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. 1[60]

« 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 codecode. »*

Ethereum Whitepaper
Vitalik Buterin, 2013, p.1[61]

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

[60] 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 [consultation au 01/06/2022].
[61] 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)[62]. Ce design parfait et immutable immunise Bitcoin contre la discrétion, 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 démystification 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

[62] 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 appréhender 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 idéel 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 restituerons 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 (1.3)**, 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

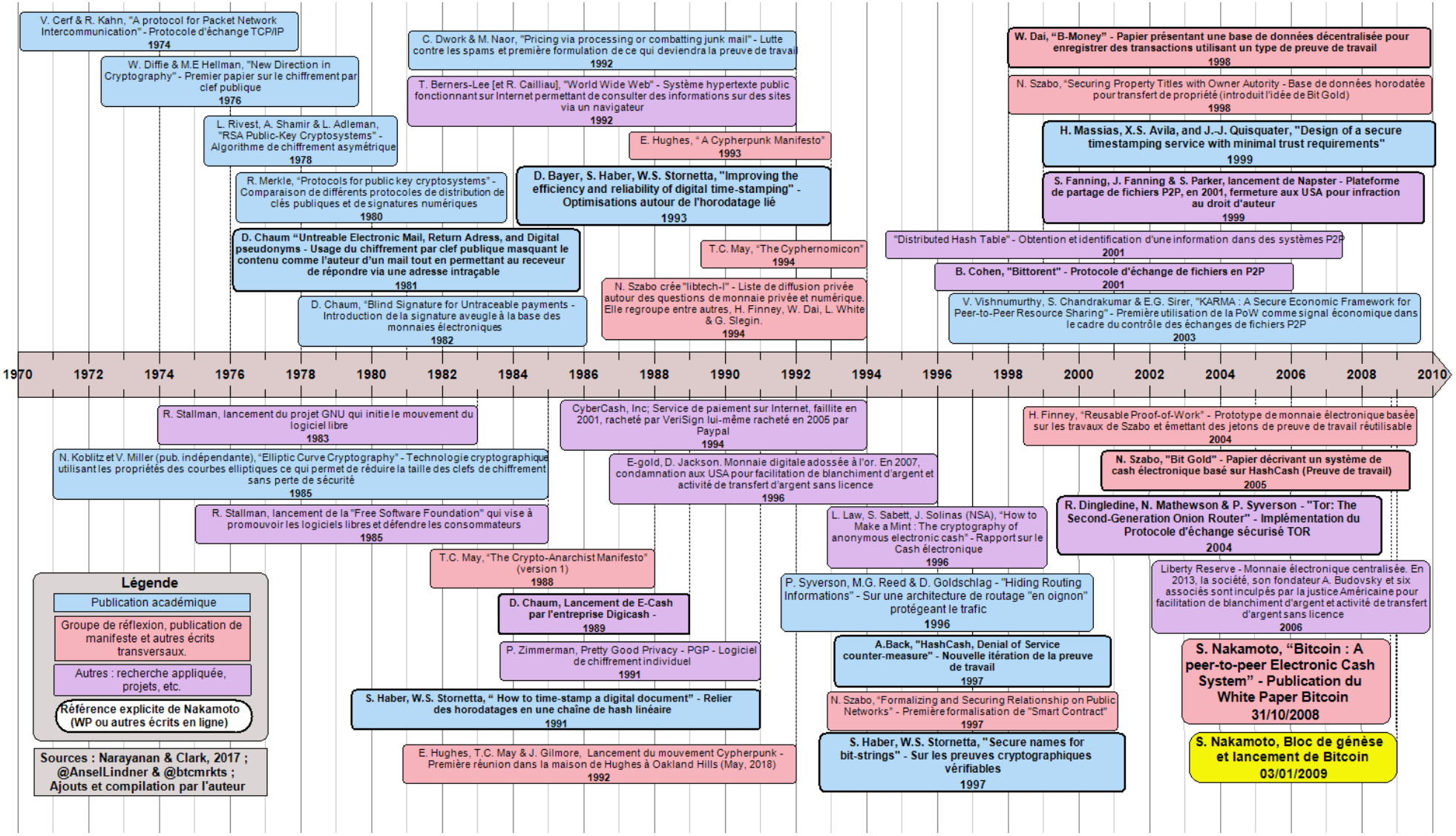
du *WP** (Nakamoto 2008c), de ses écrits en ligne (courant jusqu'en 2010[63]) et des premiers codes sources logiciels. Au-delà du caractère « sacré » qui est attribué[64] à ces productions, elles sont autant de traces renseignant ses desseins originaux. Le design de Bitcoin, comme les *récits maîtres* (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).

[63] 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).

[64] 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 [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 idéel 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[65]. 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*[66]*, 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[67]). 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 libertarianisme, 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

[65] 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.

[66] 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.

[67] 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* »[68] - 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*[69]. 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[70] et fonde le forum *Bitcointalk*[71], 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

---

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

[69] 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].

[70] « *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]).

[71] 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*[72] le message : « *The Times 03/Jan/2009 Le Chancelier est sur le point de lancer un deuxième plan de sauvetage pour les banques* »[73]. 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)[74]. Face aux gouvernements, Nakamoto vise modestement[75] 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 connaissions 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*[76]. 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[77] soit numériques, avec la création de la liste de diffusion « *cypherpunk*

---

[72] 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/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f/) 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.

[73] Titre à la une du Times du 3 janvier 2009. https://en.bitcoin.it/wiki/Genesis_block [consultation au 24/09/2015].

[74] Cette affirmation récurrente est contrefactuelle puisqu'il faut attendre le 9 janvier pour que soit publié le premier logiciel.

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

[76] 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 cyberpunk*. » (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* ».

[77] 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[78]. 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[79]. 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[80] (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 cyberespace, « *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[81] : 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,* […]

---

[78] 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).

[79] 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).

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

[81] « *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)[82].

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*[83] *»,* 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-*

[82] 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).

[83] 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 cyberespace* » 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[84]. Aux licences *copyright* et au contrôle exclusif octroyé au propriétaire est opposée une diversité de licences libres, depuis les plus intransigeantes *copylefts* à d'autres plus *permissives*[85] (*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[86] 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

---

[84] 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).

[85] La notion de logiciel libre (« *free software* ») émerge début 1980 grâce à Richard Stallman qui créer 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)

[86] Licence de logiciel libre dite « permissive » et ouverte aux entreprises, qui limite les restrictions de réutilisation, particulièrement l'absence d'« hérédité » pour les ré-usages, qui rend les changements de licence possibles.

Wirdum 2020)[87], 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[88]. 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[89] : 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

---

[87] 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 S[t] 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].

[88] 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).

[89] 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[90]), 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 Golumbia 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

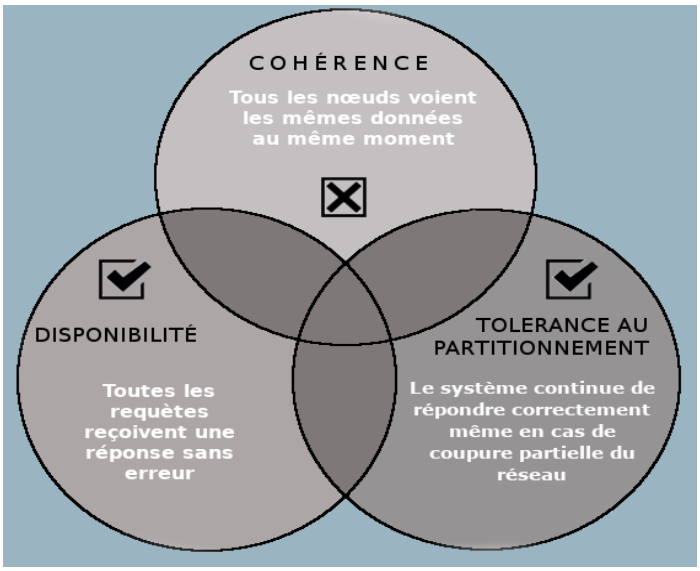
[90] Il y écrit que « *Bitcoin est une mise en œuvre de la proposition b-money de Wei Dai* », http://weidai.com/bmoney.txt sur les Cypherpunks; http://en.wikipedia.org/wiki/Cypherpunks en 1998 et de la proposition *Bitgold* de Nick Szabo http://unenumeted.blogspot.com/2005/12/bit-gold.html (Nakamoto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

(Nakamoto 2008c, p. 9)[91]. 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^{e} siècle avant J.-C., la première monnaie frappée et étalonnée au poids attribuée, suivant Hérodote, au Roi de Lydie (Galbraith 1976, Chap. 2)[92]. 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).

[91]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)

[92] 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 » (« *Pratical Byzantine Fault Tolence* », 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 prémunit 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 dépense*s », 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[93]. 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[94]. Pour l'un et l'autre, l'inventeur va devoir opérer des compromis et arbitrages et fixer des choix technologiques (*langage de programmation**, librairies 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[95], incité ou sanctionné.

[93] 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).

[94] 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).

[95] 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[96]). Loin de ne faire que « *cacher* »[97], 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 cryptographique asymétrique, à couples de clefs publiques/privées[98], 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[99]. 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

[96] 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).

[97] Étymologiquement, le terme dérive de du grec "kruptos" (κρυπτός) signifiant « caché » et "graphein" (γράφειν) signifiant « écrire ».

[98] 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)

[99] May en faisait la clef d'une souveineté individuelle hors État (May 1994, p. 294).

les *coiners*,* « *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** relève de ces clefs uniquement : elles seules *agissent* lors des transactions* *via* la production des signatures d'ordre de cession d'UCN*[100] (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[101]. Un portefeuille* 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* de transactions* 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*, mais pas supprimer, modifier ou réorganiser les transactions* 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* (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*, les structurer (fonctions de *hash**, horodatage* lié et *arbre de Merkle**), mais aussi désinciter certains comportements numériques (du

[100] Une transaction spécifie un « *hachage d'une clef publique* » qui est vérifié suivant « *une routine de validation* 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* multisignatures ou protocoles de seconde couche, traités ci-après).

[101] 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 consécutivement 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), ce traitement offrirait une résistance aux ordinateurs quantiques dont Nakamoto anticipe le développement et qui, en l'état des connaissances, compromettraient 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[102] (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* »[103] (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[104]). L'obtention d'un *hash** cible requérant (en moyenne) un temps de traitement donné, cela permet

---

[102] 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 prédécesseur, 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)

[103] 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).

[104] 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*. »[105] (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).

[105] 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 » (computationnel) 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*)[106]. 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 *attaque*s *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

[106] 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 »[107]). 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* »[108], « *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[109]). 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

---

[107] Le site https://forkmonitor.info/blocks/btc/000000000000000000004b8adbe583584f0e2370c0b752ede243535f8cfd3f354, 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].

[108] « *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).

[109] 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 intéressement 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**[110]. À la suite de l'enregistrement de genèse* du 3 janvier 2009[111], 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

[110] 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.

[111] 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. Ferron, 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)[112]. Reste qu'elles sont aussi importantes qu'arbitraires, puisqu'une multiplicité de paramètres pouvait être implémentée, suivant des considérations sociotechniques différentes[113]. 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[114]. 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 nœuds* suffisant dans un temps court, il faut que les opérateurs aient à y gagner[115]. 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*

---

[112] 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).

[113] « *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).

[114] 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).

[115] « *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 entrainer 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[116]). 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*

[116] 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).

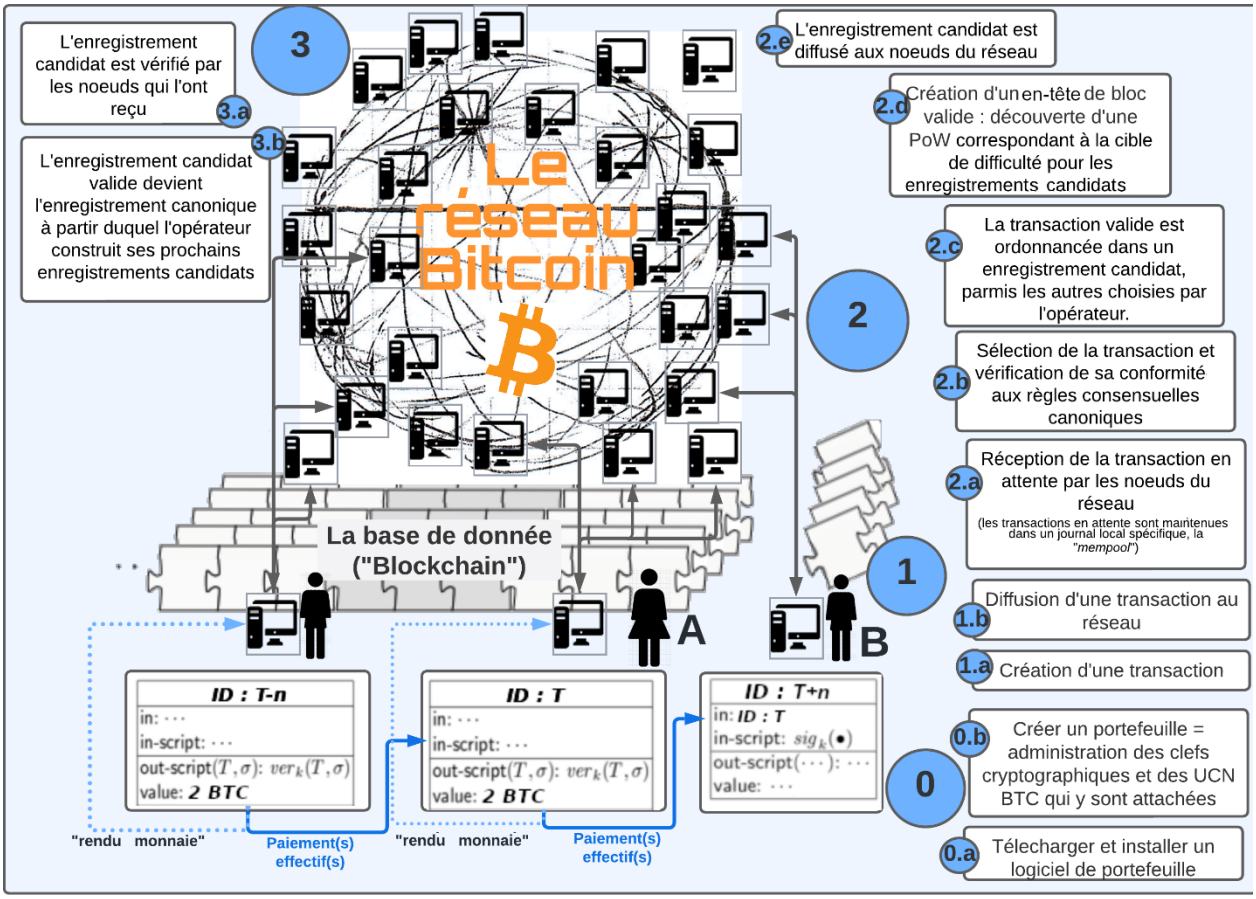
qui y est consigné), ce qui, à coût de stockage donné, conduira à terme à des coûts croissants, qui induiront en retour une centralisation des opérateurs du fait d'économie d'échelles. Nakamoto, là encore, évacue ce problème, postulant que « *les systèmes informatiques étant généralement vendus avec 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 entremêle 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[117]. 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

[117] 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 »[118] (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[119], 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. Le 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 (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.

---

[118] 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 économe 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].

[119] 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[120] 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[121]. 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'érigeant 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[122]), 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 »[123] 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

[120] 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).

[121] 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.

[122] 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.* » Buterin (2013).

[123] 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.

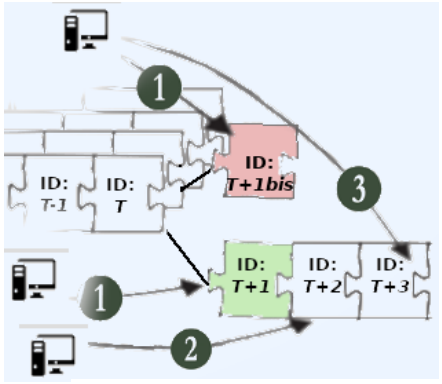
conclusive du scénario décrit par Nakamoto se reproduit à l'infini, les nœuds* restant en scène pour une nouvelle séquence identique.

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[124] (situation illustrée par l'étape 1 de la Figure 4 suivante).

Figure 4 : Réorganisation et « bloc orphelin »



Source : Rolland Maël

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.

[124] Dans cette situation « *certains 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 *« inclu[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)[125] :

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 incréments 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*

[125] 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 Ruhleder 2010, p. 118-119, s'arrêtent à la 8ème.

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[126]) 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.

[126] 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 règlementaire 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* »[127] (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[128] », 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[129] (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

---

[127] 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.

[128] De l'anglais « *Proof of Concep*t », 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.

[129] 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 nœuds* 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[130]. 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 »[131], 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'élever : 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[132] (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

[130] Entre 2010 et 2011, l'écosystème Bitcoin passe des cinq segments initiaux à 13, voire Rauch 2016, p. 49 à 56.
[131] 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.
[132] 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[133]. Mais l'offre « multi-signature », nécessaire à la mise en œuvre de solution de séquestre 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)[134]. L'émergence de solutions mieux intégrées et stabilisées ne tarde pas : apparaît en 2010 MtGox, lancé par Jed McCaleb[135], qui devient rapidement la première plateforme pour la paire BTC/$[136] : 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).

---

[133] En 2010 apparaît « *MyBitcoin* », premier service intermédié (dit de garde ou "*custodial wallet*", Rauchs 2016), permettant un accès simplifié au réseau. Un portefeuille* « léger » non intermédié (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].

[134] 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 séquestre mmunautaire 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'érige en première cotation (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.*).

[135] Créateur dans les années 2000 de la plateforme de partage P2P eDonkey, après MtGox qu'il vend à Mark Karpelès, 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).

[136] 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 prefixe « 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[137], 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)[138]. 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

---

[137] 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.

[138] 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'érige 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[139]. 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

[139] 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[140] : 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 »[141] 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 essaiment[142] 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

---

[140] 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.*).

[141] 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 illéga[l], mais aussi terriblement len[t]* », 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).

[142] Après « Silk Road », de nombreuses plateformes aux offres et propriétés différenciées 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[143]. 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

[143] 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)[144]. 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 « Satochi 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 pléthore 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

[144] 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 métaprotocoles 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...[145] 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 métaprotocole *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 métaprotocole va permettre l'émission du premier *stable coin* indexé au dollar, le « *Tether* » (USDT), catégorie d'actif dont l'importance infrastructurelle sera croissante[146]. 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[147]). Et aux services financiers *off chain** offrant déjà des usages en dépôt ou en garantie des BTC s'ajoutent dès lors une multiplicité de

[145] 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* ».

[146] Premier actif synthétique dont la valeur nominale est adossée au dollar, il est une reconnaissance de dettes émise 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).

[147] 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[148]. 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[149].

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[150], 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 affermissement 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 impressionnants 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

[148] 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).

[149] 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.

[150] 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[151]. 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 différenciées 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 « *Ligthning Network* » (LN, en rouge), implémenté 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.)[152]. Problèmes que les nombreux autres protocoles de registre* distribué concurrents, comme Ethereum, ambitionnent de corriger pour le supplanter.

---

[151] 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].

[152] 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 « inefficiences » 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…

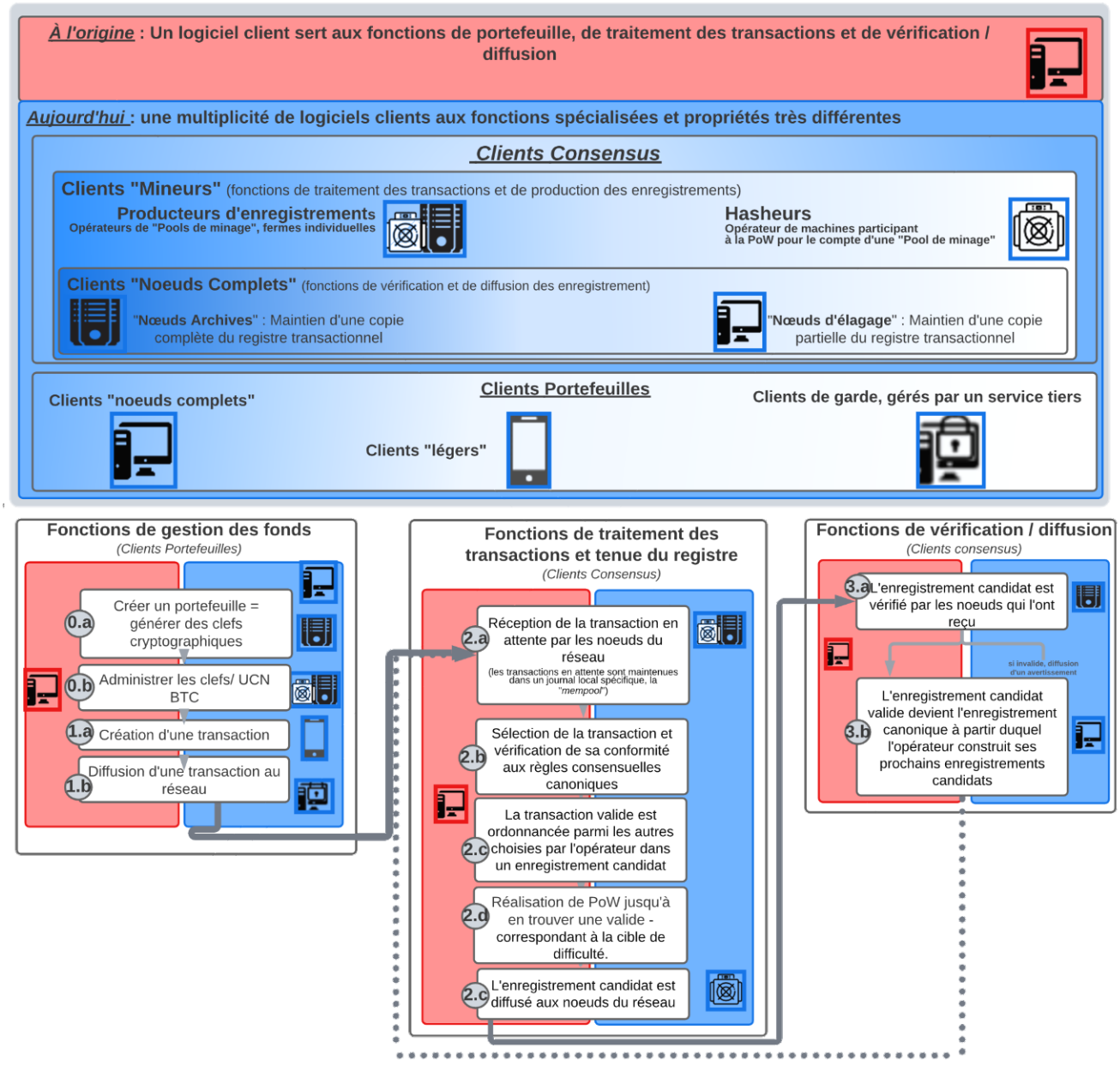
Parmi les diverses improvisations et détournements d'acteurs, attardons-nous sur deux types particulièrement signifiants : la réintermédiation des conditions d'accès à Bitcoin (portefeuille et bourse d'échange) et celle entourant l'activité de production des enregistrements (émergence de barrières à 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++[153]. Tout utilisateur participe *à* et *use de* Bitcoin *via* ce client logiciel

[153] 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 dupe. 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 intermédiés (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, dédiées 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 artisanaux 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 FGPA) verra aboutir le mouvement dans l'élaboration de machines dédiées produites de manière industrielle : les fameux ASICs[154] (« *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[155], 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

---

[154] 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)

[155] 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[156]. 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[157]. 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 *bitcoiners** : 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[158].

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

[156] 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 [consultation au 15/05/2015]).

[157] 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)

[158] Voir cette discussion Twitter initiée par Angela Walch à laquelle nous avions pris part : 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[159] (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 la 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[160]. 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[161]. 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* »[162] (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

[159] 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'érigeant 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'« e*lle 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 démontra son efficacité, en une journée la part retombe « *à 38%, contre 42%* » (Hajdarbegovic 2014).

[160] 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 implémentés (Nakamoto 2010a).

[161] 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 arrêtiez 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).

[162]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[163]. La limite de 1 Mo n'a été introduite que le 15 juillet 2010[164] 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 (Croman 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*

[163] 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 » implémentée dans les clients logiciels antérieurs à la version 0.8 (Voir https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki ou Buterin 2013) [consultation au 03/08/2020].

[164] 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;[1] ») https://github.com/bitcoin/bitcoin/commit/a30b56ebe76ffff9f9cc8a6667186179413c6349), elle est implémentée 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[165]. Finalement, ces régulations transactionnelles prescrivent (et proscrivent 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'*Altcoin*s*, à laquelle Bitcoin a ouvert la voie. En outre, ce développement ne sera abordé que

[165] 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 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 crypto-monétaire 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. Nakomoto 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)[166]. 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[167] (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

[166] 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).

[167] Données tirées du site référence CoinGecko (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)[168]. 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[169] (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 (Whitebbit1111 2022).

Sans aller au fond de ses mécanismes[170], 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 est 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

[168] 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.

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

[170] 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 (clefs) et d'attacher des données (valeurs) à ces clefs 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.*)[171]. 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* »[172]. Nakamoto vient d'inventer le « merge mining » (ou « *AuxPoW** ») qu'emprunte effectivement Namecoin en guise de consensus de PoW*[173] (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.

---

[171] 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].

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

[173] Voir https://bitcointalk.org/index.php?topic=1790.0 ; https://bitcointalk.org/index.php?topic=1790.msg28938#msg28938 ; et 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 cèdent 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 étayent, ce que certains perçoivent comme problématique. La pléthore 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 concerner 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 différenciées. 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[174]. 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[175]. 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*)[176]. 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 essentie[l] à long terme.* » (Sunny King et Nadal 2012, p. 1). Il est présenté comme un « *dérivé du Bitcoin* », plus économe en énergie quant à la découverte d'un nouvel en-tête d'enregistrement* valide[177]. 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*

---

[174] 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).

[175] 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)

[176] 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)

[177] 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[178] *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 *minteurs*. 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 déterminantes : « *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[179]. 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[180]. La distribution des XRP n'est pas la contrepartie de contributions encadrées par les règles protocolaires, mais

[178] 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)

[179] 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].

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

à la discrétion des fondateurs qui s'en sont réservé 20%[181], 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[182] 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[183]), 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[184]. 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 nœuds* de statut différent structurent le réseau* : les nœuds* simples, qui s'occupent des transactions* standards en PoW*, et les nœuds* 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

[181] 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. Brittoa, quant à lui, a reçu 1 milliard (avec accord de séquestre) (BitMEX Research 2018).

[182] 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.

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

[184] 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[185]) -, 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 pétahashs 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*

[185]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 »[186] 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 métaprotocoles 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 métaprotocole « 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 métaprotocoles doit renforcer « *la valeur et le succès du protocole Bitcoin de base »*, puisqu'il

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

« *bénéficie 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[187] 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'exchange 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 »[188] 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[189] 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[190]. 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

[187] Voir https://blockchair.com/bitcoin/address/1CounterpartyXXXXXXXXXXXXXXXUWLpVr [consultation au 02/09/2022].

[188] 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 [consultation au 02/09/2022].

[189] 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)

[190] 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)[191]. 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 métaprotocoles et leur logique de fonctionnement sont critiqués techniquement : 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 métaprotocoles 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.*).

[191] « 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 connut 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 obéraient le développement futur des solutions de pièces colorées ou des métaprotocoles, 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 métaprotocoles 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 idéel 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 métaprotocoles. Ils connaissent donc bien les heurs 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)[192]. 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[193] (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*

[192] 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].

[193] 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[194].

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[195], 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[196]. 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

[194] 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'enliser 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.

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

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

Python (Buterin 2014c)[197]. 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* »[198] 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)[199]. 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)[200]. 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

---

[197] 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 multicœur. 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.

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

[199] 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].

[200] « *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 »[201]. 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[202]), 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* »[203]. 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[204] (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[205]. En seulement 12 heures, 3 700 BTC sont

[201] 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* ».

[202] 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.

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

[204] 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).

[205] 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[206] (pour une valeur de 18 Millions de $ à l'époque)[207]. 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*[208]. Ce lancement effectif sera précédé d'efforts marketing, comme avec l'organisation de conférences dédiées à Ethereum (exemple de la *ÐΞVcon-0,* à Berlin le 24 novembre 2014[209]) 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.

I.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

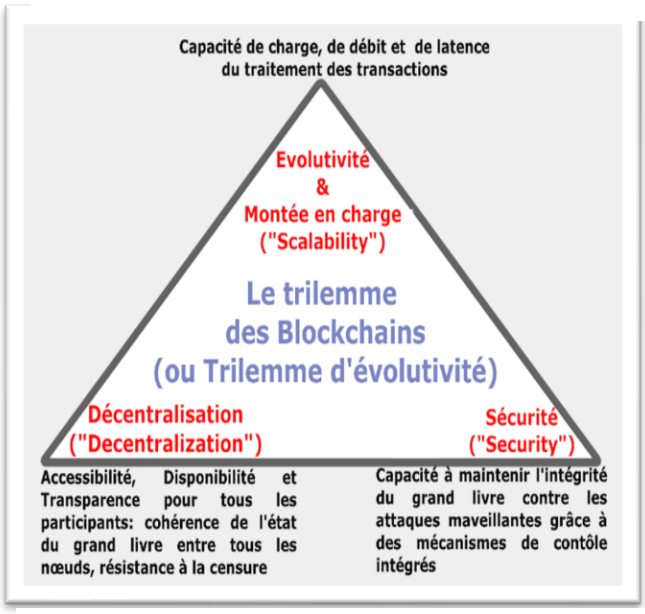
Buterin vise en premier lieu à éviter la fragmentation induite par les stratégies précédentes : différentes technologies nécessitent différentes connaissances, outils et savoir-faire (chaque CM possède différentes suites logicielles, etc.), reposant sur différentes communautés. Ensuite, créer de nouveaux 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 métaprotocoles) : « *le protocole de bas niveau sur lequel ils essaient de construire*

---

[206] Voir https://www.blockchain.com/btc/address/36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2?filter=2# [consultation au 02/04/2022].
[207] 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].
[208] Consultable ici : https://etherscan.io/txs?block=0 [consultation au 03/04/2022].
[209] 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

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 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 épigraphe 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'« a*jouter 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,

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[210].

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

[210] 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[211], 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)[212] 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 notoire, 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.*) qui en déterminent deux grands types distincts (*Ibid*, Polrot 2017) :

[211] 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.

[212] 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/reglées *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 nœuds* 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 signifiantes 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 encline 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* »)[213]. 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, érigeant 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*

[213] 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 »)[214] 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[215]. 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)[216].

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

---

[214] 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).

[215] 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*.

[216] 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 retarde 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. Comprenons 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[217]), 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'expliciter.

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[218] (devant couvrir les coûts mémoires et computationnels afférents): « *généralement, une étape de calcul coûte 1 gaz, mais certaines opérations coûtent davantage*

[217] 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 nœud* 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).

[218] 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 accidentelles 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 discrétion 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 contempteurs, 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 idéel). 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.