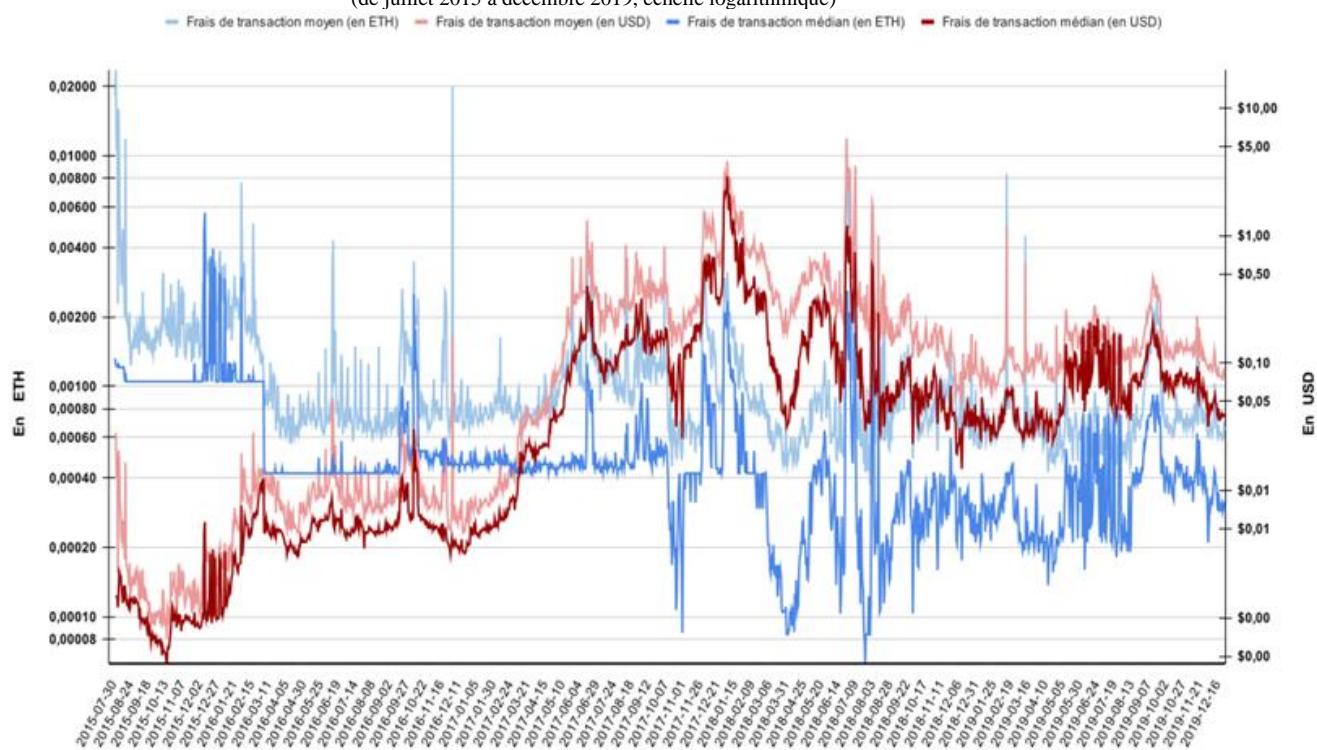
**Source des données :** <https://www.coinmetrics.io>; traitement de l'auteur.

<sup>(1)</sup> Quantité médiane d'UCN transférée (en ETH) et valeur médiane des transferts (en USD), quotidienne.

<sup>(2)</sup> Somme des frais de transaction reçus par les mineurs, en ETH et USD, quotidien (hors récompenses d'émission monétaire).

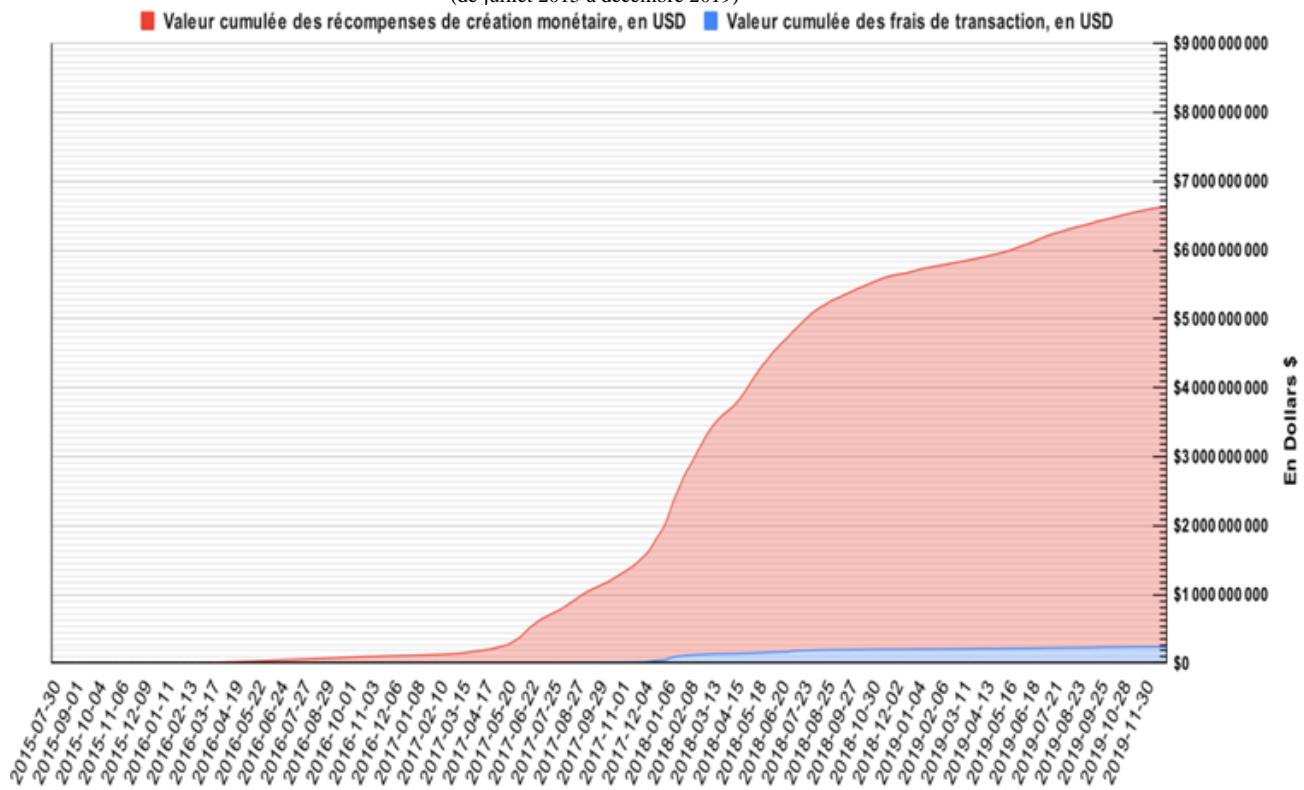
### Annexe III.10 : Frais de transaction, moyen et médian, en ETH et USD, quotidien<sup>(1)</sup>

(de juillet 2015 à décembre 2019, échelle logarithmique)



### Annexe III.11 : Revenu cumulé des « mineurs » en USD<sup>(2)</sup>

(de juillet 2015 à décembre 2019)



**Source des données :** <https://www.coinmetrics.io>; traitement de l'auteur.

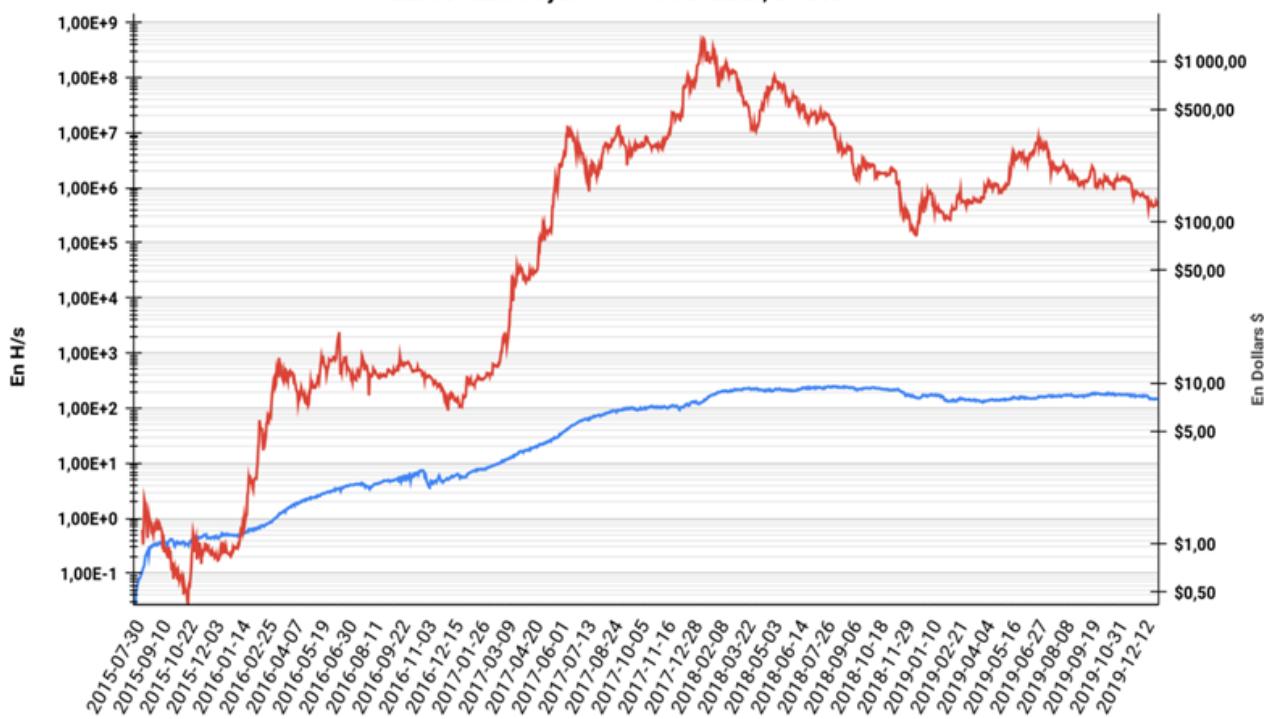
(1) Frais de transaction, moyen et médian, en ETH et en USD, quotidien.

(2) Valeur cumulée, en USD, des récompenses d'émission monétaire et des frais de transaction perçus par les « mineurs ».

### Annexe III.12 : quantité Hash/s cumulée<sup>(1)</sup> et prix de l'ETH en USD, quotidien

(de juillet 2015 à décembre 2019, échelle logarithmique)

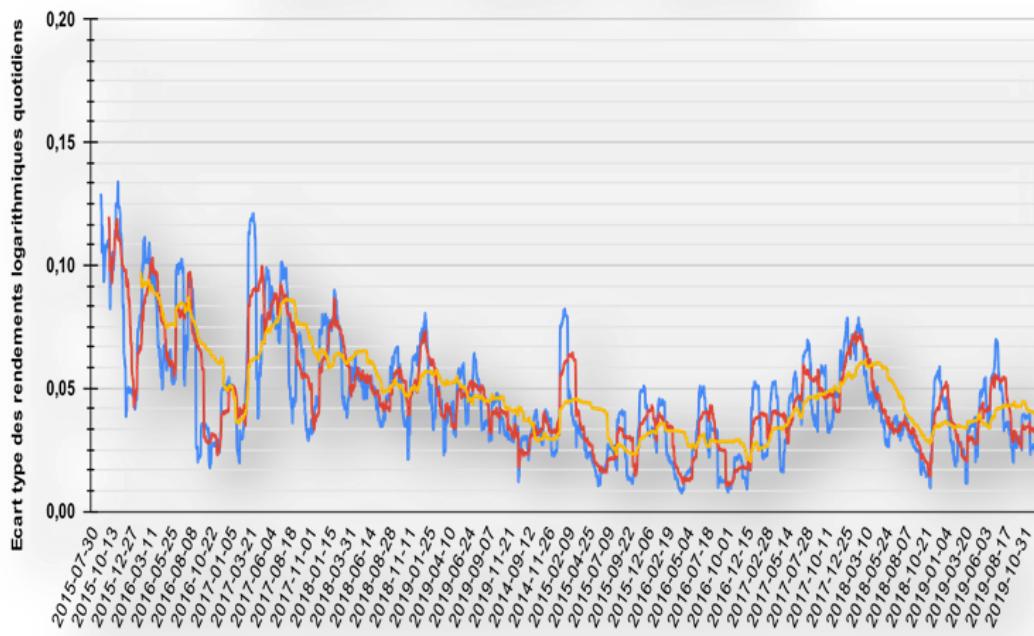
— Taux de Hash moyen — Prix de l'Ether, en USD



### Annexe III.13 : Volatilité de l'UCN ETH, en USD sur 30, 60 et 180 jours<sup>(2)</sup>

(de juillet 2015 à décembre 2019, échelle logarithmique)

— Volatilité à 30 jours — La volatilité à 60 jours — La volatilité à 180 jours



Source des données : <https://www.coinmetrics.io>; <https://www.cbeci.org/>; traitement de l'auteur.

<sup>(1)</sup>. Taux de Hash moyen et quotidien déployé dans Ethereum, exprimé en H/s.

<sup>(2)</sup>. Volatilité de l'UCN ETH, en Dollars, calculée comme écart type des rendements logarithmiques naturels quotidiens sur 30, 60 et 180 jours.

Concernant l'absence de données sur la consommation électrique d'Ethereum : si un index similaire à celui de Bitcoin est aujourd'hui disponible (voir <https://ccaf.io/cbsni/ethereum>, consultation au 05-02-2022), ces données ne couvrent pas la période qui est là notre. De fait, suivant qu'Ethereum a été conçu pour être à l'origine résistant aux ASICS (ils n'apparaîtront que tardivement), la méthodologie de cet indicateur a rendu difficile l'établissement d'une liste de machines de minage type (puisque n'importe quelle carte graphique d'ordinateur, même peu efficace, pouvait être utilisée initialement comme scénario type).

### Annexe III.14 : Les cofondateurs d'Ethereum

| Co-fondateur<br>d'Ethereum   | Biographie synthétique   |
|--|--|
| Vitalik Buterin<br> | <p><i>Sources : Bradbury 2013; Munawa 2016; Summerwill 2018; Russo 2020; Hamacher 2020, synthèse de l'auteur</i></p> <p>Il découvre Bitcoin en 2011, grâce à son père informaticien, Dmitry Buterin, alors qu'il n'a que 17 ans et est encore en études au Canada. Son intérêt pour Bitcoin le fera quitter ses études afin de se consacrer à temps plein à ses activités autour des CM. Féru de mathématique et d'informatique, il remporte en 2012 la médaille de Bronze des Olympiades Internationales d'informatique, reçoit en 2014 la bourse "Thiel fellowship" et, en 2018, reçoit à titre honorifique un doctorat en Commerce et Économie de l'Université de Bâle. Il va participer à Bitcoin en tant que programmeur - il a participé à différents projets (<i>darkwallet</i>, <i>KryptoKit</i>, <i>Fork</i>* de <i>bitcoinjs-lib</i>, <i>pybitcointools</i>, <i>multisig.info</i>, <i>Egora</i>, etc.) et auteur. En effet, avec Mihai Alisie, il co-fonde <i>Bitcoin Magazine</i> en 2012. Il travaille aussi sur la technologie des pièces colorées et sur Omni/Mastercoin. Depuis 2013, il travaille sur le développement Ethereum.</p> |
| Mihai Alisie<br>   | Diplômé en économie cybernétique à l'université de Lucian Blaga, Roumanie. A été coach et joueur de poker avant de découvrir Bitcoin en 2011. Suivant sa prise de contact avec V. Buterin, ils co-fondent <i>Bitcoin Magazine</i> . M. Alisie travaille sur une plateforme de vente en ligne dédiée à Bitcoin (Egora). Il va prendre part aux activités légales et administratives : installation en Suisse de la fondation Ethereum, ouverture de compte en banque, etc. Vice-président de la Fondation Ethereum jusqu'en 2015, il la quitte pour se consacrer à un nouveau projet, Akasha.   |

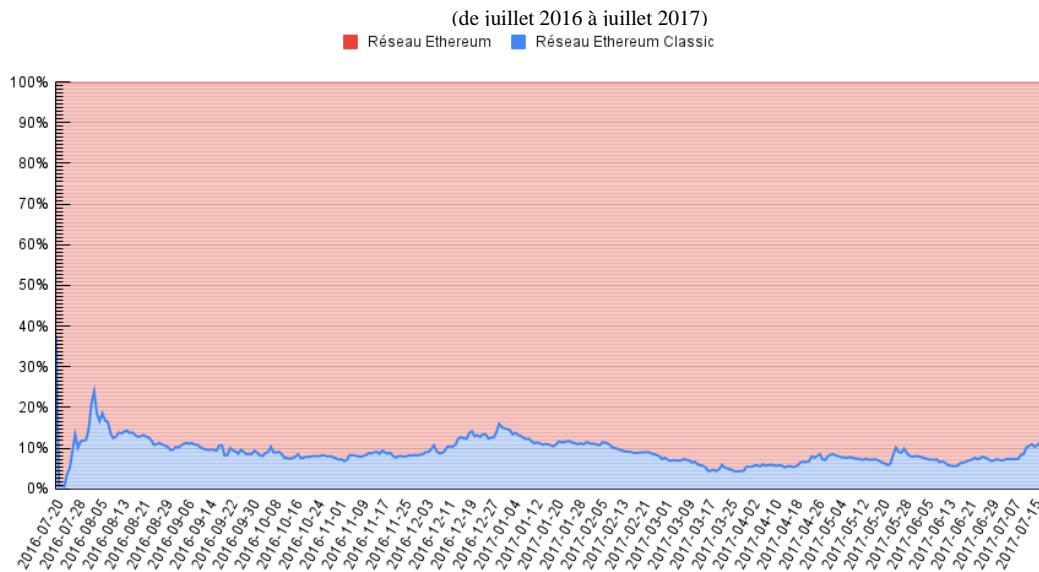
|  |   |
|--|---|
| Antony Di Iorio<br>   | <p>Investisseur et entrepreneur, il est au contact de l'informatique depuis son plus jeune âge. Il obtient un diplôme en Management du Business à l'université de Ryerson. Disposant d'un capital économique familial important, il commence par être investisseur dans une entreprise de forage géothermique avant de découvrir Bitcoin. Il est l'organisateur, en novembre 2012, des premiers "Bitcoin Meetup" à Toronto, au sein desquels il rencontre V. Buterin. Il fonde l'organisation "Bitcoin Alliance Canada", comme le site de jeux en ligne "Satoshi Circle" qu'il revend en 2013. Il est en contact avec Hoskinson, qui a réalisé un programme éducatif autour de Bitcoin pour "Bitcoin Alliance Canada" : c'est lui qui lui transmettra la première version du projet. Du fait de son capital économique, il investit largement dans Ethereum, et plus largement dans cet écosystème. Il est CEO de "Decentral" (une bourse d'échange de CM canadienne) et de Jaxx (un service des premiers portefeuilles* multi-CM). Peu favorable au statut d'organisation à but non lucratif de la fondation, il se met en retrait du projet suite à cette décision.</p>   |
| Charles Hoskinson<br> | <p>Mathématicien et entrepreneur, il a étudié la théorie analytique des nombres à l'université de Denver et de Colorado. Après un détour en politique comme bénévole de la campagne du candidat libertarien Ron Paul, il découvre Bitcoin en 2011. Intéressé par ses potentiels, il souhaite développer le premier DEX - "Decentralized Exchange", une bourse d'échange en P2P - pour les CM. En octobre 2013, cette idée aboutira au lancement, avec Dan Larimer, d'un protocole de registre* distribué <i>ad hoc</i>, "BitShare" dont Hoskinson est CEO et Larimer CTO. Ils développeront ensemble les concepts de "Distributed Autonomous Company" (DAC), ouvrant la voie à celui - central pour Ethereum aujourd'hui - des "Decentralized Autonomous Organisation" (DAO). En opposition avec Larimer, il quittera Bitshare au début 2014. On lui doit aussi l'établissement du "Cryptocurrency Research group" en septembre 2013 et la création du Comité éducation de la fondation Bitcoin, en août de la même année. Introduit à Ethereum et à Buterin par A. Di Iorio, il participe à son lancement. Son rôle principal sera la création de la fondation Ethereum, dont il sera nommé CEO en décembre 2013. Comme Di Iorio, il est opposé au fait que la fondation soit dotée d'un statut d'organisation non lucrative, ce qui conduit à des conflits avec les autres cofondateurs. Cela se traduira par son éviction en juin 2014.</p> <p>Il fondera avec Jeremy Wood, un ancien d'Ethereum, la société IOHK en 2015, dont il devient CEO. Opposé au Hard Fork* consécutif au Hack de "The Dao", il prendra part au projet Ethereum Classic (Ticker : ETC), né de la scission communautaire consécutive à la gestion de la crise. Il est aussi le fondateur du protocole de registre* distribué "concurrent" d'Ethereum Cardano (Ticker : ADA).</p> |

|   |  |
|---|--|
| Gavin Wood<br>   | <p>Programmeur informatique et entrepreneur, il étudie la science informatique à l'université de York, où il obtient un doctorat en visualisation musicale. Passionné d'informatique et de jeux vidéo depuis son plus jeune âge, il est contributeur du mouvement des logiciels libres.</p> <p>Il découvre Bitcoin dans une vidéo avec Taaki et Alisie. C'est grâce à Taaki et une autre figure reconnue de la communauté, Johnny Bitcoin, qu'il est introduit au d'Ethereum. Il rencontrera Buterin, lui proposera d'implémenter le premier client Ethereum en langage C++, et sera le WP* premier à mettre en place un réseau* "testnet" Ethereum fonctionnel, ce qui lui permet de prendre une place, malgré quelques réticences, dans l'équipe des fondateurs. En avril 2014, il publie le <i>Yellow Paper</i>, qui vise à être une traduction du WP* de Buterin posant les spécifications techniques du protocole, de son réseau* et de l'<i>Ethereum Virtual Machine</i>. Il est aussi celui qui développa le langage de programmation* natif d'Ethereum : "Solidity". Il est CTO de la fondation Ethereum jusqu'en 2016 ; CEO de Parity technology, qui développe un client logiciel Ethereum codé en langage Rust ; fondateur de la "Web3 Fondation" et du projet de protocole de registre* distribué "concurrent" d'Ethereum Polkadot (Ticker : DOT).</p> |
| Amir Chetrit<br> | <p>Il a rencontré Buterin en 2013 lors d'une conférence Bitcoin et a travaillé pour la start-up Colored Coin, projet auquel a participé Buterin.</p> <p>Dès juin 2014, critiqué pour son manque de participation par les autres co-fondateurs et développeurs*, ayant proposé de se retirer, il est évincé comme Hoskinson.</p>  |

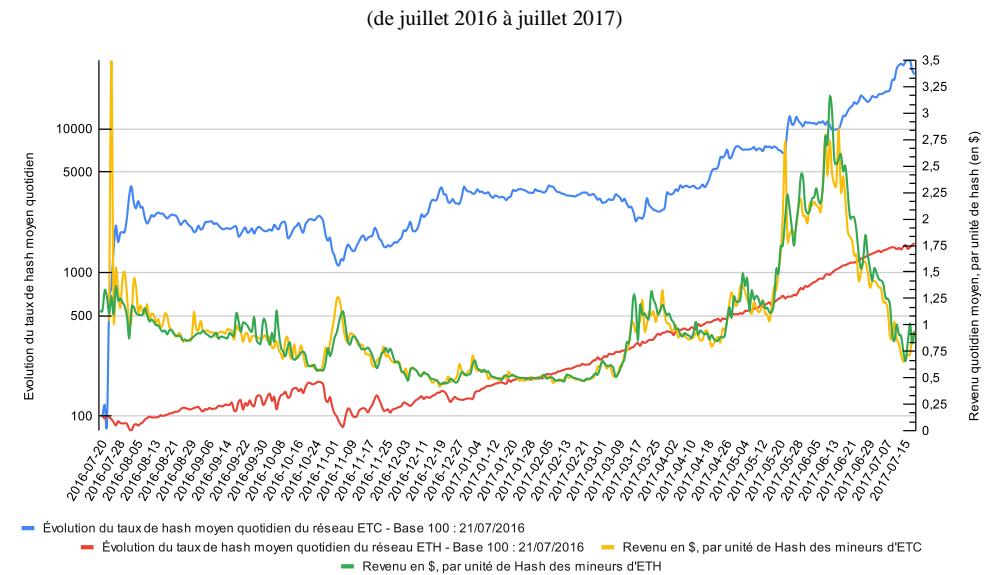
|   |  |
|---|--|
| Jeffrey Wilcke<br> | <p>Programmeur informatique néerlandais qui avait travaillé pour le projet Mastercoin/Omni avant de s'intéresser à Ethereum. Motivé par ce projet, il réalise une implémentation logicielle en langage de programmation* Go, ce qui lui doit d'être ajouté à la liste des co-fondateurs - avec Wood - au début 2014.</p> <p>Ce premier client en Go - logiciel baptisé "Geth" aujourd'hui -, qui a été réalisé en même temps et sans concertation avec le développement du client en C++, impliqua qu'Ethereum eut, dès le départ, deux implémentations logicielles différentes et compatibles. Son retrait du projet Ethereum ferait suite aux nombreuses crises qu'Ethereum a pu traverser - la résolution de la crise de "The Dao Hack" par un Hard Fork* controversé, série d'attaques informatiques, etc. - et à des choix plus personnels. À son départ, il confie le développement du logiciel Geth à Peter Szilagyi, qui est encore aujourd'hui le développeur* principal du client Geth. Il travaille aujourd'hui avec son frère pour son propre studio de développement de jeux vidéo, qu'il a financé grâce à la vente d'une partie des Ether reçus pour sa participation au projet.</p>  |
| Joseph Lubin<br>   | <p>Détenteur d'un diplôme de génie électrique et informatique obtenu à Princeton, sa carrière va du génie logiciel à la production musicale, en passant par les affaires et la finance (Goldman Sachs's Private Wealth Management, BackSmith, co-fondateur d'un hedge fund). À Princeton, il a vécu en colocation avec Michael Novogratz, qui, à partir de 2015, sera connu - avec sa société Galaxie Digitale - pour ses activités d'investissement dans le secteur des CM. Il s'intéresse aux CM et prend contact avec son compatriote A. Di Iorio par le biais de la "Bitcoin Alliance of Canada". C'est lors de "<i>Bitcoin meetup</i>" à Toronto qu'il rencontre Buterin. Disposant d'un capital économique, il va avec Di Iorio assurer le financement du jeune projet. Si le choix a été fait de doter la fondation Ethereum - en charge du développement du projet - du statut d'organisation à but non lucratif, et suivant le fait que Lubin envisageait dès le départ que la couche applicative sur Ethereum devait être liée à une logique lucrative, il fonde l'entreprise "Consensys" dès 2014, qui joue un rôle de premier plan dans le financement et l'incubation de start-ups du secteur Blockchain. Lubin, va ainsi jouer un rôle clé dans le démarchage de partenaires d'Ethereum, tels que JPMorgan, CME Group, BNY Mellon, Credit Suisse, Banco Santander, BBVA, ING, UBS, BP, Intel et Microsoft. Le 28 février 2017, "Consensys" fait partie - comme Accenture, Banco Santander, BlockApps, BNY Mellon, CME Group, ConsenSys, IC3, Intel, J.P. Morgan, Microsoft, BBVA, BP, Crédit Suisse, Fubon Financial, ING, Monax, Tendermint, Thomson Reuters, UBS, etc. - des membres fondateurs de l' "Entreprise Ethereum Alliance", une organisation visant à promouvoir le développement d'Ethereum pour les entreprises.</p> |

Annexe III.15 Ethereum Versus Ethereum Classic

*Annexe III.15.1 : Répartition du taux de Hash moyen entre ETH et ETC, quotidien<sup>(1)</sup>*

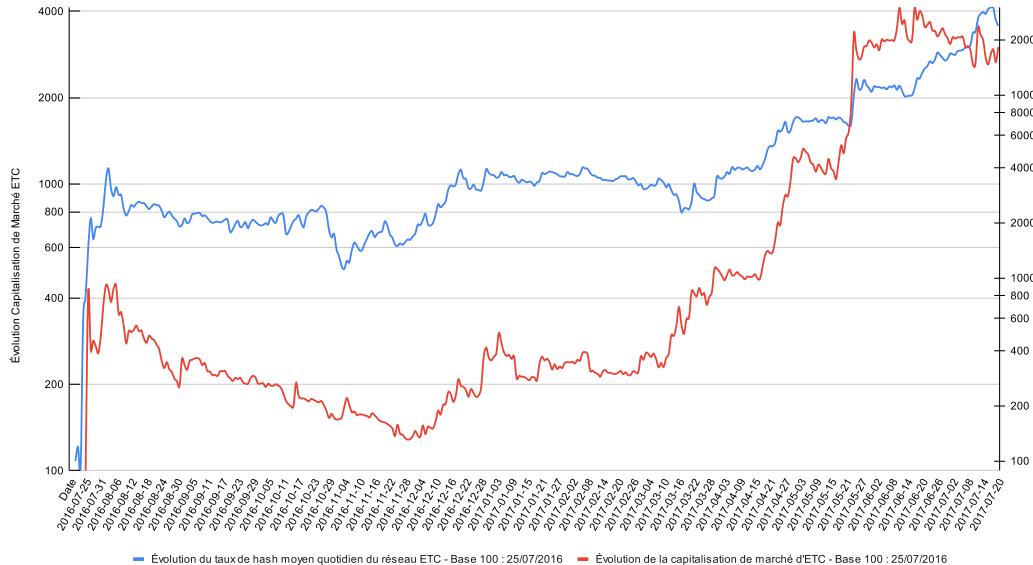


*Annexe III.15.2 : Miner de l'ETH ou de l'ETC : un dilemme philosophique et économique<sup>(2)</sup>*



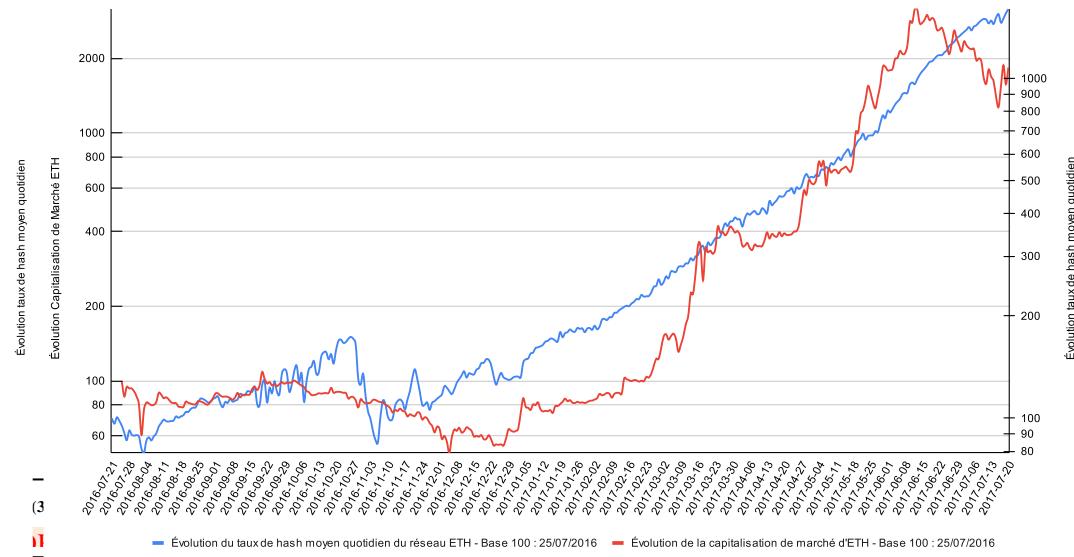
*Annexe III.15.3 : Évolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum Classic<sup>(3)</sup>*

(de juillet 2016 à juillet 2017, échelle logarithmique)



*Annexe III.15.4 : Évolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum<sup>(4)</sup>*

(de juillet 2016 à juillet 2017, échelle logarithmique)



## Annexe IV: Données synthétiques relatives à nos stratégies et dispositifs d'accès au terrain

### Annexe IV.2 : Détails des immersions participantes

Il serait impossible et fastidieux de réaliser une liste exhaustive de nos différentes expériences en ligne – *on chain\** et *off chain\** - ; aussi, ce tableau vise à ramasser certaines des expériences clefs, tout en soulignant les compétences impliquées acquises et/ou mobilisées.

| Période  | Type d'activité                    | CM impliquée et type d'interaction en ligne | Connaissance(s) impliquée(s)   |
|----------|------------------------------------|---|--|
| Fin 2015 | Création d'un portefeuille Bitcoin | Bitcoin<br><br>Hors-protocole*              | Initiation aux principes de base du fonctionnement du Bitcoin, tels que la génération et la gestion des clés privées et publiques, la création et la diffusion des transactions*, la notion d'UTXO*, etc., via la découverte du portefeuille Electrum : téléchargement via Internet, installation du logiciel client ; création d'une adresse Bitcoin et sécurisation de la « seed » (sur papier) ; réception et envoi de BTC ; découverte des UTXO* et de leur implication en termes de frais de transaction* pour les transactions* futures (voir infra « Faucet »). |

|                      |  |  |   |
|----------------------|--|--|---|
| Fin<br>2015-<br>2016 | Obtention de nos premières UCN* via “Faucet” | Bitcoin et autres Hors-protocole* et au sein du protocole* | <p>Obtention des premières UCN* <i>via</i> site de micro-dons (les « faucets ») et compréhension pratique de la gestion des UTXO* ; exploration de l'écosystème crypto-monétaire avec ses différents types de CM (générations, caractéristiques, usages, etc.) ; compréhension des enjeux liés à l'interopérabilité, à la scalabilité, à la sécurité, etc. ; sensibilisation aux aspects communautaires, économiques, culturels, éthiques, etc. des différentes CM.</p> <p>Premières transactions* vers notre portefeuille Bitcoin : effet « whaou », suivant la découverte du suivi en temps réel, du traitement de la transaction* en ligne <i>via</i> un explorateur de Blockchain, visualisation des confirmations participant de la finalisation conventionnelle du transfert ; découverte de la traçabilité des UTXO* utilisées depuis leur origine (cf. transaction* <i>coinbase</i> qui les ont émises) ; appréhension pratique du mécanisme des frais de transaction* et de la structure des UTXO* qui constituent les fonds de son portefeuille : certains sites permettent d'accumuler les récompenses <i>off chain</i>*, d'autres transfèrent directement les fonds <i>on chain</i>*, à chaque action réalisée. Les premiers évitent, au prix d'une centralisation, les coûts induits par ces micro-paiements : directement, car chaque micro-paiement doit s'acquitter de frais forcément élevés rapportés à leur valeur propre et indirectement, car recevoir une multitude d'UTXO* de faible valeur se traduit à l'avenir par des transactions* lourdes, donc chères, car constituées d'un grand nombre d'UTXO* de petit montant (d'où l'appellation de « dust » pour les UTXO* plus couteux à récupérer que ce qu'ils ne valent).</p> <p>Création d'autre portefeuille pour les autres CM et premières transactions*, appréhension des points communs et des différences d'architecture (temps d'enregistrement*, frais de transaction*).</p> |
|----------------------|--|--|---|

|              |  |   |   |
|--------------|--|---|---|
| Janvier 2016 | Teste minage de BTC  | Bitcoin<br><br>Hors-Protocole* : installation d'un client de minage (échec)   | Confrontation aux contraintes matérielles et logicielles du minage de Bitcoin, telles que la puissance de calcul, la consommation électrique, le système d'exploitation, le choix du logiciel, la configuration du réseau*, etc. : échec lié aux difficultés techniques (problème de compatibilité avec mon ordinateur sous Linux).   |
| Janvier 2016 | Premier achat de BTC sur la plateforme en ligne VirWox   | Hors-Protocole* : achat sur la plateforme et attente que le BTC/USD augmente afin que les frais de sortie exprimés en BTC ne soient pas trop importants<br><br>Au sein du protocole* : transaction* de sortie | Découverte d'une première plateforme d'échange en ligne BTC contre fiat – Virwox, originellement conçue pour la monnaie numérique du jeu « Second life » – et de ces modes de paiement, de ces frais, etc. ; confrontation aux notions de taux de change, de liquidité, etc. ; Expérience du transfert de Bitcoin entre les plateformes et les portefeuilles* personnels, de la gestion des délais, des confirmations, des frais. Cf. les BTC achetés ont été retirés après un temps long (trois ans), pour éviter des frais, nominalement exprimés en BTC, trop importants : exprimés en \$, ils étaient très élevés en BTC au moment de leur achat, et ont baissé suivant l'appréciation du cours.  |
| 10-02-2016   | Création d'un compte sur Kraken, puis sur d'autres bourses d'échange (Coinbase, Poloniex, Bitfinex, Cryptopia, Liqui, Tux, etc.) | Hors-Protocole* : achat sur différentes plateformes<br><br>Au sein du protocole* : transaction* d'entrée/sortie entre adresse et compte   | Découverte de la diversité des plateformes d'échange de CM ; confrontation aux différentes offres de paires de trading (CM et/ou de fiat monnaies), des conditions d'enregistrement plus ou moins exigeantes (cf. divulgation d'identité), des modes de paiement, des frais afférents, des risques (« Cryptopia » a fermé suite à un Hack et nos fonds, de faible valeur, ont été perdus) et des avantages relatifs ; confrontation à la pratique du trading et ses concepts (taux de change, liquidité, volatilité, <i>spread</i> , <i>slippage</i> , <i>bid</i> et <i>ask</i> , <i>market order</i> , le <i>limit order</i> , etc.) ; confrontation aux contraintes liées à l'achat/vente de CM et au transfert de celles-ci entre adresses personnelle et compte de plateforme (coûts et délais de confirmation différents suivant les CM, etc.) ; diversification des CM détenues et exploration de la galaxie des Altcoins* présentée en Chapitre I. |

|                        |   |   |   |
|------------------------|---|---|---|
| 01-10-2016             | Achat de contrat de minage chez Genesis Mining (Dash, Bitcoin, Ethereum, Zcash) | Hors-Protocole* : achat sur différentes plateformes<br><br>Au sein du protocole* : transaction* de sortie vers nos adresses et/ou compte  | Suite à l'échec de notre tentative de minage personnel, découverte du minage en nuage (cloud mining), des différentes offres (contrats de location différents, pour différentes CM), des coûts et frais afférents, des rendements (très largement décroissants) et des contraintes en termes de rentabilité : évaluation des CM minées en fonction de leurs caractéristiques, de leurs algorithmes, de leurs difficultés, des prix, etc. ; suivi des performances et des revenus du minage en nuage et de leur grande dépendance à l'évolution du marché et à la concurrence entre mineurs (arrivée de nouvelles machines rendant les anciens contrats non rentables).  |
| De mai 2016 à mai 2017 | Activité de minage individuel sur mon ordinateur portable <i>via</i> Minergate  | Bitcoin, Ethereum, Zcash, etc.<br><br>Hors-Protocole* : Installation d'un client de minage « en un click »<br><br>Au sein du protocole* : transaction* de sortie vers adresses ou compte                              | Retour sur minage individuel <i>via</i> expérimentation d'un logiciel dédié aux utilisateurs non techniciens : confrontation aux contraintes matérielles (chauffe et bruit), aux différents paramètres possibles entourant la répartition des récompenses entre hash*eurs d'une même pool de minage; là encore, sélection des CM à miner, suivant leurs caractéristiques et les performances en termes de revenu.   |
|                        | Beta-testeur pour Spell of Genesis  | Bitcoin, Counterparty<br><br>Hors chaîne* : installation d'un client logiciel et échanges avec les développeurs*<br><br>Au sein du protocole* : réception de BTC et de <i>tokens</i> sur un portefeuille Counterparty | Participation à la phase de test d'un jeu vidéo basé sur la blockchain Bitcoin et le meta protocole Counterparty (cf. Chap I) ; découverte et échange avec des acteurs d'un écosystème souhaitant développer des activités économiques autour des propriétés de Bitcoin (micro-paiement, in games tokens et CM) ; gain en nature sous forme de jetons numériques du jeu (CM native et tokens) ; découverte du gameplay, des graphismes, des scénarios, des personnages, des cartes, des quêtes, des récompenses, qui tournent autour de la culture crypto et de son histoire ; confrontation aux aspects techniques, ludiques, artistiques, économiques, sociaux, etc. ; confrontation aux difficultés posées par l'augmentation des frais de transaction* Bitcoin. |

|                |  |  |   |
|----------------|--|--|---|
|                | Beta-testeur pour Storj  | Bitcoin, Counterparty<br><br>Hors chaîne* : installation d'un client logiciel, partage de notre disque dur en P2P et échanges avec la communauté<br><br>Au sein du protocole* : réception de la CM native en guise de revenu de location et récompense de participation sur un portefeuille Counterparty | Participation à la phase de test d'un service de stockage cloud décentralisé – SorJ – utilisant le métaprotocole Counterparty basé sur Bitcoin ; installation d'un client logiciel, partage du disque dur en P2P afin de participer au réseau* de stockage ; échanges avec la communauté de testeurs ; réception de la CM native (STORJ) en guise de revenu de location et de récompense de participation, sur un portefeuille Counterparty ; connaissance des aspects techniques, économiques, sociaux, etc. du stockage cloud décentralisé ; confrontation aux difficultés posées par l'augmentation des frais de transaction* Bitcoin, le projet migre vers Ethereum (cf. Chap 1).   |
| De 2016 à 2017 | Participation au projet “Rare Pepe Cards” sur la plateforme CounterParty | Bitcoin, Counterparty<br><br>Hors chaîne* : création de nos premiers tokens/NFT, achat / vente et don /contre-don au sein de la communauté<br><br>Au sein du protocole* : réception/ envoi de CM et tokens, achat et vente via DEX Counterparty  | Participation à un projet communautaire artistique et ludique, basé, là encore, sur le métaprotocole Counterparty : on retrouve dans le chat Telegram les acteurs importants des communautés Spell of Genesis, Storj et, plus généralement, des différents projets lancés sur Counterparty ; réception de la CM native Pepecash en don, nous permettant de créer et payer les frais de soumission de notre première carte numérique de collection (tokens/NFT), représentant des variantes du même Pepe ; création de nos premiers tokens/NFT, en utilisant le protocole Counterparty et en respectant les critères de rareté et de qualité ; achat, vente, don et contre-don des cartes au sein de la communauté : réception et envoi de CM (Bitcoin, XCP, Pepecash) et de tokens/NFT (nous en avons créé trois au total), en utilisant un portefeuille compatible ; premier achat et vente de tokens/NFT via le DEX (Decentralized Exchange) de Counterparty, qui permet de faire des transactions* directement via le protocole ; connaissance des aspects techniques, artistiques, culturels, économiques, sociaux, etc. du projet Rare Pepe Cards et des controverses l'entourant à l'époque (réécriture de ce symbole par l'extrême-droite et volonté de la communauté Rare Pepe de contester cette réécriture). Appréhension très réelle de l'opprobre que certains Bitcoiners* rencontrés aux Meet Up jettent à ces usages. |

|                       |   |  |  |
|-----------------------|---|--|--|
| De 2016 à 2019        | Investissement dans des ICO   | <p>Ethereum, mais aussi Bitcoin via Counterparty</p> <p>Hors chaîne* : découverte de la galaxie d'Altcoin* qui continue d'émerger</p> <p>Au sein du protocole* : réception/ envoi de CM</p>  | <p>Participation à des levées de fonds en CM - les ICO ou <i>Initial Coin Offering</i> - qui permettent de financer des projets basés sur la blockchain ; confrontation à la croissance extensive et intensive de l'écosystème avec les différent(e)s caractéristiques, usages, valeurs, des CM et crypto-actifs* lancés, etc. ; réception et envoi de CM (ETH surtout, BTC un peu), en utilisant des portefeuilles* compatibles avec les protocoles des projets financés par les ICO; confrontation aux opportunités et risques liés aux ICO, tels que le potentiel de croissance et retour sur investissement important, mais aussi les pertes tout aussi importantes, voire totales, les questions de régulation, de sécurité, d'escroquerie : participation à des ICO plus ou moins réussies, telles que Mycelium, The DAO, Vslice, Bancor, BTU Protocol, etc. ; analyse critique des projets, de leurs objectifs et réalisations effectives, de leurs échecs et des leçons tirées ou non par le projet lui-même ou ceux concurrents.</p>  |
| De 2016 à aujourd'hui | Utilisation de Dapp : sur Ethereum d'abord, sur de nombreux autres protocoles ensuite | <p>Ethereum, mais aussi Polygon, Cosmos et son écosystème, Solana, les solutions de seconde couche d'Ethereum (comme Optimism, Arbitrum, ZksyncEra, etc.)</p> <p>Hors chaîne* : exploration continue de la diversité des usages émergents (financiers ou non).</p> <p>Au sein du protocole* : exploration continue de la diversité des usages émergents (financiers ou non).</p> | <p>Utilisation de DApps (applications décentralisées), notamment Ethereum, ses protocoles de seconde couche (cf. Optimism, Arbitrum, ZksyncEra, etc) et les protocoles de L1 concurrents (cf. Polygon, Cosmos, Solana etc.) ; exploration continue de la diversité des usages émergents, qu'ils soient financiers (DeFi) ou non (NFT, jeux, réseaux* sociaux, etc). Des usages financiers d'abord avec les protocole et services de DEFI : trading de CM et crypto-actifs* <i>on chain*</i> via différents type de DEX avec plus ou moins de fonctionnalités (à découvert ou non, type d'ordres, etc.) ; market making <i>via</i> provision de liquidité dans des DEX (Decentralized Exchange), tels que Uniswap, qui permettent de faire des transactions* directement sur la blockchain, sans intermédiaire ; nous avons bénéficié d'Airdrop et participé à la campagne de liquidity mining, qui consiste à recevoir des tokens gratuits ou à les gagner en échange de la fourniture de liquidité à des DApps ; nous avons réalisé des dépôts rémunérés (Aave, Compound, etc.) et des demandes de crédit en stable coin, garanties par nos CM mises en séquestre comme garantie en utilisant des protocoles de prêt, tels que MakerDAO ou QiDAO; achat et fourniture de produits d'assurance, qui permettent de se couvrir contre les risques liés aux DApps, tels que les bugs, les hacks, les pertes de fonds, etc., en utilisant des protocoles d'assurance, tels que la coopérative Nexus Mutual dont nous sommes membre : nous avons pris part à la fourniture d'assurance, et subi les pertes liées au</p> |

|  |  |  |
|--|--|--|
|  |  | <p>paiement des couvertures, bénéficié nous-même de paiement de couverture et voté à la gouvernance. Des usages non financiers ensuite, avec notre participation : à des réseaux* sociaux distribués (cf. Steemit, Lensprotocol, Farcaster, FriendTech) ; à des protocoles d'identité/réputation décentralisés (Proof of Humanity ; Degenscore ; Gitcoin passeport, etc.) ; à des jeux mêlant plus ou moins directement de la DEFI (cf. Aavegotchi, Age of Gods) ; à la collection des NFT <i>via</i> le marché primaire (les mint d'artistes ou de projets) ou le marché secondaire (achat/vente sur place de marchés comme Opensea, Blur) ; à un protocole de dispute décentralisé comme juré tiré au sort (cf. Kléros), etc. Appréhension des aspects techniques, économiques, sociaux, etc. des DApps et des protocoles de CM : interaction utilisant des portefeuilles*, des navigateurs, des extensions, etc. compatibles avec les réseaux* blockchain considérés; confrontation aux opportunités et aux risques liés à de tels services : notons que, comme tout usager, des pertes ont été encourues, qu'elles soient liées à de mauvaises utilisations (cf. erreur d'envoi, perte de clef cryptographique de hotwallet de faible valeur), à des attaques/effondrement de plateformes (Terra Luna, <i>via</i> son stablecoin UST, majoritairement utilisé dans l'écosystème Cosmos) ou des attaques personnelles (si de nombreuses tentatives ont été subies, aucune perte de fonds ou de NFT n'est à déplorer ici).</p> |
|--|--|--|

## Annexe IV.2 : Détails des observations participantes

|  | Date<br>Lieu        | Type<br>d'événement             | Nom de l'événement et Thématique(s)  | Temps<br>(Heure) |
|--|---------------------|---------------------------------|--|------------------|
|  | 15-10-2016<br>Paris | <i>Meet Up</i> Asseth           | Lancement de l'association Asseth et débriefing DEVCON2  | 3                |
|  | 10-12-2016<br>Paris | <i>Meet Up</i> Asseth           | Atelier monnaies locales et tokens sur Ethereum  | 2                |
|  | 02-11-2016<br>Paris | <i>Meet Up</i><br>Bitcoin-Paris | Social Meetup of Sofbar  | 3                |
|  | 17-11-2016<br>Paris | <i>Meet Up</i><br>Bitcoin-Paris | Inauguration du “Bitcoin Boulevard” à Paris (Passage du Grand Cerf)  | 2                |
|  | 29-11-2016<br>Paris | Meetup Chaintech                | Découvrez des projets Blockchains concrets !<br>(Consilium; DACA; Iex.ec; Beyond The Void; Kidner Project; Woleet; IOTA) | 3                |
|  | 01-12-2016<br>Paris | <i>Meet Up</i><br>Bitcoin-Paris | Présentation de Bitsquare avec la “Team” de Barcelone  | 2                |
|  | 01-02-2017<br>Paris | <i>Meet Up</i><br>Bitcoin-Paris | Social Meetup of Sofbar  | 2                |
|  | 01-03-2017<br>Paris | <i>Meet Up</i><br>Bitcoin-Paris | Social Meetup of Sofbar  | 2                |
|  | 05-04-2017<br>Paris | <i>Meet Up</i><br>Bitcoin-Paris | Social Meetup of Sofbar  | 2                |

|          |                           |  |  |     |
|----------|---------------------------|--|--|-----|
| <b>0</b> | 18-04-2017<br>Paris       | <i>Meet Up</i> Asseth                          | 3 présentations autour du web 3.0 et du stockage décentralisé  | 2   |
| <b>1</b> | 03-05-2017<br>Paris       | <i>Meet Up</i><br>Bitcoin-Paris                | Social Meetup of Sofbar  | 2   |
| <b>2</b> | 30-05-2017<br>Paris       | Conférence<br>Bitcoin                          | Bitcoin Paribus Impar<br><br>Programme : <a href="https://bitcoin.fr/bitcoin-pluribus-impar-3/">https://bitcoin.fr/bitcoin-pluribus-impar-3/</a>                     | 4   |
| <b>3</b> | 29-06-2017<br>Paris       | <i>Meet Up</i> Asseth                          | Meetup Identité décentralisée  | 2   |
| <b>4</b> | 09 et 10-09-2017<br>Paris | Conférence<br>Bitcoin                          | Breaking Bitcoin 2017<br><br>Programme : <a href="https://breaking-bitcoin.com/otherPages/2017/2017.html">https://breaking-bitcoin.com/otherPages/2017/2017.html</a> | 6   |
| <b>5</b> | 20-09-2017<br>Paris       | <i>Meet Up</i> Asseth                          | Blockchain for Finance<br><br>Présentation de VaribL, NapoleonX et Airswap   | 2   |
| <b>6</b> | 04-10-2017<br>Paris       | <i>Meet Up</i><br>Bitcoin-Paris                | Social Meetup of Sofbar  | 2   |
| <b>7</b> | 19-10-2017<br>Paris       | Repas de<br>L'association du<br>Cercle du Coin | 27 <sup>ème</sup> Repas du Coin  | 2 . |
| <b>8</b> | 10-03-2018<br>Paris       | Conférence<br>Ethereum                         | EthCC 2018   | 12  |
| <b>9</b> | 25-05-2018<br>Paris       | <i>Meet Up</i> Asseth                          | Asseth reçoit Parity + Snips chez Talan Labs   | 2   |

|          |  |  |  |     |
|----------|--|--|--|-----|
| <b>0</b> | 06-06-2018<br>Paris                            | <i>Meet Up</i><br>Bitcoin-Paris                | Social Meetup of Sofbar  | 2   |
| <b>1</b> | 23-10-2018<br>Paris                            | Présentation<br>d'ouvrage et<br>discussion     | Présentation et dédicace de l'ouvrage <i>Bitcoin Metamorphose</i> + discussion                                     | 2   |
| <b>2</b> | 21-02-2019<br>Conflans-<br>Sainte-<br>Honorine | Repas de<br>L'association du<br>Cercle du Coin | 42 <sup>ème</sup> Repas du Coin  | 3   |
| <b>3</b> | Du 05 au<br>07-03-2019<br><br>Paris            | Conférence<br>Ethereum                         | EthCC 2019<br><br>Programme : <a href="https://ethcc.io/">https://ethcc.io/</a>                                    | 24  |
| <b>4</b> | 03-04-2019<br><br>Paris                        | <i>Meet Up</i><br>Bitcoin-Paris                | Social Meetup of Sofbar  | 2   |
| <b>5</b> | 08 et 09-<br>06-2019<br><br>Amsterdam          | Conférence<br>Bitcoin                          | Breaking Bitcoin 2019<br><br>Programme : <a href="https://breaking-bitcoin.com/">https://breaking-bitcoin.com/</a> | 16  |
| <b>6</b> | 04-03-2020                                     | <i>Meet Up</i><br>Bitcoin-Paris                | Social Meetup of Sofbar  | 3   |
| <b>7</b> | Du 03 au<br>05-03-2020                         | Conférence<br>Ethereum                         | EthCC 3 2020<br><br>Programme : <a href="https://ethcc.io/">https://ethcc.io/</a>                                  | 24  |
|          |  | (d'environ deux<br>en Moyenne = )              | total  | 124 |

### Annexe IV.3 : Statut(s) et Rôle(s) couvert(s) par les acteurs de nos entretiens

| Entretien n° | Les « développeurs* » |                    | Les « opérateurs du traitement » et de la « vérification » des transactions* |                                      |                              |                 | Autres Services (marchands ou non) |                                  |                   |                               |                      |                                    |                                   | Utilisateurs finaux                                 |
|--------------|-----------------------|--------------------|--|--------------------------------------|------------------------------|-----------------|------------------------------------|----------------------------------|-------------------|-------------------------------|----------------------|------------------------------------|-----------------------------------|---|
|              | Couche protocole      | Couche applicative | "Pool de minage"   | "Hash*eurs" (individuel & collectif) | Fabricants de machine (ASIC) | Nœuds* complets | Portefeuilles *                    | Conservation de fonds & paiement | Bourses d'échange | Services d'analyse de données | Média & événementiel | Conseil, formation et enseignement | Autres (app/Dapp, projets divers) | Utilisateurs (Utilisateurs, investisseurs, traders) |
|              | NON                   | OUI                | NON  | OUI                                  | NON                          | OUI             | NON                                | NON                              | NON               | NON                           | NON                  | OUI                                | OUI                               | OUI   |
|              | NON                   | OUI                | NON  | OUI                                  | NON                          | OUI             | NON                                | NON                              | OUI               | NON                           | NON                  | NON                                | OUI                               | OUI   |
|              | NON                   | OUI                | NON  | NON                                  | NON                          | OUI             | NON                                | NON                              | NON               | OUI                           | NON                  | NON                                | OUI                               | OUI   |
|              | NON                   | NON                | NON  | OUI                                  | NON                          | OUI             | NON                                | NON                              | NON               | NON                           | OUI                  | OUI                                | OUI                               | OUI   |
|              | NON                   | NON                | NON  | NON                                  | NON                          | OUI             | NON                                | NON                              | NON               | NON                           | OUI                  | NON                                | OUI                               | OUI   |
|              | NON                   | NON                | NON  | NON                                  | NON                          | OUI             | OUI                                | NON                              | NON               | NON                           | NON                  | NON                                | OUI                               | OUI   |
|              | NON                   | NON                | NON  | NON                                  | NON                          | OUI             | NON                                | NON                              | NON               | NON                           | NON                  | NON                                | OUI                               | OUI   |
|              | NON                   | OUI                | NON  | NON                                  | NON                          | OUI             | OUI                                | NON                              | NON               | NON                           | NON                  | NON                                | OUI                               | OUI   |
|              | NON                   | NON                | NON  | NON                                  | NON                          | NON             | NON                                | NON                              | NON               | NON                           | NON                  | NON                                | OUI                               | OUI   |
| 0            | NON                   | OUI                | NON  | NON                                  | NON                          | OUI             | NON                                | NON                              | NON               | NON                           | NON                  | NON                                | OUI                               | OUI   |
| 1            | NON                   | NON                | NON  | NON                                  | NON                          | OUI             | NON                                | NON                              | OUI               | NON                           | NON                  | OUI                                | OUI                               | OUI   |
| 2            | NON                   | OUI                | NON  | OUI                                  | NON                          | OUI             | OUI                                | NON                              | NON               | NON                           | NON                  | NON                                | OUI                               | OUI   |

|          |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|----------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| <b>3</b> | NON | OUI | NON | OUI | NON | OUI | OUI | NON | NON | NON | NON | NON | NON | OUI | OUI |
| <b>4</b> | NON | OUI | NON | NON | NON | OUI | NON | NON | NON | NON | OUI | OUI | OUI | OUI | OUI |
| <b>5</b> | OUI | OUI | NON | NON | NON | OUI | NON | NON | NON | NON | NON | NON | OUI | OUI | OUI |
| <b>6</b> | NON | NON | NON | OUI | NON | OUI | NON | NON | NON | NON | OUI | OUI | OUI | OUI | OUI |
| <b>7</b> | NON | NON | NON | OUI | NON | OUI | NON | NON | NON | NON | NON | NON | OUI | OUI | OUI |
| <b>8</b> | NON | NON | NON | OUI | NON | OUI | NON | NON | NON | NON | NON | NON | OUI | OUI | OUI |
| <b>9</b> | NON | NON | NON | NON | NON | OUI | NON | NON | NON | NON | OUI | OUI | OUI | OUI | OUI |
| <b>0</b> | NON | OUI | NON | NON | NON | OUI | NON | NON | NON | OUI | OUI | NON | OUI | OUI | OUI |
| <b>1</b> | NON | OUI | NON | NON | NON | OUI | NON | NON | NON | NON | OUI | NON | OUI | OUI | OUI |
| <b>2</b> | NON | OUI | NON | NON | NON | OUI | NON | NON | NON | NON | NON | NON | OUI | OUI | OUI |
| <b>3</b> | NON | OUI | NON | NON | NON | OUI | NON | NON | NON | NON | OUI | OUI | OUI | OUI | OUI |
| <b>4</b> | NON | NON | NON | NON | NON | OUI | NON | NON | OUI | NON | NON | NON | OUI | OUI | OUI |

|          |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|----------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| <b>5</b> | NON | NON | NON | NON | NON | OUI | NON | OUI | OUI |
| <b>6</b> | OUI | OUI | NON | NON | NON | OUI | NON | NON | NON | NON | NON | NON | OUI | OUI |     |
| <b>7</b> | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   |     |
| <b>8</b> | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   | /   |     |

#### Annexe IV.4 : Liste des entretiens menés et notice biographique succincte des enquêtés

| Réf. | Nom <sup>487</sup> | Éléments Biographiques :<br><i>Âge ; Formation ; Découverte des cryptomonnaies* ; Expérience avec Bitcoin et / ou Ethereum ; Activités dans l'écosystème ; Revenu annuel</i>  | Communauté | Conditions & Matériaux              | Date (Durée)            |
|------|--------------------|---|------------|-------------------------------------|-------------------------|
| #1   | Anon 1             | 34 ans ; Ingénieur Bac +5 ; Découvert Bitcoin en 2012, intéressé par la technique et surtout l'activité de minage qu'il réalisera brièvement (il nous précise qu'il continue à miner de l'Ether). Il va se regrouper avec d'autres pour former la communauté parisienne. Lance au début quelques projets sur son temps libre avant d'en faire son activité principale - en conseil, service et sécurité - après un plan social en 2017 dans l'entreprise qui l'employait.<br><br>Revenu annuel : ~40 k.   | Bitcoin    | Face-à-face<br>Enregistrement audio | 13/02/2019<br>(150 min) |
| #2   | Anon 2             | 43 ans ; Bac +5 dans le domaine de l'informatique médicale. Découvert Bitcoin en 2013, brève activité de minage avec sa GPU. Puis cherche à se reconvertis dans des projets Bitcoin, du fait de sa longue expérience dans le <i>langage de programmation*</i> C++. Il va travailler sur différents petits projets Bitcoin avant de se retrouver à travailler, faute d'opportunités, dans le secteur du paiement Internet. Il travaille aujourd'hui dans le secteur des bourses et du trading de CM – ce qui l'a poussé à apprendre le langage de programmation* « Python », utilisé dans ce milieu - et il reconnaît regretter de ne pas utiliser les codes Bitcoin dans son activité. Rev. ann. 60k euros. | Bitcoin    | Face-à-face<br>Enregistrement audio | 19/02/2019<br>(120 min) |

<sup>487</sup> Voir l'encadré précaution d'écriture concernant les principes d'anonymisation que nous avons suivi.

|    |                          |   |                |   |  |
|----|--------------------------|---|----------------|---|--|
| #3 | Anon 3                   | 45 ans ; Bac +5 école d'ingénieur, spécialisation en génie logiciel ; S'il a entendu parler de Bitcoin dès 2011, ce n'est qu'en 2013, à l'occasion d'une flambée des cours et d'une couverture médiatique, qu'il va vraiment commencer à s'y intéresser. La perte de son emploi d'alors lui laisse le temps d'étudier le WP*, ce qui le décidera à creuser ce qu'il considère comme une innovation technologique là pour rester. De par ses compétences et intérêt, il travaille à différents projets tournés vers la préservation de la vie privée. Rev. ann. ~ 42K (variable, car travailleur indépendant).   | <b>Bitcoin</b> | Face-à-face<br>Enregistrement audio   | 19/02/2019<br>(45 min)                                   |
| #4 | Jérôme De Tychet         | 32 ans ; Master en Économie théorique et empirique (Bac +5) à Paris 1 et une Maîtrise en Gestion des Organisations et de la Performance à Paris Dauphine, ; Il a toujours été attiré par le Hardware, les jeux vidéo et la lecture du WP* de Bitcoin l'a beaucoup interpellé. Il commence par du minage GPU sur Bitcoin en 2013, puis en 2014 mine différentes cryptos avant de passer sur Ethereum dès son lancement. Il a d'abord travaillé comme économiste statisticien pour diverses organisations (Eurostat, Bercy, ministère des Affaires sociales) avant de se rediriger vers le secteur des cryptos. Co-fondateur de l'association française Ethereum France (ex-Asseth), dont il est encore président, il participe à l'organisation de <i>Meet Up</i> et de conférence sur l'écosystème Ethereum (ETHCC Paris). De 2017 à 2020, il va travailler chez « Consensys » comme « Blockchain tech lead », puis il passe chez « Ledger » comme « Global Head of Client Success », avant de fonder, en octobre 2021, le jeu fondé sur la blockchain « Cometh ». Il est aussi, depuis 2020, professeur associé au Conservatoire National des Arts et Métiers. Rev. ann. 100k < annuel (beaucoup de variable) [~ 80% de son épargne en crypto; précise - d'un Million] | Ethereum       | - 1 <sup>er</sup> Face-à-face; prise de notes<br><br>- 2 <sup>ème</sup> Face-à-face<br>Enregistrement Audio | 21/02/2019<br>(30min)<br><br>+<br>01/03/2019<br>(65 min) |
| #5 | Marc Zeller (pseudonyme) | Âge : non indiqué ; Hypokhâgne, un peu de Droit et d'Économie à Paris 1, de Droit et de Philosophie à Saint Hyppolyte mais surtout autodidacte. Vient des milieux underground et militants (squat avec "Jeudi noir", producteur de musique) avant de découvrir Bitcoin, mais surtout Ethereum pour qui il a plus d'intérêt. Va en faire son activité principale à partir de 2014 : <i>Freelance</i> , analyste chez « La maison du Bitcoin » (auj. « Coinhouse »), co-fondateur de l'association AssEth (auj. Ethereum France), de « The Block Cafe » et « Integration Lead » chez « Aave » (Ethereum).   | Ethereum       | Face-à-face<br>Prise de notes   | 22/02/2019<br>(80 min)                                   |
| #6 | Taylor Monahan           | Âge : non indiqué ; Études "Film and Television" à la New York University ; En 2014-2015, elle se redirige vers le développement web (Front End) ; En août 2015 avec le lancement d'Ethereum, elle co-fonde le service de portefeuille MyEtherWallet qu'elle quitte, après des controverses avec l'autre co-fondateur, pour fonder son propre projet de portefeuille Mycrypto, dont elle est actuellement la CEO. Personnalité très impliquée dans l'écosystème Ethereum depuis son lancement (modératrice de forum Ethereum, aide aux utilisateurs particulièrement lors de l'événement The DAO).  | Ethereum       | Face-à-face<br>Prise de notes   | 06/03/2019<br>(25 min)                                   |

|     |               |  |                    |   |   |
|-----|---------------|--|--------------------|---|---|
| #7  | Jordi Baylina | Âge : non indiqué ; Études d'ingénieur en télécommunication et Bac+5 (MBA) en Business Administration à l'Université de Navarra. Développeur* depuis ses 12 ans, il découvre Bitcoin en 2014 et lit le WP* qu'il trouve très stimulant. Militant et activiste, il s'intéresse aux technologies de décentralisation et va réellement s'intéresser aux crypto <i>via</i> Ethereum dès son lancement. Ethereum lui permet, contrairement à Bitcoin, des usages plus sophistiqués. Il va devenir une personne influente, particulièrement pour le projet The DAO.  | Ethereum           | Face-à-face<br>Enregistrement Audio   | 06/03/2019<br>(14 min)  |
| #8  | Nicolas Bacca | 42 ans ; Ingénieur de l'ENSI CAEN, Bac +5. Travaille dans les années 2000 sur la carte à puce avant de créer différentes start-ups dans le domaine de la sécurisation de secret. En 2012, création de l'entreprise BTChip, autour d'une carte à puce de sécurisation physique de Bitcoin ( <i>Hardware Wallet</i> ). Rapprochement avec Joël Pobeda (Chronocoin), Eric Larchevêques et Thomas France (La maison du Bitcoin/Coinhouse), et co-fondation de l'entreprise Ledger, une des entreprises leaders dans le secteur des portefeuilles* physiques. Actuellement CTO de Ledger. Rev. ann. ~100k euros.  | Bitcoin & Ethereum | Face-à-face<br>Enregistrement Audio   | 15/03/2019<br>(45 min)  |
| #9  | Vlad Zamfir   | 30 ans ; Bac +3 en Mathématique à l'université de Guelph. Se décrit comme autodidacte (apprentissage des mathématiques très jeune avec son grand-père, sur les crypto beaucoup d'apprentissage en ligne). Travail en freelance comme consultant, analyste et chercheur dans les architectures distribuée (PoS). Découverte de Bitcoin en 2013. Chercheur à l'Ethereum Fondation depuis 2014, suivant sa rencontre avec V. Buterin, et travaille spécifiquement sur le passage d'Ethereum à la PoS. Personnalité vocale dans la communauté, il avait lors de The DAO des avis assez dissonants (avait prévu un HF avant même l'attaque). Il n'est pas capable de me donner son rev. ann., car il ne gère pas lui-même ses finances. | Ethereum           | - 1 <sup>er</sup> Face-à-face;<br>prise de notes<br><br>- 2 <sup>ème</sup> Face-à-face;<br>Enregistrement Audio | 13/03/2019<br>(90 min)<br><br>+<br><br>14/03/2019<br>(91 min) |
| #10 | Anon 4        | 39 ans ; Après le Bac, a commencé à travailler dans l'informatique au bas de l'échelle de salaire. VAE Bac+ 4 ; 15 ans de travail salarié dans différentes entreprises en Administration système. Découvre Bitcoin sur les réseaux* sociaux en 2011. En train de créer une entreprise en lien avec Bitcoin. Dernier salaire annuel ~ 100K, aujourd'hui sans salaire.   | Bitcoin            | Face-à-face<br>Enregistrement audio   | 04/04/2019<br>(120 min)                                       |

|     |                     |   |                    |   |                         |
|-----|---------------------|---|--------------------|---|-------------------------|
| #11 | Alexis Roussel      | 43 ans ; Études de droit : licence de l'Université d'Aix-Marseille, maîtrise à l'Université Panthéon Sorbonne et un DESS de « Droit public des nouvelles technologies » à l'Université de Paris X Nanterre (BAC+5). D'abord juriste spécialisé dans les nouvelles technologies, il va travailler 7 ans aux Nations-Unies pour la Cour Internationale de Justice, sur les questions de gouvernance électronique. En 2009, il s'implique en politique et devient président du jeune Parti Pirate Suisse, poste qu'il occupera pendant près de deux ans. Il déclare avoir découvert Bitcoin dès 2009-2010, de par son intérêt pour les nouvelles technologies et son réseau* social largement ouvert aux activistes numériques (des membres du Parti Pirate et des connaissances se revendiquant Cypherpunk). Dès fin 2013-début 2014, il co-fonde - avec Y. Honoré, G. Bochlser et R. Braud - la plateforme d'échange de cryptomonnaie* « SBEX », renommée « Bity ». Il en sera le CEO durant près de 6 ans, avant de devenir le président de son conseil d'administration. En 2020, il devient administrateur* et COO de l'entreprise « Nym Technologies SA », qui travaille au développement de nouvelles infrastructures préservant la vie privée. Lui et « Bity » jouèrent un rôle important dans les événements entourant « The DAO Hack » : Bity a été partenaire de l'entreprise « Slock It » à ses débuts, ce qui a permis de résoudre les problématiques juridiques que l'équipe rencontrait en Allemagne ; après la survenue de l'attaque de « The DAO », M. Roussel va conseiller et aider l'équipe de développement comme les membres des « White Hackers » (WHG et RHG) à leur protection juridique. Il publiera également, via le blog de Bity, des informations sur le déroulé des événements et sur la résolution de crise. Salaire non communiqué, mais déclare qu'il est dans la catégorie des cadres et professions intellectuelles supérieures, au vu des statuts des membres de son ménage : lui, dirigeant d'entreprises, et sa femme, avocate, tous deux ayant des salaires suisses. | Bitcoin & Ethereum | Face-à-face<br>Enregistrement audio     | 15/05/2019<br>(102 min) |
| #12 | Fabian Vogelsteller | 37 ans ; Études en communication et média à l'université de Buffalo, Master en Beaux-Arts (bac+5), en design média et développement web, film, audio et design d'interface à l'Université Bauhaus-Universität Weimar. Il a d'abord exercé des activités de designer web avant de travailler en <i>freelance</i> à partir de 2015 et, pour près de 4 ans, pour la Fondation Ethereum. Il participe au développement du navigateur Internet « Mist » - avec A. Van de Sande - qui permet d'interagir avec les Dapp* Ethereum -, du portefeuille Ethereum principal. On lui doit d'autres contributions notables dans l'écosystème Ethereum, comme le développement de la bibliothèque « web3.js », qui n'est autre que la bibliothèque JavaScript la plus utilisée sur Ethereum. Enfin, il est parfois qualifié de « père des ICO », ayant participé grandement au développement des standards ERC20 et ERC 725, permettant de faciliter le déploiement de token sur Ethereum. Aujourd'hui fondateur et “Chief Blockchain Architect” pour Lusko. De par ses activités, il a participé activement à la résolution de la crise « The DAO » et était proche du RWG à l'époque.   | Ethereum           | Vidéoconférence<br>Enregistrement Audio | 25/05/2019<br>(124 min) |

|     |                   |  |          |   |                         |
|-----|-------------------|--|----------|---|-------------------------|
| #13 | Alex Van de Sande | Âge : non indiqué ; Études de design graphique à l'Université d'État de Rio de Janeiro. Activités professionnelles de designer d'interface et d'architecture de l'information. Ayant travaillé en freelance pour la Fondation Ethereum pendant près de 6 ans (UX designer et conseil), il y a participé au développement du portefeuille / navigateur Internet « Mist » - avec Fabian Vogelsteller - qui permet d'interagir avec les Dapp* Ethereum directement via son navigateur Internet ; il est aussi co-fondateur d' « UniLogin » sur Ethereum - et travaille aujourd'hui pour « Balancer Labs », entreprise qui développe des services de « bourse d'échange décentralisée » sur Ethereum (il s'agit d'un protocole de « tenue de marché automatique », appelé aussi « AMM* ») sur. A participé à la résolution de la crise « The DAO » et était proche du RWG à l'époque.  | Ethereum | Vidéoconférence<br>Enregistrement Audio | 04/06/2019<br>(120 min) |
| #14 | Jimmy Song        | Âge : non indiqué ; Licence de mathématique à l'Université du Michigan, des formations en mathématique et cryptographie*. Suite à la crise de 2008, il déclare s'être intéressé à la monnaie et à l'économie, à travers la lecture d'ouvrages économiques « libéraux » et/ou relevant de l'« école autrichienne ». D'abord développeur* informatique avant de se reconvertis dans Bitcoin à travers différentes start-up. En tant que développeur*, il a travaillé pour la firme « Monetas » où il a pris la tête de l'équipe en charge de l'intégration de Bitcoin, comme manager du développement pour la firme « Armory Technologies », qui développe un portefeuille, il a aussi réalisé quelques PR sur le répertoire Bitcoin Core (~15 commit), relatifs majoritairement à des procédures de test. Aussi, bien qu'il soit développeur*, il préfère se décrire comme formateur et éducateur Bitcoin, reconnaissant que ses compétences et son expérience sur les codes sources Bitcoin ne sont pas suffisantes pour qu'il prenne part plus activement à cette activité. Il est une personnalité reconnue et vocale dans la communauté Bitcoin, se qualifiant volontiers de « Bitcoin Maximalist » pourfendeur de « shitcoin », et porte différents statuts : il produit des billets de blog et des vidéos éducatives sur Bitcoin, est l'auteur du livre <i>Programming Bitcoin</i> paru chez O'Reilly, est chargé de cours à l'Université d'Austin au Texas, réalise du conseil, et est membre de Blockchain Capital. | Bitcoin  | Vidéoconférence<br>Enregistrement Audio | 14/06/2019<br>(58 min)  |

|     |                      |  |          |   |                         |
|-----|----------------------|--|----------|---|-------------------------|
| #15 | Matt Corallo         | 28 ans ; Obtention d'une Licence de Sciences Informatiques à l'Université de Caroline du Nord, à « Chapel Hill ». Il devient tôt, dès 2011, contributeur sur le répertoire logiciel Bitcoin alors qu'il n'a que 18 ans et va rapidement devenir, suivant son engagement, un des « Core développeurs* » du logiciel Bitcoin Core. En 2014, après avoir été brièvement ingénieur logiciel chez Google, il co-fonde - avec A. Back, P. Wuille, G. Maxwell, M. Friedenbach, J. Timon, A. Hilll, J. Wilkins, F. Hall, A. Fowler - l'entreprise canadienne « Blockstream », spécialisée dans le développement des technologies de Blockchain, les systèmes distribués et les technologies associées à Bitcoin (« Liquid Network », « Blockstream Satellite », « Blockstream explorer », etc.). En 2017, M. Corallo commence à travailler chez « Chaincode Labs » - firme spécialisée dans la recherche et le développement sur Bitcoin – et son contrat couvre en partie le financement de ses activités de « Core développeur* » Bitcoin. En 2019, il change d'équipe pour travailler comme ingénieur « open source » au sein de la firme « Square » - entreprise américaine spécialisée dans les services de paiement numérique créée par J. Dorsey, aussi CEO de Twitter – qui lui offre, là encore, un contrat couvrant ses activités volontaires de « Core développeur* ». Revenu annuel : « Assez pour vivre à New York, mais pas pour toucher un salaire de Wall Street :) ».   | Bitcoin  | Vidéoconférence<br>Enregistrement Vidéo | 18/06/2019<br>(120 min) |
| #16 | Simon Polrot         | 35 ans ; Études de droit à l'Université Paris 1 (Bac +5), École de Formation professionnelle des Barreaux de la Cour d'Appel de Paris. D'abord avocat fiscaliste et conseil, avant de se reconvertis et de s'intéresser aux cryptomonnaies*, particulièrement Ethereum. Lance en 2017 le projet « VariabL » intégré à l'entreprise « Consensys » Paris, en 2018. Co-fondateur de l'Asseth et aujourd'hui président de l'Adan (Association visant à défendre les Actifs numériques en France).  | Ethereum | Face-à-face<br>Enregistrement Audio     | 27/06/2019<br>(100 min) |
| #17 | Sébastien Gouspillou | 50 ans ; Maîtrise de marketing et de management à l'Institut Supérieur des Cadres Supérieurs de la Vente (ISCV-CNAM, Bac +4). Il a d'abord travaillé dans le commerce international, particulièrement avec l'Asie où il était spécialisé dans les produits financiers agroforestiers. Il découvre Bitcoin vers 2013, grâce à son ami informaticien Jean-François Augusti, et dit débuter sa réflexion sur l'économie et la monnaie. Mais c'est en 2015, suite à sa rencontre avec Robert Corby, un « mineur » américain développant alors des fermes en Ukraine, qu'il achète son premier mineur ASIC qu'il met en opération dans la ferme de Corby. Cette rencontre est pour lui un « élément déclencheur », qui le voit, début 2016, avec des amis français, lancer sa propre ferme de minage, hébergée alors dans les locaux de Corby. Pour ne pas porter seul les investissements initiaux importants, il développe un modèle de ferme, où les machines qu'il héberge et opèrent appartiennent à ses clients, qui lui donnent en gestion. En 2017, il co-fonde, avec J-F Augusti, l'entreprise « BigBlock Datacenter » sur le même modèle ; ils créent leur première « mine » en France qui, suivant la survenue d'une phase baissière importante du cours du bitcoin, ne s'avère pas rentable. Ils délocalisent alors leur ferme chez un « confrère » à Irkoutsk, en Sibérie et développent des fermes au Kazakhstan et en Azerbaïdjan. S. Gouspillou, via l'entreprise « BigBlock Datacenter », est aujourd'hui un des principaux acteurs de la filière du minage en France et de son expertise, il intervient dans les médias pour promouvoir ce secteur d'activité | Bitcoin  | Vidéoconférence<br>Enregistrement Vidéo | 06/11/2019<br>(56 min)  |

|     |                       |   |                    |   |                         |
|-----|-----------------------|---|--------------------|---|-------------------------|
|     |                       | et répondre aux nombreuses critiques auxquelles ce secteur fait face.   |                    |   |                         |
| #18 | Jean-François Augusti | 50 ans ; Études d'ingénieur en informatique et système d'information à l'Université de Nantes et au Conservatoire National des Arts et Métiers. Il a travaillé en tant qu'administrateur* réseau* et système pour l'entreprise Servier, comme chef de projet chez BNP Paribas, et travaille encore à son propre compte en tant que consultant en informatique. Il dit avoir découvert Bitcoin en deux étapes. D'abord, vers 2013 via un ami informaticien avec lequel il commence par découvrir le minage de Bitcoin (les premières UCN* gagnées n'ayant jamais été récupérées). Puis en 2017, S. Gouspillou est revenu vers lui pour lui parler de Bitcoin et c'est de là qu'il dit avoir vraiment commencé à s'y intéresser, particulièrement intéressé et « impressionné » par ses aspects techniques et sécuritaires. Ils co-fondent ensemble l'entreprise « BigBlock Datacenter », intervenant dans le secteur du minage, pour laquelle M Augusti est en charge des dimensions techniques en tant que CTO. Revenu annuel ~50K en tant dirigeant de société.  | Bitcoin            | Vidéoconférence<br>Enregistrement Audio | 13/11/2020<br>(40 min)  |
| #19 | Morgan Phuc           | 35 ans ; Études dans les mathématiques et la mécanique des fluides. Destiné à être ingénieur, il se met à jouer au poker afin de financer ses études et devient joueur professionnel pendant près de 11 ans. Il découvre Bitcoin et les « cryptos » fin 2011 via un camarade de promotion, Benoist Huget. Fin 2014, avec B. Huget et son frère, il co-fonde la start-up et le média « Bitconseil », qui produit des articles et ressources pratiques relatives à l'écosystème crypto en direction des lecteurs francophones. Il reconnaît s'être aussi intéressé à Bitcoin du fait de son côté militant, et se déclare lui-même proche de pensées « libertariennes ». En 2017, M. Phuc et B. Huget développent une activité de formation, dont ils ont la charge. En 2018, ils rencontrent et associent à « Bitconseil » les deux co-fondateurs du <i>Journal Du Coin</i> , un média au positionnement similaire qu'ils décident par la suite de développer plus fortement. La start-up « BitConseil/Journal du Coin », qui intervient dans le secteur des médias, du conseil, de la formation et de l'événementiel, dispose aujourd'hui d'une équipe d'une quinzaine de personnes et M. Phuc y est directeur du contenu et rédacteur en chef, formateur et, plus sporadiquement qu'avant, rédacteur d'articles sur les CM et crypto-actifs*. | Bitcoin & Ethereum | Vidéoconférence<br>Enregistrement Vidéo | 30/01/2020<br>(127 min) |

|     |                   |   |                    |   |                         |
|-----|-------------------|---|--------------------|---|-------------------------|
| #20 | Antoine Le Calvez | 26 ans ; Études en génie informatique, spécialité analyse de données, à l'Université de Technologie de Compiègne (Bac+5). Il découvre Bitcoin et les « cryptos » début 2013, durant ses études. Son intérêt est directement aiguillé par son intérêt et ses compétences pour l'analyse de données, qui lui sont directement accessibles, puisque ces systèmes financiers sont « ouverts » et « libres d'accès ». Il commence son activité d'analyse de données <i>au sein de la chaîne*</i> sur Bitcoin, avec la publication d'un site d'information intitulé « P2SH.info » (aujourd'hui txstats.com en collaboration avec « Bitmex Research » et « Coinmetrics », dont M. Le Calvez est salarié), qui dénombrait les transactions* Bitcoin utilisant le format de transaction* « Pay to Script Hash* ». C'est cette réalisation qui le fera connaître, ce qui va lui permettre d'entrer en contact avec des entreprises du secteur intéressées par ses compétences. Ainsi, en 2016, il réalisera son stage de fin d'études à Londres, à « Blockchain.info » – l'un des plus gros fournisseurs de services de portefeuille en ligne –, entreprise qu'il quittera en 2018 pour rejoindre l'équipe de « Coinmetrics ». Il travaille toujours aujourd'hui pour cette entreprise au sein de laquelle il est « Lead Blockchain Data Engineers ». | Bitcoin & Ethereum | Vidéoconférence<br>Enregistrement Vidéo | 06/02/2020<br>(69min)   |
| #21 | Léa Thiebaut      | 27 ans ; Études d'ingénieur « agronome environnementaliste » à l'Institut Supérieur d'Agriculture de Lille (niveau Bac +5). A travaillé un an dans les objets connectés en agriculture de précision avant sa découverte de Bitcoin fin 2014 et sa reconversion dans ce secteur. Co-organisatrice des conférences Breaking Bitcoin avec Pierre Lorcry et Kevin Loaec. Organisatrice de <i>Meet Up Bitcoin</i> à Neuchâtel. Elle a depuis pris ses distances avec l'écosystème et entamé une formation vétérinaire.   | Bitcoin            | Vidéoconférence<br>Enregistrement Audio | 12-02-2020<br>(110 min) |
| #22 | Clément Lesaige   | Âge : non indiqué ; Études d'ingénieur informatique, double diplôme de Master en Science de l'informatique, l'un à l'Université Technologique de Compiègne et l'autre à Georgia Tech (bac+5) ; Intéressé par les « cryptos » dès 2013 avec Bitcoin avant même le lancement d'Ethereum. Va d'abord jouer avec les Smart contracts* sur Bitcoin (les portefeuilles* multi-signatures), avant de découvrir l'ambition d'Ethereum de faire du SC beaucoup plus complexe et facile. Depuis 2016, travaille à plein temps dans le secteur, d'abord comme freelance dans la sécurité des Smart contracts*, puis à partir de 2017 comme CTO de Kleros (plateforme sur Ethereum financer <i>via ICO</i> ). A acheté un peu d'Ether pour commencer à « jouer » avec Ethereum dès le lancement. A investi dans « The DAO », car le projet lui semblait intéressant. Reconnu dans l'audit et la sécurité des Smart contracts*.  | Ethereum           | Vidéoconférence<br>Enregistrement Vidéo | 13-02-2020<br>(80 min)  |

|     |                |  |                    |   |                        |
|-----|----------------|--|--------------------|---|------------------------|
| #23 | Stéphane Roche | <p>34 ans ; Études d'histoire et d'archéologie (double licence) à l'Université de Toulouse-le-Mirail, Master professionnel de "Documentaliste audiovisuel" à l'université de Paris Est Créteil (niveau Bac+ 5) et obtention d'un certificat professionnel en « Développement Web » au Conservatoire National des Arts et Métiers. Découvre Bitcoin en 2014 pendant sa formation au Cnam, ce qui l'amène à réaliser, en 2015, un stage de fin d'études de six mois chez « Ledger » - une des entreprises leaders dans le secteur des portefeuilles* physiques. Après cette « première introduction » à Bitcoin, il va travailler près d'un an et demi sur Ethereum, avant de revenir à Bitcoin dont il se sent plus proche des valeurs communautaires. Il dit s'être éloigné d'Ethereum du fait de l'apparition des « ICO », des « scams » et du « bullshit », préférant la communauté Bitcoin qu'il décrit comme plus ancienne, technique et avec laquelle il partagerait la philosophie crypto anarchiste, la revendication « d'être souverain de son argent ». Il a été co-fondateur de l'association « Asseth », et il travaille depuis 2018 à Lisbonne – à « The Block Cafe » -, exclusivement sur Bitcoin. Il a monté une micro-entreprise, « Bitcoin Studio », avec laquelle il propose du développement et de la formation autour de Bitcoin. Cela génère peu d'activité, et il est actuellement en recherche d'emploi. Revenu annuel : « très faible » (~5000 euros), il « vit sur [s]es bitcoins depuis longtemps », dont une partie a été reçue de son activité chez Ledger, bien qu'il ait de temps en temps de courtes missions à « quelques milliers d'euros ».</p> | Bitcoin & Ethereum | Vidéoconférence<br>Enregistrement Vidéo | 14-02-2020<br>(55 min) |
| #24 | Pierre Noizat  | <p>Âge : non indiqué ; Formation d'ingénieur à l'école polytechnique suivie de l'obtention d'un Master à l'université Telecom ParisTech (spécialisation Telecom, niveau BAC +5) et réalisation d'un MBA en « Marketing et finance » à l'université de Colombia (NY). C'est de sa présence aux États-Unis et sa spécialisation en Telecom qui va le rapprocher de la cryptographie*, puisqu'il va travailler à l'époque pour une entreprise de télévision à péage (« directTV »). Il découvre Bitcoin et y « adhère » très tôt (dès son lancement), puisque ces activités lui permettent de travailler avec des cryptographes de haut niveau, comme d'être en mode veille technologique pour ce qui a trait à la cryptographie*. D'ailleurs, il souligne qu'il était déjà intéressé par les questions monétaires du fait d'amis intéressés par les monnaies alternatives. Dès 2011, il fonde – avec un associé – la première place de marché Bitcoin euro au monde : « Paymium.com », qui compte près de 15 salariés aujourd'hui. En 2018, il co-fonde la place de marché « Blockchain.io », offrant un plus large choix de cryptomonnaies* et crypto-actifs*.</p> <p>Revenu annuel : ~ 60 000 euros, il se « paye 5000 euros bruts /mois », considérant que se payer plus dans cet écosystème n'est pas très cohérent et que se « payer plus ne serait pas en lien avec l'économie de cet écosystème ».</p>  | Bitcoin & Ethereum | Vidéoconférence<br>Enregistrement Vidéo | 14-02-2020<br>(80 min) |

|     |                 |  |                             |   |                         |
|-----|-----------------|--|-----------------------------|---|-------------------------|
| #25 | Hervé Hababou   | <p>44 ans ; Diplôme d'ingénieur informatique de l'ENSIIE – École Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise - Lisieux, complétée de formations professionnelles à la <i>London Business School</i>. Plus de 22 ans d'expérience dans l'informatique, où il tient différents postes (développeur*, commercial, chef de projet, directeur d'entreprise), le conduisant à être aujourd'hui chef d'entreprise et investisseur. Découvre Bitcoin assez tôt (la date n'est pas précisée) grâce à son ami Vidal Chriqui, avec qui il partage un intérêt pour la « <i>partie technique</i> ». Cet intérêt joint ses « <i>deux passions</i> » pour « <i>l'informatique et l'économie</i> », et le constat que « <i>des entreprises voulaient se financer pour travailler sur Bitcoin</i> », le poussera à « <i>creuser</i> » en tant qu'investisseur et entrepreneur. Comme investisseur, il se penche « <i>sur les entreprises et les business modèles qui allaient éclore</i> » de cet écosystème et, de « <i>fil en aiguille, [il a] investi à la fois [...] dans Ethereum au tout début, et dans des entreprises qui travaillaient soit sur Bitcoin, soit sur Ethereum</i> ». En tant qu'entrepreneur, il lance avec Vidal Chriqui fin 2018 la start-up « BTU Protocol » : ambitieuse de développer des solutions de distribution utilisant le protocole de registre* distribué ; le protocole est lancé à la faveur d'une ICO sur Ethereum (finalisée début octobre 2018, elle récoltera pas moins de près de 5,5 millions de dollars à l'époque). Revenu annuel : relativement élevé, en tant que « <i>CSP++</i> », « <i>ça marche</i> » et il « <i>paye le plus à la cantine des enfants</i> ».</p>  | Ethereum                    | Vidéoconférence<br>Enregistrement Vidéo | 24-02-2020              |
| #26 | Bob Summerhill  | <p>Âge : non indiqué ; Études d'ingénieur informatique. Il rencontre V. Buterin en juin 2014, lors d'un repas à Vancouver (CA) organisé par son ami D. Lowi, et prend part au lancement d'Ethereum. De juillet 2015 et jusqu'à aujourd'hui, il travaille bénévolement pour la fondation Ethereum. Polyvalent, il participe à différentes activités : il travaillera sur le code source d'un client Ethereum en langage C++ (« <i>cpp-ethereum</i> ») dans l'équipe de C. Reitwiessner ; participera au développement de la première plateforme Ethereum finalisée, « <i>Homestead</i> » ; à la restauration du dépôt de <i>cpp-ethereum-1.3.0</i> ("Homecoming") ; aux activités entourant le <i>Fork*</i> consécutif à l'attaque de « <i>The DAO</i> » ; à l'échec de la tentative d'octroi d'une nouvelle licence Apache 2.0 ; puis à la conférence DEVCON2 à Shanghai. Il a aussi travaillé pour le projet « <i>Hyperledger</i> », une initiative open source à l'initiative d'entreprises régies par la Fondation Linux, visant à faire progresser la technologie blockchain. Il va aussi être engagé par Joe Lubin, de l'entreprise « <i>ConsenSys</i> », pour laquelle il travaille à la formation de l' « <i>Entreprise Ethereum Alliance</i> » (aujourd'hui le plus gros consortium sur les technologies de protocole de registre* distribué). Il va aussi créer l'entreprise « <i>Sweetbridge</i> ». Enfin, de janvier 2019 jusqu'à aujourd'hui, il est le directeur exécutif de l' « <i>ETC Cooperative</i> », dont l'objet est de conduire le développement du protocole Ethereum Classic et son écosystème et qui est née du conflit communautaire autour de la résolution par un hard Fork* de l'attaque de « <i>The DAO</i> ». Acteur « <i>passerelle</i> » refusant le « <i>tribalisme</i> », il travaille tant pour Ethereum que pour Ethereum Classic, et il est le seul acteur de la communauté Ethereum Classic qui ai accepté notre demande d'entretien.</p> | Ethereum & Ethereum Classic | Face-à-face<br>Enregistrement Vidéo     | 03-03-2020<br>(120 min) |
| #27 | “Non-entretien” | <p>Âge : non indiqué ; Formation : non indiquée ; Découverte des cryptomonnaies* : non indiquée ; Expérience avec Bitcoin et/ou Ethereum : développeur* Bitcoin Core à partir de 2014, il devient Core</p>   | Bitcoin                     | Échange mail &                          | 02/2021                 |

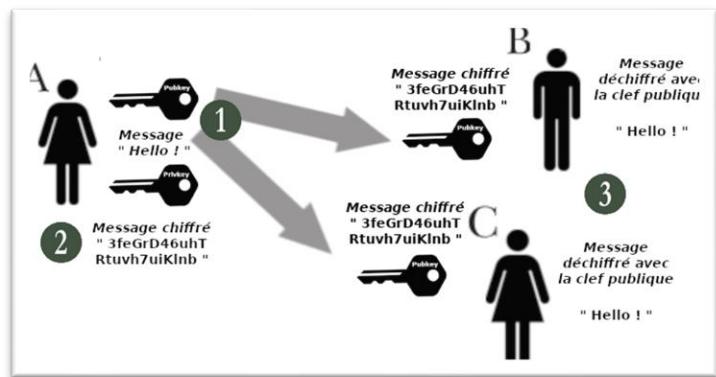
|   |                  |   |  |                                    |  |
|---|------------------|---|--|------------------------------------|--|
|   | avec Marco Falke | mainteneur en 2016, où il est en charge des tests ; il a aussi travaillé sur des outils de seconde couche, comme avec ses BIP 157/158, et on lui doit plus de 2 000 contributions au code source de Bitcoin Core. Pour ces activités, il a été financé par « Chaincode Labs » jusqu'en 2020, puis par « OKCoin » depuis 2021, et a annoncé son intention de quitter son rôle de mainteneur en 2023 (comme de nombreux autres Core mainteneurs) ; Revenu annuel : non indiqué. En l'absence d'entretien <i>stricto sensu</i> , les informations biographiques qui précèdent sont extraites de <a href="https://bitcoinmagazine.com/culture/marco-falke-bitcoin-network">https://bitcoinmagazine.com/culture/marco-falke-bitcoin-network</a>  |  | <i>via un Forum</i> <sup>488</sup> |  |
| / | SuperAnon        | Correspond à un « acteur fictionnel » créé pour tenir le rôle de paravent, permettant de protéger l'anonymat d'acteurs, eux bien réels, que nous avons rencontrés. Si l'anonymisation totale a pu être demandée par certains, beaucoup des acteurs rencontrés ont accepté de le faire nommément. Reste que ces derniers ont pu nous demander explicitement que certaines des paroles qu'ils nous avaient données restent « en off », ne soient pas retranscrites ou tout du moins que leur origine ne soit pas dévoilée (avis / critiques privées, enjeux de réputation, information non publique, etc.). Aussi, nous leurs avons proposé une telle stratégie d'anonymisation : créer un personnage unique qui livrera l'ensemble de ces avis jugés controversés. À l'exception d'une information que l'on nous a livrée tout en nous précisant qu'elle ne pourrait en aucun cas être divulguée, même sous cette forme (impliquant un face-à-face, il aurait été possible à l'autre interlocuteur d'identifier cette source), les différents acteurs rencontrés ont ainsi accepté que de telles paroles soient portées par ce personnage. |  |                                    |  |

<sup>488</sup>Le forum « bitcoin.stackexchange.com »

## Annexe V: Retours circonstanciés sur les composants clefs et le fonctionnement d'une CM

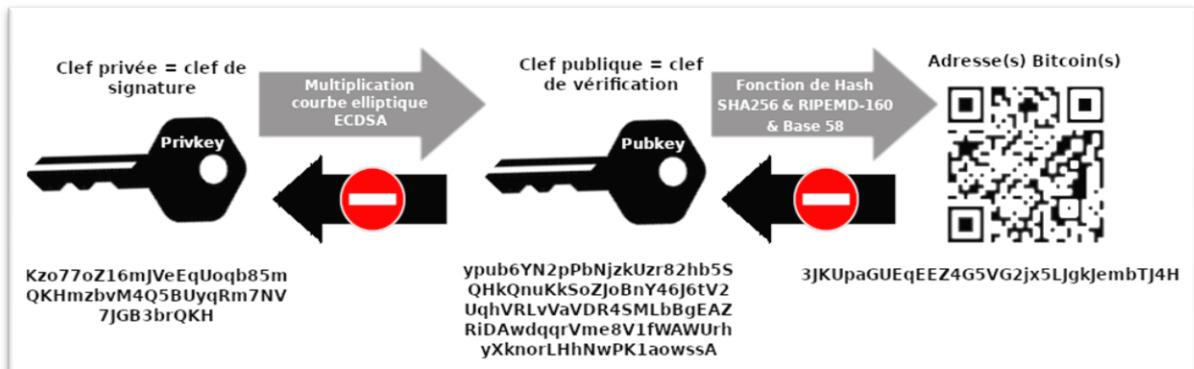
### Annexe V.1 : Cryptographie asymétrique et souveraineté individuelle

Le chiffrement asymétrique permet de résERVER des informations aux seules personnes disposant des clefs adéQUATES, en garantissant une identification réCiproque (Hughes 1993). Dans le schéma ci-contre, Alice (A) dispose d'un couple de clefs publique et privée. La première étape (1) est pour elle de partager sa clef publique. Dans un deuxième temps (2), elle chiffre un message ("Hello !") avec sa clef privée et transmet le message chiffré : "3feGrD46uhTRtuvh7uiKlnb" aux personnes B et C, qui peuvent (3) le déchiffrer grâce à la clef publique qui leur a été transmise.



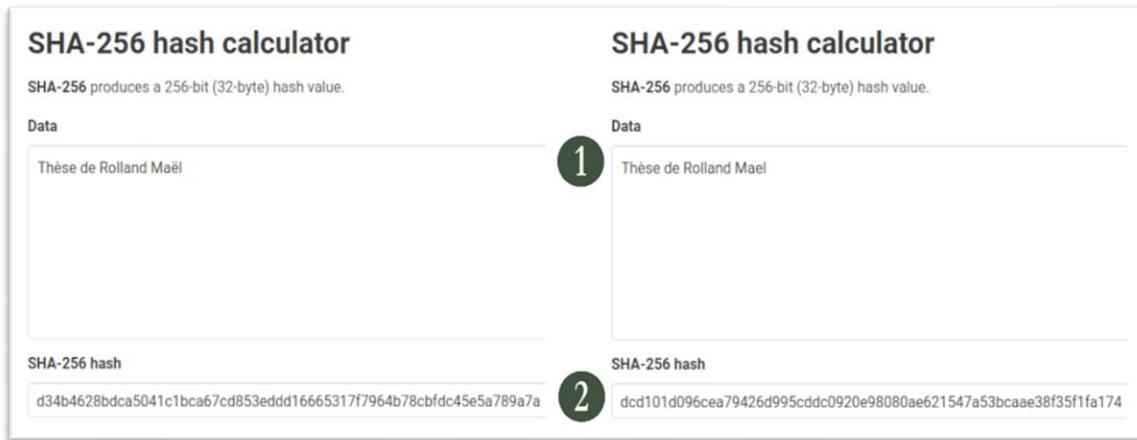
À l'inverse, B et C peuvent envoyer un message chiffré avec la clef publique de A, qu'ils connaissent, qu'elle seule pourra déchiffrer grâce à sa clef privée

### Annexe V.2 : Clefs privées, clefs publiques et adresses Bitcoin



Le processus permettant de générer un couple de clés cryptographiques utilise une courbe elliptique, spécifiquement l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm) pour Bitcoin. Cet algorithme dispose de procédures distinctes pour la signature et la vérification. La clé privée est utilisée pour signer les transactions\*. La clé publique, dérivée de la clé privée *via* la courbe elliptique, est utilisée pour vérifier ces signatures. L'adresse Bitcoin est ensuite dérivée de la clé publique en appliquant les fonctions de hachage SHA-256 et RIPEMD-160, suivies du format d'encodage Base58Check pour faciliter l'utilisation et la vérification. Voir Rykwalder (2014).

### Annexe V.3 : La fonction de Hachage SHA 256

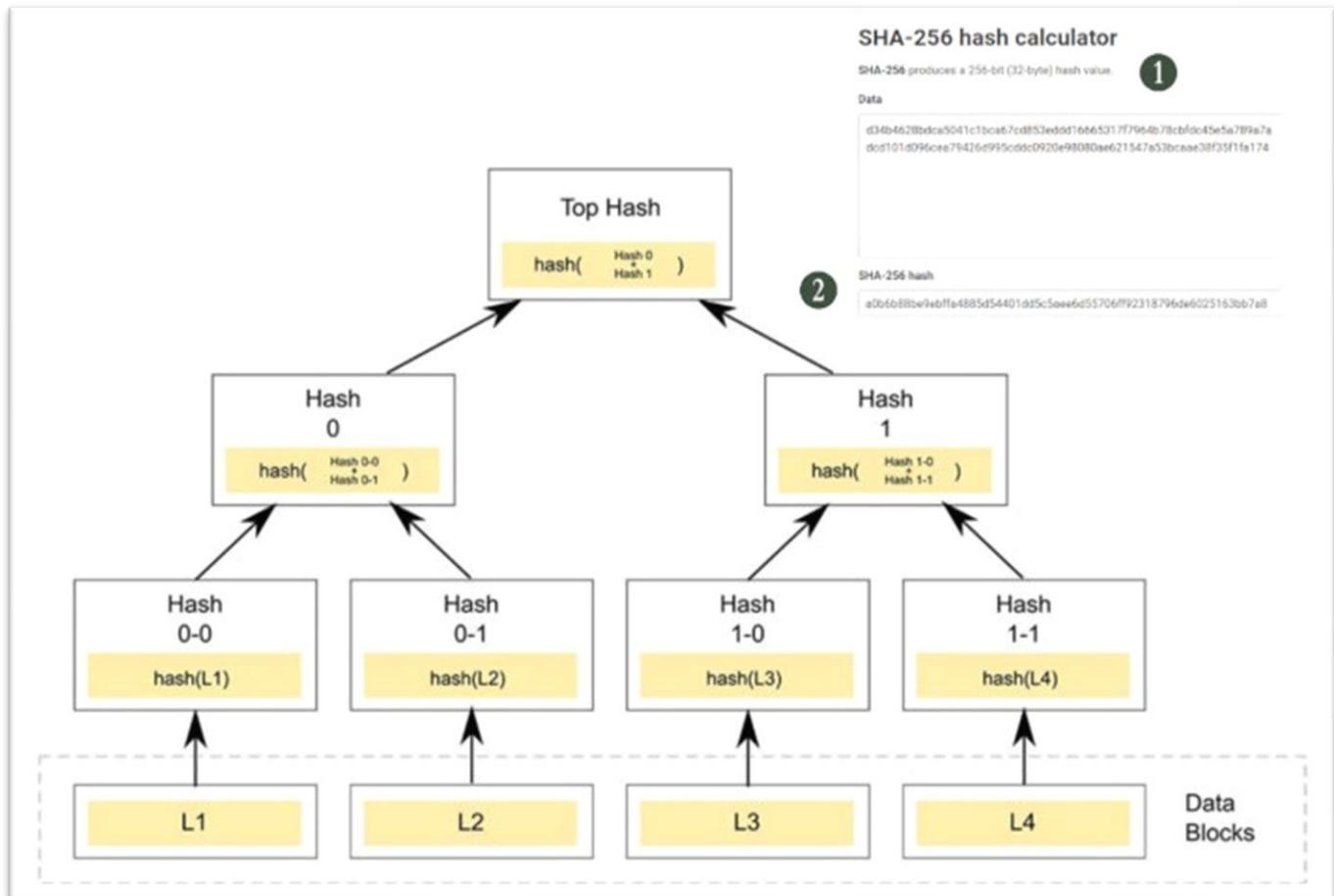


Une fonction de Hash\*age est un algorithme cryptographique qui prend en entrée des données de taille variable et produit en sortie une donnée de longueur fixe, appelée « empreinte cryptographique »\* ou « hash\* ». Toute variation des données en entrée (ici, la présence ou l'absence de tréma sur le « e »), modifie les empreintes en sortie (2)<sup>489</sup>. Ainsi, toute personne disposant des données entrantes peut vérifier leur intégrité *via* le hash\* transmis, qui doit correspondre à celui qu'elle réalise elle-même de son côté. Parmi les différents algorithmes de hash\*age existants, Nakamoto a choisi pour les opérations de traitement des transactions\* le SHA 256 (« Secure Hash\*ing Algorithm 256 », utilisé dans notre exemple).

### Annexe V.4 : L'arbre de Merkle

L'arbre de Merkle\* renvoie à un usage particulier des fonctions de hachage qui permet à un ensemble de données, potentiellement très volumineux, d'être transformé tout en permettant de les retracer, en un hash\* unique : le hash\* sommet (ou « *Merkle root* »), dont il est possible de vérifier l'intégrité. Ce dispositif, proposé en 1980 par R. Merkle (pionnier de la cryptographie\* asymétrique dont dérive le nom), visait à « *produire un condensé pour un répertoire public de certificats numériques* » de site Internet et les preuves numériques afférentes (Narayanan et Clark 2017, p. 8).

<sup>489</sup> Avec tréma, le hash\* est “d34b4628bdca5041c1bca67cd853eddd16665317f7964b78cbfdc45e5a789a7a” ; en son absence, il devient “dcd101d096cea79426d995cddc0920e98080ae621547a53bcaaee38f35f1fa174”.

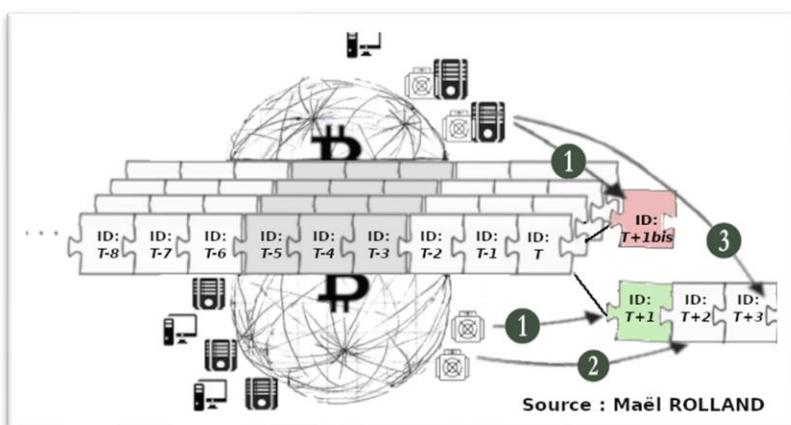


source : [https://en.bitcoinwiki.org/wiki/Merkle\\_tree](https://en.bitcoinwiki.org/wiki/Merkle_tree)

Bitcoin utilise l'arbre de Merkle\* dans la construction de chaque enregistrement sous la forme de bloc, où les feuilles sont des transactions<sup>\*490</sup>. Une telle structure de données offrent des « propriétés importantes » : le hachage du dernier bloc – l'en-tête d'enregistrement\* – est un condensé unique où toute modification de l'une des transactions\* (« feuille ») modifie « jusqu'à la racine du bloc et [les] racines de tous les blocs suivants ». Ainsi, avec simplement la connaissance du dernier hachage valide, tout acteur peut « télécharger le reste du grand livre depuis une source non fiable et vérifier qu'il n'a pas changé » (*Ibid.*, p. 7). Dans le même sens, il est facile de « prouver qu'une transaction\* particulière est incluse dans le grand livre » sans avoir à divulguer beaucoup d'informations (*Ibid.*). L'empreinte (2) est liée cryptographiquement aux empreintes des données initiales (pour nous (1)) et permet, en plus d'un gain important de taille, d'être facilement vérifiable.

<sup>490</sup> Dans l'exemple, les feuilles (Hash 0-0 et Hash 0-1) sont le *hash\** de chacun des blocs de données initiales ("Thèse de Rolland Maël" et "Thèse de Rolland Mael") qui, concaténés deux à deux (1), permettent de calculer un *hash\** parent Hash 0, ici (2) « a0b6b88be9ebffa4885d54401dd5c5aee6d55706ff92318796de6025163bb7a8 ».

## Annexe V.5 : Cas d'une réorganisation malicieuse de type « Attaque 51% »



**L'attaque 51% permettant une double dépense *off chain\** repose sur ce principe.**

Si l'hypothèse de majorité des nœuds\* honnêtes tombe, à un instant T, un attaquant est assuré de manière probabiliste de trouver les enregistrements plus rapidement que les autres

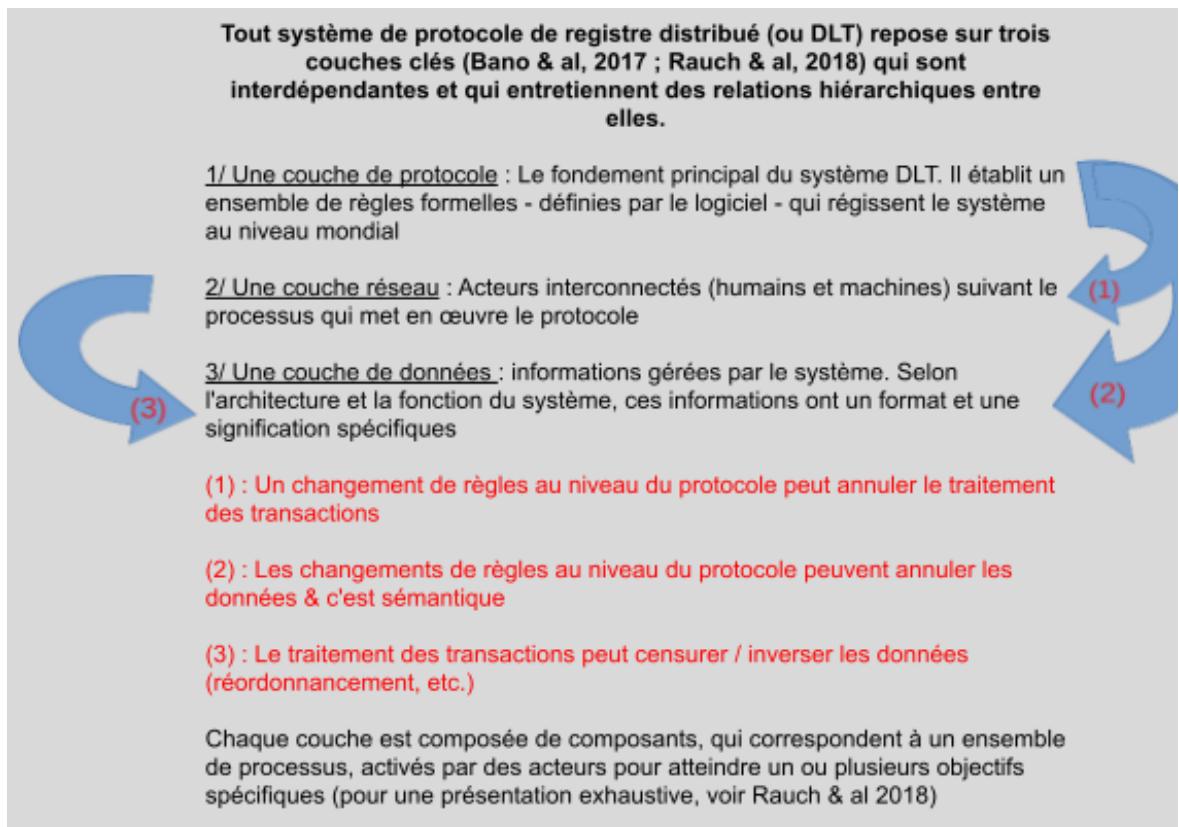
nœuds\*, ce qui lui permet d'imposer à terme sa version de l'HISTORIQUE DES TRANSACTIONS\* contre une autre. L'attaque consiste à réaliser une double dépense dans le monde réel *via* une même UTXO\* *on chain\** : il s'agit d'un type particulier de double dépense (l'autre cas sera traité en Chapitre V) qui joue sur le principe de réorganisation précédent. Dans notre exemple, l'attaquant dispose d'une UTXO\* de 10 BTC et (1) crée deux transactions\* différentes la dépensant : l'une transfert les 10 BTC vers une plateforme d'échange et se trouve intégrée dans le bloc **ID : T+1** ; l'autre vers un portefeuille appartenant à l'attaquant, intégrée dans un bloc **ID : T+1bis**. *Cet enregistrement candidat\* valide a été produit par l'attaquant qui ne le diffuse pas au réseau\**. Sur cette chaîne **ID : T+1bis** cachée de tous, l'attaquant continue d'ajouter des nouveaux enregistrements (**ID : T+2bis**, **ID : T+3bis**, **ID : T+4bis**, etc.) : comme il dispose de plus de la moitié de la puissance de calcul, il est assuré que la construction de la chaîne **ID : T+1** sera, sur un temps donné, moins rapide et donc moins longue et lourde que la sienne. Conventionnellement, une plateforme d'échange va créditer le compte de l'attaquant après 6 enregistrements consécutifs (appelé “confirmation”), pour nous **ID : T+6**. Une fois crédités sur le compte de l'attaquant, les 10 BTC seront échangés contre d'autres actifs et retirés de la plateforme vers un portefeuille que l'attaquant possède. Pour l'heure, il dispose seulement d'actifs d'une valeur équivalente aux 10 BTC. Reste que, si les nœuds\* honnêtes ont trouvé 6 nouveaux enregistrements (**ID : T+6**), l'attaquant lui, a déjà ajouté 8 enregistrements (**ID : T+8bis**) à la chaîne qu'il construit en secret. Une fois retirés les actifs achetés, il est temps de révéler à l'ensemble du réseau\* la chaîne **ID : T+8bis**. Dès réception de ce nouvel enregistrement, constituant une chaîne plus lourde relativement à la chaîne « honnête », il devient canonique et tous les nœuds\* convergent sur l'historique **ID : T+1bis**, **ID : T+2bis**, **ID : T+3bis**, **ID : T+4bis**, etc., annulant *de facto* toutes les transactions\* qui avaient été traitées et enregistrées dans la chaîne **ID : T+1**, **ID : T+2**, ..., **ID : T+8bis**. L'attaque est réalisée ! L'attaquant dispose donc de ses 10 BTC, qu'il s'est envoyé à lui-même *via* la transaction\* inscrite dans l'enregistrement **ID : T+1bis** ET des actifs équivalents à 10 BTC qu'il a obtenus de la plateforme d'échange. C'est elle qui subit la double dépense et perd 10 BTC, puisque la transaction\* première, inscrite en **ID : T+1**, n'a finalement jamais existé, et le compte de l'attaquant n'aurait pas dû être crédité. Les cas de doubles dépenses sur Bitcoin sont rares, mais pas impossibles<sup>491</sup> du fait de la grande puissance de calcul accumulée et de sa distribution, mais des cas de double dépense de ce type

<sup>491</sup> Voir par exemple <https://twitter.com/BitMEXResearch/status/1221673450986565633>

ont été rencontrés sur des CM moins sécurisées (voir, par exemple, le cas d’Ethereum Classic qui a connu des situations similaires à plusieurs reprises, forçant les bourses d’échange à allonger le nombre de confirmations qu’elles demandent (Voell 2020; Balakrishnan 2020).

La création monétaire s’opère à cette étape. L’enregistrement reconnu comme canonique contient la transaction\* de récompense qui est traitée comme toutes les autres. Si l’opérateur victorieux peut directement dépenser les frais de transaction\* payés par les utilisateurs (définis en (1)) qu’il a traités, ce n’est pas le cas des UCN\* nouvellement émises. L’UTXO\* créée par la transaction\* *coinbase* a la particularité de ne pouvoir être dépensée qu’après que 100 enregistrements ont été produits au-dessus de celui qui la contient (Walker, Greg 2017). Il s’agit là d’une mesure de protection dans le cas où un bloc reconnu canonique un temps soit rendu orphelin, suite à une réorganisation de l’historique consécutive à un Fork\* de chain. Malicieuses ou non, ces situations sont régulées par la compétition en PoW\* - étape (2) – et la convergence se réalisera à terme via l’étape (3).

#### Annexe V.6 : Relations hiérarchiques entre les trois couches d’un protocole de registre distribué



Un système de protocole de registre\* distribué correspond à l’articulation de 3 couches de clés interdépendantes et soumises à des relations hiérarchiques entre elle (les flèches bleues). La couche protocolaire est hiérarchiquement supérieure en ce qu’elle établit l’ensemble de règles formelles - définies par le logiciel - qui régissent le protocole et ce faisant, des changements de règles protocolaires peuvent (1) servir à annuler le traitement des transactions\* ou (2) à annuler les données consignées et leur sémantique. On trouve un niveau

en dessous une couche réseau\*, correspondant à un ensemble d'acteurs non humains interconnectés opérés par des opérateurs humains suivant le processus que met en œuvre le protocole. Cette couche est elle-même hiérarchiquement supérieure à la couche base de données où se trouve consigné l'ensemble des données endogènes\* administrées par le protocole de registre, car ce sont ces opérateurs qui choisissent ou non de les consigner, et peuvent censurer / inverser les données (réordonnancement, etc.) qu'ils reçoivent.