L'Élégance de Bitcoin

L'Élégance de Bitcoin

Histoire, enjeux et principes

Ludovic Lars

KONSENSUS NETWORK

L'Élégance de Bitcoin : Histoire, enjeux et principes

Version : v1.3.0

Typesetting : Konsensus Network

Conception de la couverture : ImTechnicolor

ISBN 978-9916-723-61-6 Hardcover
978-9916-723-62-3 Paperback
978-9916-723-63-0 Ebook

KONSENSUS NETWORK ★ https://konsensus.network

« Messieurs, s'écria-t-il d'une voix sonore qui s'adressait à tous, le prince affirme que la beauté sauvera le monde ! »

Fiodor M. Dostoïevski,
L'Idiot

Préface de Jacques Favier

Ludovic Lars est assez unanimement considéré comme l'un des grands « érudits » francophones en matière de Bitcoin. Ce mot, qui est revenu dans plusieurs conversations au sujet de son projet éditorial, m'a inspiré le fil de trame de cette préface.

En me faisant l'honneur de me demander celle-ci, il m'avait prévenu que le ton « libéral » de son *Élégance du Bitcoin* pourrait trancher avec ma propre sensibilité. J'y ai perçu une forme d'*élégance* morale. En vérité, l'auteur a lu les économistes dits « autrichiens » mais aussi Proudhon et il n'est pas davantage que moi maximaliste buté ou toxique. Étant surtout ennemi des extrémismes idéologiques et des raisonnements à une seule dimension, je ne saurais m'offusquer de ce qu'au sein d'une communauté supportant l'essor de solutions décentralisées règnent des opinions différentes, avec ce que cela implique comme visions ou comme biais.

Tout en assumant ce que l'on appelait jadis un vrai « travail de bénédictin » l'auteur a d'ailleurs demandé et obtenu la confiance de multiples spécialistes qui ont assuré à son travail une prise en compte d'un très large spectre de connaissances et une relecture soigneuse. Il y a eu, au-delà de ce concours d'experts, un véritable engagement communautaire, financier et moral pour que soit publié le présent livre.

On trouvera donc ici un travail qui, tant par un ton rarement polémique que par une profonde érudition et une inscription dans un mouvement collectif, participe de la tradition de l'*Encyclopédie* française. On sait que les promoteurs de la *Britannica* accusèrent celle de Diderot et d'Alembert de « propager l'anarchie » et l'on ne peut nier que, rédigée alors qu'éclosaient les Lumières,

cette somme des connaissances de toute nature – tant théoriques que pratiques – n'ait pris courageusement parti dans les combats politiques et philosophiques de son temps, avec l'intention explicite d'ouvrir une réflexion critique et de « changer la façon commune de penser ». Sans doute pourrait-on en dire autant ici : Bitcoin et ce livre ne vous invitent pas tant, ou pas seulement, à changer de monnaie qu'à changer de pensée.

Ayant senti cela, je suis allé fureter dans l'*Encyclopédie*. L'article « érudition », rédigé par d'Alembert lui-même, expose que celle-ci « renferme trois branches principales, la connaissance de l'Histoire, celle des Langues, & celle des Livres ». En changeant peut-être *langues* par *protocoles*, il aurait pu goûter lui-aussi et préfacer mieux que moi le livre que vous venez d'ouvrir.

Mon propre esprit, formé aux études historiques, s'est délecté des premiers chapitres, qui constituent de véritables Annales de Bitcoin. Les historiens d'aujourd'hui et de demain ne pourront qu'apprécier l'ampleur des informations fiables et des références compilées. Mathématicien de formation, l'auteur a produit d'abord un très important travail archivistique, dont atteste près d'un millier de notes savantes.

Comme me l'a écrit le créateur du site Bitcoin.fr « il déniche et déchiffre des débats abscons qui ont pourtant eu une importance capitale dans l'évolution du protocole, et les rend compréhensible à tous ». Ainsi, si ce qu'il restitue de l'histoire de la monnaie peut être critiqué ou remis dans la perspective de ses convictions personnelles, ce qu'il construit de l'histoire de Bitcoin est un apport dont d'autres feront utilement leur miel.

Au-delà de l'Histoire, il y a donc les Langues et les Livres : des références, du code, de la théorie des jeux et des mathématiques. Il y a beaucoup à glaner dans ces pages, dont beaucoup de choses austères mais aussi de petits faits plaisants. Si le livre narre en détail l'inévitable geste de la fameuse pizza, il rappelle aussi qu'un robinet à bitcoin a fonctionné 2 ans en envoyant 5 bitcoins à chaque demande, ou que celui qui a découvert la première faille a gentiment prévenu Satoshi au lieu de profiter de sa découverte pour tricher. Il souligne ainsi qu'avant sa phase de « croissance conflictuelle » les premières années de l'aventure ont vu « une croissance organique et prudente, à l'abri de l'opportunisme et de la propagande de notre monde » et que la communauté a fait montre, depuis l'origine, d'une extraordinaire résilience, chose qui doit être méditée.

L'abondance des citations rend justice aux cypherpunks, parfois traités comme de sinistres sires fomentant une révolte fiscale autour d'un intempestif barbecue. Elle restitue la profondeur historique et intellectuelle de ce

qui fut un mouvement de fond collectif et non une réaction épidermique sectaire. Accessoirement, les trajets individuels finement retracés montrent que l'influence autrichienne, non négligeable, ne fut ni universelle ni complète. Bien des cryptographes, cypherpunks ou non, n'y ont pas adhéré comme à un dogme révélé ou à une vérité scientifiquement établie.

Ludovic Lars rappelle en outre ce point crucial : les cypherpunks ne furent pas les seuls à essayer de construire des systèmes distribués qui puissent servir à l'échange monétaire. Parce qu'il y avait un vrai problème et un vrai besoin. Dans le bouillonnement intellectuel, les échanges étaient nombreux : il est amusant de rappeler que Ripple s'inspira aussi du localisme des SEL ! En fait la différence avec toutes les autres tentatives c'est que Bitcoin (le premier à ne pas reposer sur une confiance au sens classique) a réussi comme monnaie parce qu'il a réussi à construire une communauté élective, philosophique, politique. Bitcoin est la plus large monnaie communautaire de tous les temps.

S'intéresser à sa (longue) geste avant autant qu'après 2009 n'est donc pas une marotte d'historien. Outre une compréhension indispensable de ses racines, des intentions et des ambitions qui animaient précurseurs et témoins de sa naissance, on trouve de quoi démonter bien des escroqueries intellectuelles hélas persistantes. Non, les monnaies numériques de banques centrales ou les *stablecoins* algorithmiques ne représentent pas des perfectionnements de Bitcoin ni d'ailleurs des promesses d'amélioration de notre existence à venir.

Les *altcoins* plus ou moins communautaires, souvent entrepreneuriaux voire bancaires, sont largement cités, essentiellement pour illustrer le propos, l'enrichir d'exemples, souligner des impasses ou des objections, jamais, il faut le répéter, et même si l'auteur les connaît fort bien, pour « dépasser » ou « perfectionner » Bitcoin, dont le développement organique et le perfectionnement est l'affaire des bitcoineurs.

L'auteur est un expert technique mais il sait aussi écrire. Tout ce qui est technique (et ignoré par beaucoup de gens, même de ceux qui se présentent comme des « experts »), tout ce que d'Alembert nommerait « les Langues » est disséqué dans cet ouvrage avec un scalpel extrêmement méticuleux et restitué dans la langue où ce qui est bien conçu « s'énonce clairement ». Ceci mériterait d'être donné à lire au prochain politique, financier, économiste ou publiciste qui dira que « ça ne repose sur rien » !

Le titre du livre est aussi celui d'une conclusion agréablement équilibrée, entre ceux qui voient en Bitcoin la solution à tout et ceux qui n'y voient que du mal. Elle pourra surprendre certains adeptes fervents et naïfs mais elle reste dans l'esprit de d'Alembert : « Il y a dans la critique deux excès à fuir

également, trop d'indulgence, & trop de sévérité ».

Curieusement, l'auteur s'appesantit peu sur le mot d'*élégance* lui-même, que sa formation mathématique lui fait sans doute percevoir comme embrassant les sens de vérité, de beauté et de rigueur. Comme Aristote, il a pu penser ici à l'ordre, à la précision, à la capacité de faire jouer ensemble plusieurs concepts, de les ajuster ensemble efficacement, performance que Satoshi Nakamoto a réalisée au plus haut point.

Pour m'adresser au lecteur au seuil de ce livre utile, dense et à tous égards distingué, je donne une dernière fois la parole à d'Alembert qui opinait que « les secours que nous avons aujourd'hui pour l'érudition la facilitent tellement, que notre paresse seroit inexcusable, si nous n'en profitions pas ».

Jacques Favier, le 21 novembre 2023

Remerciements

Un ouvrage n'est jamais le fruit du seul travail de son auteur attitré. Ce dernier est toujours aidé, financé, encouragé, inspiré par d'autres personnes. Le livre que vous tenez entre les mains, ou que vous observez sur un écran, n'échappe pas à la règle. Je tiens par conséquent à remercier l'intégralité des gens qui m'ont apporté leur assistance d'une manière ou d'une autre, et en particulier la communauté francophone de Bitcoin qui a été là pour soutenir ce projet.

Je remercie d'abord mes lecteurs pour m'avoir lu et avoir partagé mes articles. Un créateur n'est rien sans son public. Je suis spécialement reconnaissant envers JohnOnChain pour son soutien de la première heure vis-à-vis de ma démarche d'écriture. Merci aussi aux gens derrière Cryptoast et le Journal du Coin avec qui j'ai pu travailler pendant des années.

Je remercie ceux qui m'ont aidé à mettre en place la campagne de financement en mars 2022. Merci à Lounès Ksouri pour ses conseils à propos d'Umbrel. Merci à Benjamin Favre pour son aide à la mise en place de la campagne sur le serveur. Merci à CryptoSou pour m'avoir apporté de la liquidité sur Lightning quand j'en ai eu besoin.

Je remercie les contributeurs au financement du projet, par ordre alphabétique : Yanis Adoul, Autrement, Valentin Becmeur, Bitcoin.fr, btcfork, Caulla, Chamigrou, Copinmalin, CryptoSou, Steve Deplus, Marek Fijalkowski, Édouard Gallego, Alexandre Gonzalez, Gladsponk, Greglem, Grittoshi, Benoît Huguet, ImTechnicolor, Jacques-Edouard, Jazaronaut, Lionel Jeannerat, Jeffbeck, JohnOnChain, Clément Junca, François Juno, Jybe, Kolkoz, Mike Komaransky, Konohime, Maxime Kouamen, Lounès Ksouri, Les-

lie, Louferlou, Marco.BTC.fr, Loïc Morel, Ali Mitchell, Yorick de Mombynes, Nexus 8, Leonardo Noleto, Olivier, Romain Pariset-Wagnon, PaulADW, Pivi, RaHaN, Anthony RoBin, Robin de Cryptoast, Rogzy, Thibaut Spanier, André Stilmant, François-Xavier Thoorens, Trigger, ainsi que tous ceux qui ont souhaité préserver leur anonymat.

Je remercie les relecteurs des premières versions de cet ouvrage, qui m'ont donné de bons conseils pour l'améliorer, tant au niveau de la forme que du fond. Merci à Jybe, ProfEduStream, Loïc Morel, Steve Deplus, Alexandre Gonzalez, Romain Daubigny (Recktosaurus), Pierre L. (alias Scrypto), Jacques-Edouard de BTC Touchpoint, Bastien Desteuque, Cédric, Meffysto, Beemo, Caroline et Marie-Christine, Gloire Wanzavalere, Gatien, et Martin Pellemoine.

Je remercie l'équipe de Konsensus, la maison d'édition spécialisée qui publie ce livre. J'ai une immense gratitude envers Édouard Gallego pour son soutien indéfectible dans l'édition de cette œuvre. Merci aussi à David St-Onge pour ses conseils éditoriaux. Merci également à l'illustrateur de talent ImTechnicolor qui a produit la présente couverture.

Je remercie profondément Jacques Favier, cofondateur du Cercle du Coin et coauteur de trois ouvrages sur Bitcoin en français, qui m'a fait l'honneur de lire l'intégralité de l'ouvrage et d'en rédiger une superbe préface.

Je rends évidemment hommage à Satoshi Nakamoto pour avoir découvert Bitcoin et l'avoir partagé au monde. Merci aussi à toutes les personnes qui m'ont permis de mieux comprendre Bitcoin au cours du temps, et en particulier à Andreas Antonopoulos, Julia Tourianski, Eric Voskuil et Aaron van Wirdum.

Merci enfin à mes proches – à ma famille et à mes amis – qui ont été des soutiens essentiels au cours de ces longs mois d'écriture et de relecture.

Avant-propos

Depuis sa conception en 2008 par Satoshi Nakamoto, Bitcoin a fait couler beaucoup d'encre. Au fil des années, il a suscité les plus grandes passions et il a été l'objet récurrent de débats enflammés. À son sujet, des milliers d'articles ont été écrits, des centaines de vidéos ont été tournées, et des dizaines de livres ont été publiés. La hausse de son prix lui a donné une visibilité extraordinaire dans les médias, à tel point qu'il s'est fait une place dans l'imaginaire collectif mondial.

Cependant, Bitcoin reste largement incompris. D'un côté, beaucoup de gens en parlent en n'ayant qu'une connaissance artificielle du sujet et ne parviennent pas à distinguer son utilité. Certains pensent qu'il ne sert qu'à spéculer, d'autres imaginent qu'il ne devrait être utilisé que par les criminels, d'autres encore vont jusqu'à dire qu'il ne s'agit que d'une pyramide de Ponzi. De l'autre côté, un certain nombre de personnes nourrissent des attentes démesurées, pensant qu'il pourrait devenir la monnaie de réserve mondiale, voire remplacer tous les échanges monétaires dans l'économie en quelques années seulement. Dans cette délusion, elles s'attachent à l'espoir que son prix atteigne des niveaux stratosphériques, dans la continuité des hausses spéculatives précédentes. Toutefois, peu de gens tentent d'adopter un point de vue réaliste et sobre, qui ferait la part des choses entre la vision des vendeurs de rêve pour qui Bitcoin serait la solution à tous les problèmes du monde, et les détracteurs de mauvaise foi pour qui Bitcoin représenterait un fléau à arrêter à tout prix.

J'ai personnellement entendu parler de Bitcoin pour la première fois en avril 2013, à la suite de la crise financière chypriote. Initialement assez scep-

tique, je me suis quand même intéressé à ce système, car celui-ci était mis en avant par les libéraux français et les libertariens américains que je suivais. Le 9 juillet 2015, j'ai essayé la chose : je me suis procuré 50 € de bitcoins (0,2 BTC) auprès de la plateforme d'achat-vente suisse Fastcoin (nommée aujourd'hui Bity) que j'ai reçus sur mon portefeuille Electrum nouvellement créé. J'ai réalisé ma première transaction sur la chaîne de Bitcoin dans la journée. Ces quelques fractions de bitcoin m'ont servi à faire des dons : d'abord au blogueur H16, puis à l'activiste Adam Kokesh, ensuite au projet DarkWallet de Amir Taaki et Cody Wilson, et enfin à la plateforme Sci-Hub gérée par Alexandra Elbakyan.

Mon implication dans Bitcoin n'a débuté réellement qu'au printemps 2017, lorsque le prix a recommencé à monter après des années de stagnation. Jusque-là, je m'étais contenté de suivre la cryptomonnaie de loin et cette hausse m'a intrigué. C'est à ce moment-là que je me suis pleinement plongé dans cet univers. J'ai lu à ce propos, notamment en me procurant des ouvrages comme *Bitcoin, la monnaie acéphale* d'Adli Takkal-Bataille et Jacques Favier, *Mastering Bitcoin* d'Andreas Antonopoulos ou encore *Digital Gold* de Nathaniel Popper. Je me suis également mis à spéculer à mon échelle en achetant du bitcoin, puis toutes sortes de cryptomonnaies alternatives.

En parallèle, j'ai commencé à écrire sur le sujet, si bien que je suis devenu rédacteur pour des sites spécialisés comme Cryptoast et le Journal du Coin. Au fil des années, j'ai rédigé plus de 150 articles de fond, sur divers sujets liés à la cryptomonnaie, que ce soit sous un angle technique, économique ou politique. Ma vision de Bitcoin a mûri en conséquence, de telle sorte que je pouvais prétendre « comprendre Bitcoin », même si ma conception restait évidemment parcellaire et influencée par ma propre perspective.

Cependant, ce n'était pas forcément le cas autour de moi, où les gens en avaient une idée superficielle, n'ayant probablement pas le temps de creuser davantage. C'est ce qui m'a poussé à écrire ce livre. En particulier, puisque le protocole monétaire dépendait des actions économiques de ses utilisateurs, il me paraissait important de partager la connaissance réelle qui avait émergé de mes recherches et de mon expérience. De plus, avec la progression de la censure bancaire, le développement des monnaies numériques de banque centrale, la guerre contre l'argent liquide et le retour de l'inflation, je pense qu'il est plus que jamais essentiel de bien appréhender cet outil afin de pouvoir l'utiliser correctement à l'avenir.

Cet ouvrage a pour but de présenter Bitcoin de manière claire et complète, en adoptant de multiples points de vue. Il narre le long cheminement qui a mené

à sa création, ainsi que sa courte mais dense histoire, des origines à aujourd'hui. Il décrit son fonctionnement essentiellement économique découlant de sa nature monétaire. Il aborde les enjeux politiques auxquels Bitcoin répond, et en particulier le problème de la censure. Enfin, il examine ses rouages techniques de manière détaillée et précise. En lisant ce livre, vous finirez peut-être, comme moi, par voir en Bitcoin un ensemble harmonieux, dont le modèle de base est d'une rare élégance.

J'espère en tout cas que vous saurez apprécier cette modeste contribution à quelque chose qui nous dépasse : le projet d'une monnaie alternative, libre et résiliente, offrant aux simples individus la possibilité de résister aux puissances de ce monde. *Vires in numeris*.

Ludovic Lars, le 1er décembre 2023

Table des matières

1

Les débuts de Bitcoin

Le 31 octobre 2008, un individu se faisant appeler Satoshi Nakamoto partageait sur Internet un court document qui décrivait le fonctionnement technique d'un système novateur de monnaie numérique : Bitcoin. Ce livre blanc de 9 pages, présenté comme un article scientifique, s'intitulait en anglais *Bitcoin: A Peer-to-Peer Electronic Cash System – Bitcoin : un système d'argent liquide électronique pair à pair*. Dans celui-ci, Satoshi proposait une solution au problème des paiements en ligne, par la mise en œuvre d'un serveur d'horodatage distribué basé sur un algorithme de preuve de travail.

Mais cela allait beaucoup plus loin. Le livre blanc de Bitcoin posait les bases d'une révolution conceptuelle profonde : une monnaie exclusivement numérique qui ne reposait sur aucun tiers de confiance, ni pour la confirmation des transactions, ni pour l'émission des nouvelles unités. Ce que Satoshi venait de découvrir, c'était bien plus qu'un système de paiement ; c'était un nouveau type de monnaie, quelque chose que nul n'avait su concevoir jusqu'alors, un phénomène économique et social qui rencontrerait un succès inouï au cours des années qui suivraient.

En particulier, la création de Satoshi Nakamoto réalisait le vieux rêve d'une monnaie numérique échappant au contrôle de l'État : un rêve cher aux cypherpunks dont le mouvement, remontant au début des années 1990, prônait l'utilisation proactive de la cryptographie dans le but d'assurer la confidentia-

lité et la liberté des individus sur Internet. Ces cryptographes rebelles avaient en effet désiré et tenté de concevoir un tel argent liquide électronique pendant des années, celui-ci étant un élément constitutif de leur idéal. Malheureusement, cela n'avait pas abouti, du moins jusqu'à l'apparition de Bitcoin.

À partir de cette date fatidique, Bitcoin a été mis en œuvre et a connu un certain nombre d'évènements fondateurs qui l'ont mené où il est aujourd'hui. Ces évènements ont façonné la compréhension que nous en avons, et l'histoire des débuts de Bitcoin constitue donc un récit unique qu'il convient de raconter.

Une naissance difficile

Bitcoin a été conçu par un individu qui utilisait le pseudonyme de Satoshi Nakamoto et prétendait être un homme japonais de 33 ans [1]. On sait peu de choses sur lui en dehors de ses messages publics et du code informatique qu'il a publié. Satoshi a disparu en 2011, et on ignore s'il est toujours vivant.

D'après son propre témoignage, Satoshi Nakamoto se met à travailler sur Bitcoin au printemps 2007. Pendant plus d'un an, il garde son modèle secret, souhaitant être sûr qu'il fonctionne correctement avant de le présenter au monde. Il affirmera ainsi avoir codé le prototype avant d'écrire le papier [2].

En août 2008, Satoshi a terminé de rédiger le livre blanc et commence à préparer l'annonce de la sortie de Bitcoin. Le 18 août, il réserve le nom de domaine Bitcoin.org via le service anonyme AnonymousSpeech [3]. Le nom de domaine sera utilisé pour héberger le site principal de Bitcoin.

Quelques jours plus tard, il rentre en contact avec Adam Back, le cryptographe et cypherpunk britannique à l'origine de Hashcash, la technique utilisée dans Bitcoin pour calculer la preuve de travail. Adam Back le renvoie vers le cryptographe Wei Dai, inventeur en 1998 du concept de b-money, un concept qui possède des similarités notables avec Bitcoin. Le 22 août, Satoshi envoie donc un courriel à Wei Dai pour lui dire qu'il « se prépare à publier un document qui étend [ses] idées à un système complètement fonctionnel » et pour lui demander « l'année de publication de [sa] page sur la b-money » afin d'y faire référence dans le livre blanc [4]. Cependant, malgré ces interactions, Adam Back et Wei Dai ne s'intéressent pas à Bitcoin immédiatement. Ce ne sera que des années plus tard qu'ils reviendront vers la découverte révolutionnaire de ce mystérieux personnage.

À l'automne 2008, Satoshi décide de rendre public son système. Le 5 octobre, il s'inscrit sur la plateforme de gestion de projets SourceForge, là où le code source ouvert de Bitcoin sera hébergé et maintenu jusqu'en 2011. Le 31 octobre, il publie le livre blanc sur une liste de diffusion de courrier

électronique dédiée à la cryptographie. Cette liste est la *Metzdowd Cryptography Mailing List* gérée par Perry Metzger sur son site web Metzdowd.com où participent un certain nombre d'anciens cypherpunks [5]. Dans son courriel d'introduction, il écrit :

> « J'ai travaillé sur un nouveau système d'argent liquide électronique qui est entièrement pair à pair, dépourvu de tiers de confiance [6]. »

Le livre blanc est centré sur le problème des paiements en ligne et le but de Bitcoin est clairement énoncé dès le début :

> « Le commerce sur Internet repose aujourd'hui presque exclusivement sur des institutions financières qui servent de tiers de confiance pour traiter les paiements électroniques. Bien que ce système fonctionne assez bien pour la plupart des transactions, il souffre toujours des faiblesses inhérentes à son modèle basé sur la confiance. [...] Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur des preuves cryptographiques plutôt que sur la confiance, qui permettrait à deux parties volontaires de réaliser directement des transactions entre elles sans avoir recours à un tiers de confiance [7]. »

D'un point de vue technique, il s'agit de mettre en place un registre de transactions distribué sur un réseau pair à pair et ouvert d'ordinateurs. Ce registre est composé de blocs de transactions qui sont liés les uns à la suite des autres au cours du temps, formant une « chaîne de blocs ». Bitcoin constitue ainsi un « serveur d'horodatage distribué », qui répertorie l'ordre des transactions de façon à créer un historique cohérent, sans « double dépense ». Cela permet de gérer l'émission et les échanges d'une unité de compte numérique, qui sera appelée le bitcoin.

La fiabilité du système repose sur des « preuves de travail » qui lient les blocs entre eux de façon à rendre difficile la modification de la chaîne. Ces preuves sont produites périodiquement par des membres du réseau qui fournissent de l'énergie pour cela et qui sont rémunérés par une « incitation » en bitcoins composée des unités nouvellement créées et des frais de transaction. Les personnes qui dépensent ainsi leur énergie électrique sont comparées par Satoshi aux « mineurs d'or qui dépensent des ressources pour ajouter de l'or dans la circulation », d'où le nom de mineurs qu'ils prendront plus tard.

Suite à l'annonce de Bitcoin et la publication du livre blanc, Satoshi reçoit peu de réponses, et beaucoup d'entre elles sont sceptiques. D'abord, le cypherpunk James A. Donald remet en cause le passage à l'échelle du système en disant qu'« il ne semble pas pouvoir s'adapter à la taille requise [8] ». Ensuite, John Levine critique sa sécurité en évoquant la puissance de calcul détenue par

les « fermes de machines zombies [9] » composées d'ordinateurs contrôlés par des pirates. Enfin, un troisième individu du nom de Ray Dillinger s'interroge sur la valeur de l'unité de compte, déplorant le fait que « les preuves de travail informatiques n'ont pas de valeur intrinsèque [10]. »

Cependant, cet accueil sceptique n'est pas partagé par l'intégralité des personnes inscrites sur la liste de diffusion. En particulier, Hal Finney, un informaticien et cryptographe américain d'une cinquantaine d'années, est résolument enthousiaste et écrit dans son message du 7 novembre que « Bitcoin semble être une idée très prometteuse [11] ». Hal Finney n'est pas une personne comme les autres : il s'agit d'un membre historique du mouvement cypherpunk qui a participé au développement du logiciel de chiffrement PGP dans les années 90 aux côtés de Philip Zimmermann, qui a expérimenté avec les premiers systèmes de monnaie électronique et qui a même tenté de créer son propre système de preuves de travail réutilisables. Malgré son expérience, il reste optimiste et devient ainsi le tout premier soutien de Satoshi dans son projet. Quelques années plus tard, il déclarera à ce sujet que « les cryptographes grisonnants [...] ont tendance à devenir cyniques » mais que lui « était plus idéaliste » ayant « toujours aimé la cryptographie, son mystère et son paradoxe [12]. »

Par la suite, Satoshi distribue les principaux fichiers du code aux personnes intéressées, dont notamment Hal Finney, Ray Dillinger et James A. Donald [13]. Hal et Ray réalisent alors un examen minutieux du code, en se concentrant chacun sur une partie spécifique du système. Ce code inclut déjà tous les éléments constitutifs de Bitcoin. Le prototype est alors prêt à être lancé.

Une enfance timide

Deux mois après la publication du livre blanc, le 8 janvier 2009 à 19 heures 27, Satoshi Nakamoto partage la première version du logiciel sur la liste de diffusion de Metzdowd. Le code source en C++ est publié de manière ouverte sous licence libre (MIT), de sorte que n'importe qui peut copier, modifier et utiliser le logiciel à sa guise. Celui-ci contient les données du bloc de genèse, le premier bloc de la chaîne à partir duquel celle-ci doit se prolonger.

Quelques heures plus tard, Satoshi commence à miner. Le deuxième bloc de la chaîne, le bloc 1, est validé par Satoshi le 9 janvier à 2 heures 54 du matin, ce qui marque le lancement effectif du réseau.

Le 10 janvier, Hal tente de faire fonctionner le logiciel. Après avoir échangé avec Satoshi pour faire en sorte que le logiciel fonctionne, il se met à miner

et trouve son premier bloc (le bloc 78) à 1 heure du matin (UTC), gagnant de ce fait 50 bitcoins. Deux heures et demie plus tard, il partage son expérience sur Twitter (média social alors naissant) en écrivant « *Running bitcoin* [14] ». Le lendemain, dans la nuit du 11 au 12 janvier, Satoshi envoie 10 bitcoins à Hal par l'intermédiaire de son adresse IP : il s'agit du premier transfert d'une personne à une autre sur le réseau [15].

Hal n'est pas la seule personne à expérimenter sur le réseau à ce moment-là : c'est également le cas de Dustin Trammell, un chercheur en sécurité informatique américain ayant découvert Bitcoin par la liste de diffusion. Celui-ci communique aussi avec Satoshi par courriel, et reçoit 25 bitcoins de sa part le 15 janvier [16].

Mais les quelques personnes qui font fonctionner le logiciel ne suffisent pas. Dès le début, Satoshi sait bien que peu de gens se sont penchés sérieusement sur son modèle et qu'il va être compliqué d'attirer de nouveaux utilisateurs et contributeurs. C'est pourquoi il essaie de susciter l'enthousiasme en vendant son idée du mieux possible.

Le premier élément est le programme d'émission du bitcoin, qui a pour limite 21 millions d'unités. Dans le courriel d'annonce du prototype, Satoshi explicite le rythme de création monétaire :

> « Le nombre total de pièces en circulation sera de 21 000 000. Elles seront distribuées aux nœuds du réseau lorsqu'ils créeront des blocs, la quantité émise étant divisée par deux tous les 4 ans. [...] Une fois cette somme épuisée, le système pourra prendre en charge les frais de transaction si nécessaire [17]. »

Le bitcoin a donc vocation à devenir une monnaie à offre fixe, déflationniste par nature, et cette particularité crée un enthousiasme. Le 11 janvier, Hal Finney est le premier à réagir en se réjouissant du fait que « le système peut être configuré de manière à n'autoriser qu'un certain nombre maximum de pièces à être générées ». Il estime que si « Bitcoin [est] un succès et [devient] le système de paiement dominant utilisé dans le monde entier », chaque pièce aura alors « une valeur d'environ 10 millions de dollars [18] ». L'estimation est contestable mais le raisonnement reste pertinent en raison du fonctionnement de Bitcoin.

Le 16 janvier, Satoshi reprend ainsi cet élément de communication dans un courriel qu'il partage à la liste de diffusion, où il déclare qu'il « pourrait être judicieux de s'en procurer au cas où le phénomène prendrait de l'ampleur » et que « si suffisamment de gens pensent la même chose, on pourra assister à une prophétie autoréalisatrice [19] ». Cet élément est crucial, comme le montre le témoignage de Dustin Trammell qui confie à Satoshi que le raisonnement

de Hal est « l'une des raisons pour lesquelles [il a] démarré un nœud si rapidement ».

Outre le programme d'émission du bitcoin, Satoshi choisit de communiquer sur les défaillances du système bancaire, ce qui constitue le deuxième élément dans sa stratégie pour attirer l'attention.

En réalité, il le fait dès le bloc de genèse en y incluant le titre de la une du quotidien britannique *The Times* du 3 janvier 2009 annonçant que le ministre des finances britannique est sur le point de renflouer les banques pour la deuxième fois :

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Cette phrase présente dans le premier bloc de la chaîne possède un rôle double : d'une part, elle empêche l'antidatage en prouvant que le système n'a pas été lancé avant le 3 janvier (Satoshi ne pouvait pas connaître cette une avant) ; d'autre part, elle indique symboliquement ce à quoi Bitcoin s'oppose en faisant référence au contexte monétaire et financier de l'époque.

En janvier 2009, le monde subit en effet de plein fouet les effets de la crise financière amorcée en 2007 par le dégonflement de la bulle immobilière aux États-Unis aussi connu sous le nom de la crise des subprimes. Les États renflouent les banques pour éviter de nouvelles faillites bancaires après celle de Lehman Brothers survenue le 15 septembre 2008, et les banques centrales procèdent à des assouplissements quantitatifs en injectant des liquidités sur les marchés financiers. Cette utilisation d'argent public, qui est littéralement créé pour l'occasion, choque profondément un certain nombre de citoyens qui réalisent que le système bancaire est en fait un système de profits privés et de pertes socialisées.

De par son absence de tiers de confiance, Bitcoin n'est, lui, pas soumis à l'arbitraire d'une banque centrale. Il contraste ainsi avec les monnaies étatiques, telles que le dollar ou l'euro, dont la quantité peut être modifiée arbitrairement par ceux qui contrôlent la création monétaire, au moyen de ce qu'on appelle une politique monétaire. La politique monétaire du bitcoin est programmée, inscrite en dur dans le protocole, pour en théorie ne plus jamais être altérée.

C'est ce que met en avant Satoshi lorsqu'il intervient sur le forum de la Fondation P2P, une organisation étudiant l'impact des infrastructures pair à pair sur la société, le 11 février 2009. Dans son message d'introduction à Bitcoin, il écrit :

« Le problème fondamental de la monnaie conventionnelle est toute la confiance

> nécessaire pour la faire fonctionner. Il faut faire confiance à la banque centrale pour qu'elle ne déprécie pas la monnaie, mais l'histoire des monnaies fiat est pleine de violations de cette confiance. Il faut faire confiance aux banques pour détenir notre argent et le transférer par voie électronique, mais elles le prêtent par vagues de bulles de crédit avec à peine une fraction en réserve [20]. »

Sur son profil, où il indique être un homme de 33 ans habitant au Japon, il donne une date de naissance particulière : le 5 avril 1975. Cette date, probablement fictive et composite, fait vraisemblablement référence à l'interdiction pour les particuliers de détenir de l'or aux États-Unis. Le jour du 5 avril se rapporte au jour de l'instauration de cette interdiction par l'Ordre exécutif 6102 signé par Franklin Delano Roosevelt le 5 avril 1933, et l'année 1975 correspond à son année d'abrogation lors de l'entrée en vigueur de la *Public Law* 93-373. Ce détail n'est pas anodin, puisque cette prohibition a permis en fin de compte d'instaurer un régime monétaire flottant n'ayant plus aucun lien avec l'or.

Ce n'est pas la seule référence aux métaux précieux. Satoshi écrit dans les commentaires le 18 février :

> « Il n'y a [...] personne pour agir en tant que banque centrale ou réserve fédérale afin d'ajuster l'offre monétaire au fur et à mesure que le nombre d'utilisateurs augmente. [...] En ce sens, c'est un système qui se comporte davantage comme un métal précieux. Plutôt que de faire varier l'offre pour que la valeur reste la même, on détermine l'offre à l'avance et la valeur change. À mesure que le nombre d'utilisateurs croît, la valeur par pièce augmente. Cela est susceptible de créer une boucle de rétroaction positive : plus les utilisateurs sont nombreux, plus la valeur augmente, ce qui peut attirer davantage d'utilisateurs désireux de profiter de cette hausse [21]. »

Cette méthode de communication porte peu à peu ses fruits. Ainsi, même si certaines personnes finissent de se détourner de Bitcoin à l'instar de Hal Finney, Satoshi continue de recevoir des messages de la part de personnes intéressées. Le 11 avril 2009, Mike Hearn, un développeur britannique travaillant pour Google et s'adonnant au logiciel libre sur son temps libre, lui envoie un courriel posant une série de questions à propos de Bitcoin, en précisant qu'« il est rare de rencontrer des idées vraiment révolutionnaires [22] ». Hearn s'intéresse alors aux monnaies numériques, et notamment à Ripple.

Début mai 2009, c'est un jeune étudiant en informatique finlandais qui contacte Satoshi : il s'agit de Martti Malmi. Celui-ci a découvert Bitcoin début avril, s'est mis à miner et a même rédigé une courte description de Bitcoin sur le forum de Freedomain Radio où il soutenait l'hypothèse anarchiste que

la monnaie pair à pair pourrait faire disparaître l'État [23]. Dans son courriel à Satoshi, il écrit :

> « J'aimerais aider avec Bitcoin, s'il y a quelque chose que je peux faire. J'ai une bonne connaissance des langages Java et C grâce aux cours que j'ai suivis à l'école (j'étudie l'informatique), mais je n'ai pas encore beaucoup d'expérience en matière de développement [24]. »

Malgré son manque d'expérience, Martti devient dans les mois qui suivent le principal contributeur à Bitcoin en dehors de Satoshi. Étant étudiant, il a en effet beaucoup de temps à consacrer au projet.

En particulier, Satoshi lui confie la charge du site web. Dès le mois de mai, Martti Malmi rédige une première version de la description sur SourceForge où il présente Bitcoin comme une « monnaie numérique anonyme basée sur un réseau pair à pair » permettant de « transférer de l'argent facilement via Internet, sans avoir à faire confiance à des tiers » et d'être « à l'abri de l'instabilité causée par le système de réserves fractionnaires et par les mauvaises politiques des banques centrales [25] ». Cette ébauche servira de base pour la présentation de Bitcoin sur le site web.

À l'époque, le bitcoin n'a pas de prix. Les gens qui testent le système se contentent de lancer le logiciel pour « générer des pièces ». Les transactions sont peu nombreuses, et consistent le plus souvent en des auto-transferts. Les bitcoins sont alors vus comme des objets de collection réservés aux passionnés d'informatique. Les utilisateurs ont l'impression de contribuer à quelque chose, à l'instar des projets de calcul distribué (dits « @home ») où les gens mettent à disposition leurs ressources informatiques au service de bonnes causes.

Certains individus minent en continu. C'est le cas de Hal Finney qui fait fonctionner le logiciel entre janvier et mars, de James Howells qui valide des blocs entre février et avril, de Dustin Trammell qui fait tourner ses serveurs pendant plus d'un an, ou de Martti Malmi qui met son ordinateur portable à profit à partir d'avril. Mais le principal mineur de l'année de 2009 reste Satoshi, qui déploie une puissance de calcul bien plus grande et dont la production de blocs représente près de la moitié de celle du réseau.

En 2009, la difficulté de minage est de 1, ce qui impose à tous les nœuds du réseau de réaliser environ 4,3 milliards de calculs pour miner un bloc, et ce n'est pas rien pour un processeur. De ce fait, la production est plus lente que prévue : entre le 9 janvier 2009 et le 9 janvier 2010, seulement 33 802 blocs sont trouvés sur les 52 560 attendus, ce qui correspond à une durée moyenne entre chaque bloc de 15 minutes et 30 secondes au lieu des 10

minutes prévues. En particulier, le mois d'août 2009 constitue le pire mois pour l'activité minière : seuls 1 564 sur 4 464 blocs attendus sont trouvés, soit un temps moyen de 28 minutes et 30 secondes !

Des premiers pas incertains

Malgré son lancement timide, Bitcoin survit à l'été et franchit une étape cruciale en octobre : son unité de compte acquiert un prix. Un individu utilisant le pseudonyme NewLibertyStandard (NLS), nouvellement arrivé dans la communauté, met en place sur sa page personnelle un service de change permettant aux gens de convertir leurs dollars en bitcoins et inversement. Pour estimer le taux de change, il se base sur le coût énergétique nécessaire pour obtenir un bitcoin, en prenant en compte le coût de l'électricité à son emplacement et la fréquence de sa production personnelle. Les prix sont publiés quotidiennement sur son site.

Le 12 octobre 2009, a ainsi lieu la première vente de bitcoins en dollars entre Martti Malmi et NewLibertyStandard : Martti cède 5050 bitcoins à NLS pour 5,02 $ virés sur son compte PayPal, ce qui correspond à un prix d'environ 0,001 $ par bitcoin [26]. NLS effectuera par la suite d'autres échanges au cours des mois suivants, constituant la seule passerelle entre le dollar et le bitcoin.

Le 22 novembre marque l'ouverture du nouveau forum, sobrement appelé le *Bitcoin Forum*, qui est hébergé sur Bitcoin.org et géré par Martti Malmi. Ce forum abrite l'essentiel des discussions sur Bitcoin à partir de cette date. Il sera renommé Bitcointalk en août 2011 et hébergé à une nouvelle adresse.

Le 16 décembre 2009, Satoshi annonce la sortie de la version 0.2 du logiciel, version pour laquelle Martti Malmi est grandement crédité, ce qui clôt la première période de développement informatique de Bitcoin. L'année se termine en beauté lorsque la difficulté augmente enfin, en passant de 1 à 1,18 le 30 décembre.

Au début de l'année 2010, le bitcoin est désigné comme une « cryptomonnaie » (*cryptocurrency*) sur le site web. Le préfixe crypto- (qui vient du grec ancien κρυπτος, kruptós, indiquant ce qui est caché, occulté) possède une signification double : il renvoie à la cryptographie sur laquelle Bitcoin s'appuie, et à la confidentialité, Bitcoin étant alors présenté comme une « monnaie numérique anonyme ».

Ce nouveau terme confirme le but central de Bitcoin : devenir une monnaie, c'est-à-dire un intermédiaire dans les échanges. Cela nécessite des personnes qui génèrent des transactions (par le biais du commerce) et d'autres qui traitent

ces transactions (par le biais du minage). C'est donc tout naturellement que l'expansion de ces deux aspects complémentaires se produit à ce moment-là.

Le premier développement est l'essor commercial dont NewLibertyStandard peut être considéré comme le pionnier. Non seulement il est le premier commerçant à accepter le bitcoin comme moyen de paiement par l'intermédiaire de son service d'échange, mais il est aussi l'un des promoteurs originels de cet effort de construction économique. Dans son premier message sur le forum le 19 janvier 2010, il écrit ainsi :

> « Des gens m'ont acheté des bitcoins et m'en ont vendus. L'offre et la demande, même si elle sont faibles, existent déjà et c'est tout ce qu'il faut. Proposer d'échanger des bitcoins contre une autre monnaie n'est en fin de compte pas différent de l'échange de bitcoins contre des biens ou des services. Les monnaies sont des biens et le change est un service. [...] Vous pouvez acheter tous mes dollars ou bitcoins aujourd'hui, mais il y en aura toujours plus demain et après-demain. Toutes les personnes qui achètent ou vendent des biens en utilisant des bitcoins, y compris les changeurs, font progresser l'économie de Bitcoin. Que tout le monde fasse sa part. Achetez ou vendez quelque chose en échange de bitcoins [27] ! »

Dans les mois qui suivent, les services de change se développent, comme BitcoinFX ou Bitcoin Market. C'est pourquoi NLS propose que le bitcoin, à l'instar des monnaies échangées sur le marché des changes, adopte le sigle boursier BTC et le symbole du baht thaïlandais. L'utilisation du sigle BTC se normalise rapidement. Quant au symbole (le B majuscule traversé par deux barres verticales rappelant immanquablement le dollar), c'est Satoshi lui-même qui le conçoit, en s'inspirant de la proposition de NLS, lors de la création du premier véritable logo de Bitcoin [28].

FIGURE 1.1 – Logo de Bitcoin conçu par Satoshi Nakamoto en février 2010.

Les vendeurs de biens et de services apparaissent également. Outre son service de change, NLS ouvre un magasin en ligne où il propose à la vente des timbres et des autocollants. D'autres services acceptant le bitcoin apparaissent

comme le service de voix sur IP Link2VoIP, l'hébergeur web Vekja.net et le vendeur de noms de domaines Privacy Shark. En parallèle, la première partie de poker mettant en jeu des bitcoins est organisée, ce qui inaugure la relation forte qui existera entre le jeu d'argent et la cryptomonnaie.

Enfin, en avril 2010, naît MyBitcoin, une application web dépositaire permettant un usage facile et serein de Bitcoin, notamment sur mobile. Grâce à celle-ci, les utilisateurs n'ont en effet pas besoin de télécharger les données complètes pour envoyer et recevoir des transactions, ni de conserver leurs bitcoins eux-mêmes en sauvegardant leurs clés privées. À cette époque, les portefeuilles légers n'existent pas, si bien que Satoshi lui-même juge qu'il est alors acceptable de passer par ce type d'application, même si cela va à l'encontre du principe de désintermédiation à la base de Bitcoin :

> « Le seul inconvénient c'est qu'il faut faire confiance au site, mais cela ne pose pas de problème pour la petite monnaie destinée aux micropaiements et aux dépenses diverses [29]. »

L'année 2010 est également celle de l'essor du minage, qui se manifeste en premier lieu par l'émergence du minage par processeur graphique (GPU). Jusqu'alors, les mineurs sollicitaient leur processeur central (CPU) pour extraire de nouveaux bitcoins. Néanmoins, ces derniers processeurs s'avèrent peu performants pour effectuer des opérations répétées, comparés aux cartes graphiques qui sont largement plus adaptées à ce type de calcul répétitif. Par conséquent, tout le monde sait à ce moment-là que cette évolution est inéluctable, y compris Satoshi qui déclare en décembre 2009 que la communauté doit se « mettre d'accord pour reporter la course aux armements des GPU aussi longtemps que possible pour le bien du réseau [30] ».

La boîte de Pandore est ouverte par Laszlo Hanyecz, un développeur américain d'origine hongroise de 28 ans, qui découvre Bitcoin en avril. Après avoir acheté des bitcoins à NLS et essayé le système de transactions, celui-ci programme début mai un logiciel de minage qui s'adapte aux cartes graphiques. Cette optimisation lui permet d'occuper rapidement une place importante dans la production des blocs. Ceci attire l'attention de Satoshi Nakamoto qui le contacte et lui demande de ralentir ses opérations afin que le minage reste accessible à tous :

> « L'un des principaux attraits pour les nouveaux utilisateurs est que toute personne disposant d'un ordinateur peut générer des pièces gratuites. Lorsqu'il y aura 5 000 utilisateurs, cette incitation s'estompera peut-être, mais pour l'instant, c'est toujours vrai. Les GPU limiteraient prématurément cette incitation à ceux qui disposent d'un matériel GPU haut de gamme. Il est inévitable que

> les clusters de calcul GPU finissent par accaparer toutes les pièces générées, mais je ne veux pas précipiter l'arrivée de ce jour-là. [...] Je ne veux pas passer pour un socialiste, je me moque de la concentration des richesses, mais pour l'instant, nous obtenons plus de croissance en donnant cet argent à 100 % des gens qu'en le donnant à 20 % [31]. »

Laszlo abaisse sa cadence, mais continue à miner avec sa carte graphique. Avec sa méthode, il accumule ainsi des dizaines de milliers de bitcoins.

Toutefois, cela n'est pas entièrement négatif pour le projet car il finit par réinjecter ses bitcoins dans l'économie de la façon la plus emblématique possible : en achetant quelque chose avec, et plus précisément des pizzas. Le 18 mai 2010, il écrit ainsi l'annonce suivante sur le forum :

> « Je paierai 10 000 bitcoins pour deux ou trois pizzas... genre peut-être 2 grandes pour qu'il m'en reste le lendemain. J'aime avoir des restes de pizza à grignoter pour plus tard. Vous pouvez faire la pizza vous-même et l'amener jusqu'à chez moi ou la commander pour moi auprès d'un service de livraison, mais mon objectif c'est de me faire livrer, en échange de bitcoins, de la nourriture que je n'ai pas à commander ou à préparer moi-même. [...] Si vous êtes intéressé, faites-le moi savoir et nous pourrons nous arranger [32]. »

Cette offre trouve preneur au bout de quatre jours. Le 22 mai, un jeune Californien du nom de Jeremy Sturdivant accepte l'échange sur la messagerie instantanée IRC : il commande deux pizzas de Papa John's qui sont livrées chez Laszlo à Jacksonville en Floride, et reçoit en échange 10 000 bitcoins [33], ce qui représente alors environ 44 $ sur Bitcoin Market. Cela clôt le premier achat d'un bien physique en bitcoins ! Cet évènement symbolique sera par la suite commémoré tous les ans à cette date comme le *Bitcoin Pizza Day*.

Une autre personne vient contribuer au succès du projet. Vers la fin du mois de mai, un développeur américain de 44 ans, nommé Gavin Andresen, découvre Bitcoin par le biais d'un article publié sur InfoWorld. De retour d'Australie, momentanément sans emploi, il se met à travailler sur son premier projet : un robinet à bitcoins (*bitcoin faucet*) qui donne des bitcoins à quiconque en fait la requête. Le 11 juin, Gavin lance son service et le présente sur le forum :

> « Pour mon premier projet de programmation sur Bitcoin, j'ai décidé de faire quelque chose qui semble vraiment stupide : j'ai créé un site web qui distribue des bitcoins. [...] Pourquoi ? Parce que je veux que le projet Bitcoin réussisse, et je pense qu'il a plus de chances de réussir si les gens peuvent obtenir une poignée de pièces pour l'essayer [34]. »

Ce *faucet*, qui offre d'abord 5 bitcoins par requête au tout début, est approuvé par Satoshi, ce dernier ayant « prévu de faire exactement la même chose si quelqu'un d'autre ne l'avait pas fait [35] ». Le service, sollicité par beaucoup de personnes, distribuera plus de 19 700 bitcoins jusqu'à sa fermeture deux ans plus tard. De plus, Gavin s'implique dans le développement du logiciel et échange beaucoup avec Satoshi par courriel. Il en devient rapidement le bras droit grâce à la confiance qu'il lui inspire.

Malgré cette croissance économique encourageante, l'activité reste extrêmement réduite sur le réseau. Le 30 juin, sur la liste de diffusion de Bitcoin, James A. Donald déclare ainsi que « Bitcoin est en quelque sorte mort » et que « le problème est que le bitcoin a besoin d'une écologie d'utilisateurs pour être utile [36] ». Toutefois, quelques jours plus tard, un évènement vient lui donner tort.

Le slashdotting

Le 11 juillet 2010, suite à la sortie de la version 0.3 du logiciel, une courte présentation de Bitcoin rédigée par un utilisateur est publiée sur Slashdot, un site d'actualité très populaire traitant de sujets pour les *nerds* comme l'informatique, les jeux vidéo, la science, Internet, etc. L'argumentaire de vente est le suivant :

> « Que pensez-vous de cette technologie disruptive ? Bitcoin est une monnaie numérique basée sur un réseau pair à pair, sans banque centrale, et sans frais de transaction. À l'aide d'un concept de preuve de travail, les nœuds brûlent des cycles de processeur pour chercher des paquets de pièces et diffusent leurs résultats sur le réseau. L'analyse de la consommation d'énergie révèle que la valeur marchande des bitcoins est déjà supérieure à la valeur de l'énergie nécessaire pour les générer, ce qui indique une demande saine. La communauté a bon espoir que la monnaie restera hors de portée de tout État [37]. »

Ceci provoque un afflux massif de nouveaux visiteurs sur le site et sur le forum, ainsi qu'une augmentation du nombre d'utilisateurs et de mineurs sur le réseau. Le réseau tient le coup malgré la montée en charge. En conséquence, le prix du bitcoin connaît la première hausse majeure de son histoire, en passant de 0,008 $ à 0,08 $ en une semaine, soit une multiplication par 10 !

Parmi les personnes qui découvrent Bitcoin grâce à Slashdot, il y a Jed McCaleb, un entrepreneur et programmeur américain de 35 ans, connu pour avoir cofondé et développé le logiciel de partage de fichiers en pair à pair eDonkey2000 dans les années 2000. Constatant à quel point il est pénible

de se procurer du bitcoin contre des dollars, il décide de créer une place de marché spécialisée. Pour ce faire, il réutilise un de ses anciens projets mis au point en 2007 : *Magic The Gathering Online eXchange* (MTGOX), un site web qui permettait d'acheter et de vendre des cartes du jeu en ligne *Magic: The Gathering Online* [38]. Il reprend le même nom de domaine au passage : mtgox.com.

Une semaine plus tard, le 18, la plateforme de change Mt. Gox (« *Mount Gox* ») est lancée et annoncée officiellement sur le forum par Jed. Grâce à son expertise, il fait en sorte que la plateforme fonctionne comme une place de marché automatisée, à l'instar des bourses en ligne modernes. Elle se distingue de Bitcoin Market par le fait qu'elle est « toujours en ligne, automatisée », que « le site est plus rapide et a un hébergement dédié » et que « l'interface est plus agréable [39] ». Par conséquent, Mt. Gox s'impose rapidement comme le moyen principal de se procurer du bitcoin, devenant la référence en ce qui concerne le cotation en dollars.

Le minage connaît également une phase ascendante. L'afflux de nouveaux mineurs fait passer le taux de hachage du réseau (le nombre de calculs par seconde) au-dessus du milliard de calculs par seconde (1 GH/s) dès le 13 juillet. Certains mineurs développent leur propre algorithme de minage par GPU. C'est le cas de ArtForz, un développeur allemand, qui se met à miner le 19 juillet et qui construit au cours du temps la première ferme de minage de Bitcoin, qui sera connue sous le nom d'« ArtFarm » [40].

Mais cette croissance suivant la présentation sur Slashdot provoque également des problèmes d'ordre technique, mettant le système à l'épreuve. Deux incidents viennent ainsi perturber le projet.

Le premier incident est la découverte d'une vulnérabilité dans le code de Bitcoin qui rend possible la dépense de bitcoins à partir de n'importe quelle adresse (cette vulnérabilité sera appelée le « 1 RETURN bug » en référence au script nécessaire pour réaliser cette dépense). C'est ArtForz qui en découvre l'existence à la fin du mois de juillet 2010. Au lieu d'exploiter cette faille et de s'emparer de la richesse présente sur le réseau pour la revendre discrètement, il choisit de prévenir Satoshi et Gavin par courriel. Satoshi s'empresse d'inclure la correction dans la mise à jour 0.3.6 et recommande à tous les utilisateurs de mettre à jour leur logiciel. La vulnérabilité n'est pas exploitée et Bitcoin échappe ainsi au pire.

Le second évènement est le *value overflow incident*. Le 15 août vers 17 heures, un bloc miné contient une transaction qui crée plus de 184 milliards de bitcoins. Cette création exploite une vulnérabilité de dépassement de mémoire

(*overflow*) dans la représentation des quantités dans Bitcoin. Une heure plus tard, le problème est repéré par Jeff Garzik, un ingénieur américain ayant découvert Bitcoin grâce à Slashdot, qui avertit la communauté sur le forum [41].

La réaction de Satoshi ne se fait pas attendre. Un peu avant minuit, il publie un correctif créant une chaîne alternative ne contenant pas la transaction incriminée. La situation conflictuelle est résolue lorsque la chaîne correcte devient plus longue que l'autre le lendemain à 8 heures 10 du matin. Cet incident perturbe l'activité du réseau pendant 15 heures environ mais le problème est vite réglé grâce à une réactivité forte de la communauté. Suite à cet incident, Satoshi implémente un système d'alerte dans Bitcoin, lui permettant d'avertir tous les nœuds du réseau en cas de problème technique [42].

Au cours de l'automne, la popularisation du minage par processeur graphique rend le minage par CPU quasi impossible. C'est ce qui provoque l'apparition de la première coopérative de minage le 27 novembre, Bitcoin.cz Mining, une organisation permettant aux petits mineurs de lisser leurs revenus en regroupant leurs puissances de calcul respectives [43]. Créée par Marek Palatinus (connu sous le pseudonyme de slush), un architecte informatique tchèque, la coopérative sera par la suite rebaptisée Slush Pool en son hommage.

De manière générale, à la fin de l'année 2010, on peut considérer que le projet Bitcoin a pris son envol : l'économie s'est fortifiée, notamment avec les services de change, le minage s'est spécialisé avec l'apparition du minage par GPU et le protocole a été mis à l'épreuve par la découverte de failles dans le logiciel. Ces éléments montrent que les incitations des différents acteurs du système sont alignées. C'est à ce moment-là que Satoshi décide de disparaître.

La disparition de Satoshi Nakamoto

La disparition de Satoshi Nakamoto se fait progressivement à partir de décembre 2010. Satoshi n'explicite pas les raisons qui le poussent à s'éclipser, mais nous pouvons les deviner. Tout d'abord, le projet a pris : il a grossi à tel point qu'il devient difficile de diriger le mouvement. Mais surtout Satoshi redoute la réaction des agences étatiques, une préoccupation qu'il exprime dans un message daté du 5 juillet 2010 (commentant le brouillon de la présentation de Bitcoin qui sera proposée à Slashdot), où il déclare ne pas vouloir mettre trop en avant l'aspect « anonyme » de Bitcoin ou son opposition aux autorités légales qui constituerait une « provocation [44] ».

L'élément déclencheur est l'affaire WikiLeaks. WikiLeaks est une orga-

nisation non gouvernementale à but non lucratif fondée par le cypherpunk Julian Assange en 2006, dont la raison d'être est de donner une audience aux lanceurs d'alertes et aux fuites d'information, tout en protégeant leurs sources. À partir de 2010, les documents confidentiels révélés par l'ONG commencent à être relayés par les grands médias et à faire du bruit dans l'opinion publique. C'est notamment le cas de l'*Afghan War Diary*, un ensemble de documents et de rapports militaires américains secrets sur la guerre en Afghanistan faisant notamment état de la dissimulation des victimes civiles, qui est publié le 25 juillet 2010 grâce à la contribution de Bradley Manning, un analyste militaire de l'armée des États-Unis [45]. On peut également citer les *Iraq War Logs*, documents secrets sur la guerre en Irak entre 2004 et 2009 publiés le 23 octobre et révélant le nombre de victimes civiles et les actes de torture perpétrés.

Le financement de WikiLeaks repose essentiellement sur les dons du public. Il s'agit d'une activité sensible pour les firmes réglementées qui craignent les potentielles représailles des autorités. C'est ainsi que la société de paiement en ligne Moneybookers gèle le compte de l'ONG le 14 octobre 2010. À la suite de ces révélations, il est ainsi de plus en plus probable que WikiLeaks s'expose à davantage de sanctions.

Le 10 novembre, Amir Taaki, un jeune anglais d'origine iranienne ayant fraîchement découvert Bitcoin, voit dans la situation de WikiLeaks une opportunité de démontrer l'utilité de la résistance à la censure du système. Il écrit ainsi sur le forum :

> « Je voulais envoyer une lettre à Wikileaks à propos de Bitcoin car, malheureusement, ils ont subi plusieurs incidents où leurs fonds ont été saisis dans le passé. [...] Quelqu'un sait où leur envoyer un message [46] ? »

Les réactions sont mitigées. D'après un utilisateur, « cela peut être bénéfique pour wikileaks, mais pas nécessairement pour Bitcoin [47] ».

Un mois plus tard, le 3 décembre, PayPal gèle le compte de WikiLeaks. Certaines personnes sur le forum suggèrent d'encourager WikiLeaks à accepter le bitcoin : cela paraît en effet le « moment idéal pour mettre en place les dons en bitcoins [48] ». Cela fait réagir Satoshi le lendemain qui s'oppose à cette évolution et déclare :

> « Le projet a besoin de grandir progressivement pour que le logiciel puisse se renforcer en cours de route.
>
> J'appelle WikiLeaks à ne pas commencer à utiliser Bitcoin. Bitcoin est une petite communauté expérimentale encore naissante. Vous n'obtiendriez rien de plus que quelques piécettes et l'agitation que vous apporteriez nous détruirait probablement à ce stade [49]. »

Dans les jours qui suivent, c'est un véritable blocus financier qui se met en place contre WikiLeaks, auquel participent Mastercard et Visa, mais aussi Western Union, Bank of America et d'autres acteurs, ce qui met en péril la survie financière de l'ONG. Tout naturellement certains insistent pour que Bitcoin soit mis à profit.

Le 11 décembre, un article est publié sur PC World pour mettre en avant la possibilité d'un usage de Bitcoin par WikiLeaks. Cet article est rapidement évoqué sur le forum et la réaction de Satoshi est sans appel. Il écrit :

> « Il aurait été bon d'attirer cette attention dans un tout autre contexte. WikiLeaks a donné un coup de pied dans le nid de frelons, et l'essaim se dirige maintenant vers nous [50]. »

C'est son avant-dernier message public. Le lendemain, il poste son dernier message sur le forum pour annoncer la version 0.3.19 du logiciel, puis se volatilise. Il transmet les rênes du projet à ses deux bras droits historiques : Martti Malmi et Gavin Andresen.

Martti Malmi hérite du site web et du forum. Néanmoins, à l'instar de Satoshi, il se détourne progressivement de Bitcoin et délègue la gestion de ces plateformes à d'autres personnes, à qui il cèdera le contrôle entièrement en 2015 [51]. Il vendra ses 55 000 bitcoins pour s'acheter un appartement près de Helsinki.

De son côté, Gavin Andresen hérite de la clé d'alerte, du dépôt SourceForge et de la liste de diffusion. Dès le 19 décembre, il annonce « commencer à gérer le projet Bitcoin de manière plus active [52] » et crée le dépôt GitHub de Bitcoin, où le projet sera dorénavant développé. Il ignore alors qu'il est devenu le développeur en chef du projet et que le créateur de Bitcoin va disparaître.

Satoshi se volatilise définitivement durant le printemps 2011. Le 23 avril, il adresse un dernier courriel à Mike Hearn, l'ingénieur de Google qui l'avait approché deux ans auparavant et qui était resté en contact avec lui, dans lequel il écrit :

> « Je suis passé à autre chose. [Bitcoin] est entre de bonnes mains avec Gavin et les autres [53]. »

Il fait également ses adieux à Gavin et Martti. En particulier, il demande à Gavin d'éviter de parler de lui comme d'un « personnage sombre et mystérieux » à la presse [54]. Le 27 avril, Gavin annonce qu'il a été invité par la CIA à faire une présentation sur Bitcoin. Cette visite se passe le 14 juin. De manière intéressante, c'est également le jour où WikiLeaks se met finalement à accepter les dons en bitcoins [55]. Ces deux évènements viennent confirmer

ce que Satoshi redoutait.

Satoshi Nakamoto laisse derrière lui une fortune colossale : 1 122 693 bitcoins selon une estimation de 2020[56]. Cela représente plus de 5 % de la quantité totale de bitcoins. Ces fonds ne bougeront jamais.

Quelques messages émaneront de ses différents comptes[57], mais on supposera qu'ils ont été piratés.

L'identité de Satoshi Nakamoto restera inconnue, celui-ci ayant réussi à conserver son anonymat grâce à l'usage de Tor et de services respectueux de la vie privée. Dans les années qui suivront, ce « personnage sombre et mystérieux » deviendra un mythe à part entière, suscitant les spéculations les plus diverses. Tout le monde se demandera « Qui est Satoshi Nakamoto ? » à l'instar des gens s'interrogeant sur l'identité de John Galt dans le roman *La Grève* d'Ayn Rand. On cherchera à savoir qui il est, quelques pistes seront privilégiées[58], mais jamais son identité civile ne sera formellement identifiée.

En 2013, dans l'un de ses derniers messages sur le forum, Hal Finney partagera une citation énigmatique du film *Man of Steel* tout juste sorti, résumant bien la dimension mystérieuse entourant le créateur de Bitcoin :

> « Comment retrouver quelqu'un qui a toujours brouillé les pistes ? [...] Pour certains, c'était un ange gardien. Pour d'autres, [une énigme,] un fantôme, toujours un peu à l'écart. [...] Que représente le S ?[59] »

En mars 2014, on croira l'avoir trouvé en la personne de Dorian Prentice Satoshi Nakamoto suite à la publication d'un article de Newsweek[60]. Cet ingénieur des télécommunications, citoyen américain naturalisé d'origine japonaise, vivant avec sa mère à Temple City dans la banlieue de Los Angeles, se fera harceler par la presse mais niera en bloc. On découvrira cependant que la famille de Hal Finney a habité dans la même municipalité, « à quelques pâtés de maisons de la maison familiale des Nakamoto », durant l'adolescence de Hal, ce qui attirera quelques soupçons sur ce dernier[61].

Hal Finney décèdera en août 2014 des suites de la maladie de Charcot. En tant que futuriste averti, il se fera cryogéniser par la fondation Alcor.

La communauté prend le relai

Alors que Satoshi se met progressivement en retrait, la popularité de Bitcoin augmente prodigieusement. En particulier, le prix du bitcoin évolue de manière favorable : alors qu'il n'était que de 20 centimes en décembre 2010, il atteint la parité avec le dollar le 9 février 2011 et s'y maintient pendant quelque temps. Cette hausse du prix attise l'enthousiasme de la communauté, et no-

tamment celui de Hal Finney qui déclare avoir « vraiment de la chance d'avoir investi au début d'un nouveau phénomène qui risque d'être explosif [62] ».

Cette période coïncide avec l'apparition de Silk Road, une place de marché du dark web s'appuyant sur Tor et Bitcoin qui permet à ses utilisateurs d'échanger librement des produits et des services légaux et illégaux. Celle-ci est lancée à la fin du mois de janvier par un jeune Texan du nom de Ross Ulbricht, qui en fait mention sur le forum de Bitcoin en feignant d'avoir découvert le site par hasard [63].

Ross Ulbricht adhère profondément aux principes du libertarianisme, une philosophie libérale originaire des États-Unis prônant le respect impératif de la liberté individuelle, des droits de propriété et du marché. Silk Road est pour lui une incarnation de cet idéal. De ce fait, la gamme des produits et services qui peuvent être listés sur le site est restreinte et nécessite qu'aucun mal n'ait été fait à autrui : on y retrouve ainsi de la drogue, des médicaments, des pièces de métaux précieux, mais en aucun cas des cartes bancaires volées, de la pédopornographie ou des services de tueur à gages. Dans l'ensemble, le site sert principalement à la vente de drogue illicite (dont surtout de petites quantités de cannabis), chose pour laquelle il deviendra célèbre.

La promotion de Bitcoin s'intensifie également. Le 22 mars, la première vidéo expliquant Bitcoin de manière qualitative est publiée [64]. Cette vidéo, intitulée sobrement « *What is Bitcoin?* », est produite par Stefan Thomas grâce à un financement participatif de la communauté. Elle aura un succès retentissant au fil des années en totalisant plusieurs millions de vues sur YouTube. Les vidéos de ce type se multiplieront.

Bitcoin est notamment vanté dans les cercles libertariens, où son caractère libre, anonyme et hors de portée de l'État est mis en avant. À la fin de l'année 2010, l'émission de webradio FreeTalkLive commence à évoquer le cas de Bitcoin et de son utilisation illégale. Cela attire l'attention de l'entrepreneur et activiste Roger Ver, déjà millionnaire grâce à sa société de revente de composants informatiques, Memory Dealers. Il apprend l'existence de la cryptomonnaie en décembre 2010 et est instantanément conquis : il se met à lire tout ce qu'il peut sur le sujet, achète du bitcoin, et fait en sorte de l'accepter avec son entreprise quelques mois plus tard. Il deviendra rapidement l'un des promoteurs les plus zélés de Bitcoin, ce qui lui vaudra le surnom de *Bitcoin Jesus* pendant un temps.

L'existence de Silk Road est révélée au grand public le 1er juin 2011 avec un article d'Adrien Chen sur Gawker [65], ce qui a pour effet d'attirer l'attention sur Bitcoin encore un peu plus, notamment en incitant les consommateurs à

se procurer du bitcoin pour acheter des produits sur la plateforme.

Au cours du printemps 2011, on assiste par conséquent à une forte poussée du prix, due à l'augmentation de la demande. Après avoir stagné pendant quelques mois, celui-ci passe ainsi de 1 $ le 15 avril à plus de 32 $ le 8 juin.

Mt. Gox, la principale plateforme de change de l'époque, se retrouve sous pression. Celle-ci a alors été reprise depuis quelques mois par Mark Karpelès, un développeur français de 26 ans vivant au Japon, qui est quelque peu négligent et n'a pas su résoudre les problèmes d'implémentation de son prédécesseur. C'est ainsi qu'un incident malencontreux survient le dimanche 19 juin : un groupe de pirates accède au compte administrateur de Jed McCaleb et tente d'en extraire un maximum d'argent.

La limite de retrait journalière étant fixée à 1 000 $, les pirates cherchent à faire baisser le prix afin de retirer le plus de bitcoins possibles. Ils vendent les bitcoins de Jed McCaleb au marché ce qui provoque un krach éclair sur le cours : le prix, qui stationne ce jour-là autour des 17 $, chute à 0,01 $ en quelques minutes. C'est la panique dans la communauté, et beaucoup d'utilisateurs de Mt. Gox vendent sous le coup de l'émotion afin de conserver ce qui leur reste. La situation est rétablie dans la journée mais 2 000 bitcoins manquent à l'appel. Le 23 juin, Mark Karpelès prouve la solvabilité de l'entreprise en déplaçant 424 242 bitcoins d'une adresse à une autre [66].

Cet incident entraîne la fin de la folie spéculative sur le bitcoin et le prix se met à descendre doucement. C'est à ce moment-là qu'on assiste à la fermeture de MyBitcoin : début août, le service fait faillite suite à la disparition de 78 740 bitcoins, ce qui représente 51 % des fonds figurant sur les comptes des clients. Des éléments laissent à penser que son fondateur anonyme, Tom Williams, est à l'origine du vol. Dans les jours qui suivent cet évènement, le prix baisse en flèche jusqu'à 6 $, et finira par tomber à 2 $ en novembre.

Mais cela ne décourage pas pour autant les membres de la communauté. Du 19 au 21 août 2011 a lieu la première conférence sur Bitcoin à New York, qui est organisée par Bruce Wagner, l'animateur du *Bitcoin Show*, une émission d'entretiens filmés avec les acteurs de l'écosystème [67]. La conférence revêt un caractère amateur (typique de la communauté d'alors) et seules quatre présentations ont lieu : celle de Bruce Wagner ainsi que les interventions de Gavin Andresen, Jeff Garzik et Stefan Thomas. Cela permet néanmoins aux membres les plus actifs, tels que Roger Ver, Jesse Powell, Jed McCaleb, Mark Karpelès ou Charlie Lee, de se réunir en personne pour la première fois.

Le développement logiciel s'organise aussi. Jusqu'ici, il était centralisé dans les mains de Satoshi, le « dictateur bienveillant » du projet. Mais après

le départ du créateur de Bitcoin, il s'ouvre à la participation de la communauté, sous la supervision de Gavin Andresen. On voit ainsi des contributeurs talentueux commencer à s'impliquer dans l'évolution de Bitcoin comme Nils Schneider, Matt Corallo, Pieter Wuille, Jeff Garzik, Wladimir van der Laan, Luke-Jr ou encore Gregory Maxwell. Des méthodes de coordination sont rapidement mises en place comme la liste de diffusion `bitcoin-development` permettant de discuter formellement des changements à apporter [68], et le système des propositions d'amélioration de Bitcoin (*Bitcoin Improvement Proposals* ou BIP), qui décrivent publiquement ces changements [69].

L'utilisation de Bitcoin devient plus facile. On assiste à l'apparition de portefeuilles légers permettant d'utiliser Bitcoin sans avoir à télécharger et vérifier l'intégralité de la chaîne. Ces derniers utilisent la vérification de paiement simplifiée décrite par Satoshi Nakamoto dans la section 8 du livre blanc. Celle-ci est mise en œuvre par Mike Hearn au sein de sa bibliothèque logicielle BitCoinJ programmée en Java, qui permet entre autres une meilleure compatibilité avec les applications sur les téléphones multifonctions fonctionnant sous Android. Le premier portefeuille pour mobile, le *Bitcoin Wallet for Android*, est lancé par Andreas Schildbach en mars 2011. Celui-ci montre que l'usage direct de Bitcoin dans la vie de tous les jours est possible. Du côté ordinateur, Thomas Voegtlin crée Electrum en novembre 2011, présenté comme un portefeuille qui permet à l'utilisateur de récupérer ses fonds par le biais d'une phrase mnémotechnique. Cette pratique sera plus tard standardisée et adoptée largement dans l'écosystème.

Ce développement décentralisé est également source de tensions. Sans son fondateur, le projet ne dispose plus d'un meneur incontestable : certes Gavin Andresen possède le contrôle du dépôt, mais n'a pas l'autorité technique suffisante pour imposer toutes ses vues aux autres développeurs. Les décisions sont prises relativement collectivement, ce qui pose la question de la gouvernance de Bitcoin : qui décide d'apporter un changement au protocole ?

À la fin de l'année 2011 et au début de l'année 2012, le premier débat technique en l'absence de Satoshi a lieu. Le groupe de développeurs est alors encore très restreint mais cela suffit pour créer un conflit à propos de l'amélioration de la programmabilité des transactions, qui permettrait notamment de créer des comptes multisignatures. On s'en souviendra comme la « bataille pour P2SH [70] ».

De par sa nature informatique, Bitcoin constitue un système de monnaie programmable qui permet à l'utilisateur d'imposer des conditions au blocage et au déblocage des fonds. Il dispose pour cela d'un mécanisme de scripts

reposant sur des instructions logiques appelées codes opérations. Cependant, ces scripts sont compliqués à gérer. Il s'agit donc de trouver un moyen simple pour l'utilisateur d'envoyer des fonds vers un script défini préalablement par le récipiendaire. C'est l'idée derrière la proposition faite par Nicolas van Saberhagen d'ajouter un nouveau code opération appelé `OP_EVAL`. Cette proposition souffre néanmoins d'un problème de récursivité, ce qui provoque rapidement l'apparition de deux propositions concurrentes : *Pay to Script Hash* (P2SH) proposé par Gavin Andresen et `OP_CHECKHASHVERIFY` (CHV) proposé par Luke-Jr.

Une tension émerge entre les deux propositions, ce qui crée le débat. Amir Taaki, qui ne soutient ni l'une ni l'autre, appelle à la discussion et déclare le 29 janvier 2012 :

> « Ma crainte c'est qu'un jour Bitcoin soit corrompu. Développeurs : considérez cet examen supplémentaire comme une opportunité de construire une culture d'ouverture [71]. »

Finalement, c'est P2SH qui est choisi pour être intégré à Bitcoin sur l'ordre de Gavin Andresen. Cette intégration sera réalisée, non sans difficulté, le 1er avril 2012.

Dans un même temps, la popularisation de Bitcoin se poursuit. Le 28 février, un russo-canadien du nom de Vitalik Buterin, âgé de seulement 18 ans, cofonde le *Bitcoin Magazine* avec Mihai Alisie, un développeur roumain. Ce média, d'abord uniquement disponible en version web, est distribué en édition papier à partir de mai. Le jeune Vitalik y écrit de nombreux articles documentant l'actualité de l'époque. Par la suite, de nombreux sites d'information spécialisés verront le jour comme CoinDesk ou CoinTelegraph.

Le 24 avril 2012, un jeu de hasard en ligne nommé SatoshiDICE est lancé par l'entrepreneur américain Erik Voorhees [72]. Le site repose sur un fonctionnement très simple : le joueur envoie des bitcoins à une adresse spécifique et il a une probabilité prédéfinie de recevoir une récompense qui correspond à un multiple du montant envoyé (il a par exemple une chance sur deux de recevoir un peu moins de deux fois sa mise). Le procédé est instantané et aisément vérifiable, ce qui attire de nombreux parieurs.

En tant que libertarien convaincu vivant dans le New Hampshire, Erik Voorhees voit en SatoshiDICE une manière d'échapper à la réglementation. Le 20 août, il réalise même une IPO pour son entreprise sur la plateforme roumaine MPEx. Il revendra la plateforme le 17 juillet 2013 pour 126 315 bitcoins, soit 12,4 millions de dollars au moment de l'acquisition.

Le succès de SatoshiDICE provoque une augmentation significative du

nombre de transactions sur la chaîne, qui triple en quelques mois. Cette activité provenant du site est remarquée et dérange certains développeurs qui la qualifient de « spam [73] ». À la moitié de l'année 2012, Bitcoin est ainsi complètement lancé et prêt à être découvert par un public plus large.

L'amorçage organique de Bitcoin

Les premières années de Bitcoin ont été déterminantes pour son succès. Il a en effet pu grandir dans la discrétion et connaître une croissance organique et prudente, à l'abri de l'opportunisme et de la propagande de notre monde.

Bitcoin a été proposé en 2008 par Satoshi Nakamoto, qui l'a mis en œuvre en janvier 2009. Les débuts ont été difficiles, à tel point qu'il a fallu attendre neuf mois avant que le bitcoin n'acquière un prix ! Satoshi s'est dévoué pleinement à son œuvre sans jamais profiter personnellement de sa fortune accumulée. En disparaissant en 2011, il a finalement laissé la communauté s'approprier le projet.

Bitcoin a été façonné dans un creuset mêlant cypherpunks, anarchistes, libertariens et autres amoureux de la liberté. Il s'est construit en opposition au système étatico-bancaire traditionnel, où règnent la censure et les renflouements publics. C'est pourquoi le message derrière Bitcoin est si radical et que tant de gens se sont pris de passion pour lui.

Entre 2010 et 2012, les premiers cas d'utilisation de Bitcoin ont émergé. Financement de projets politiquement sensibles, jeu d'argent en ligne, achat de drogues à distance, envois de fonds à l'étranger : il s'agissait d'usages à la limite de légalité, voire complètement illégaux, qui démontraient toute l'efficacité du bitcoin en tant que monnaie incensurable et relativement anonyme. Cependant, cette tendance a été rapidement tempérée comme on a pu le constater durant les années qui ont suivi.

2

Une croissance conflictuelle

Après un début unifié autour de la figure de Satoshi Nakamoto entre 2009 et 2011, la communauté de Bitcoin s'est rapidement organisée sans sa médiation, de manière décentralisée. Gavin Andresen avait bien été nommé responsable du projet, mais il n'avait pas l'autorité morale suffisante pour imposer une vision claire de Bitcoin aux autres et préférait la conciliation. De ce fait, la communauté s'est retrouvée en proie à de multiples conflits internes, qui ont progressivement gagné en intensité avec l'afflux des nouveaux arrivants lors des différentes vagues spéculatives. La querelle entre les développeurs à propos de *Pay to Script Hash* début 2012 n'était ainsi que la préfiguration de divisions bien plus profondes.

Quatre évolutions majeures ont affecté l'écosystème de Bitcoin au cours de son histoire et ont mené à la création de clivages majeurs au sein de la communauté. Ces évolutions ont été : la financiarisation de l'économie, caractérisée par le développement des intermédiaires de confiance ; l'atteinte de la limite de capacité transactionnelle de la chaîne de blocs, ayant mis en évidence le manque de scalabilité du système (et donné lieu à la célèbre « guerre des blocs ») ; l'essor des cryptomonnaies alternatives, accueilli de façons très diverses par les utilisateurs de Bitcoin ; et l'intégration institutionnelle réalisée par les instances étatiques, posant la question du rapport à entretenir avec l'autorité.

Bitcoin a ainsi connu une croissance conflictuelle qui a forgé ce qu'il est devenu et la perception que nous en avons aujourd'hui. C'est pourquoi nous nous concentrerons sur ces quatre clivages dans ce chapitre.

La financiarisation

La financiarisation de Bitcoin se caractérise par une professionnalisation de l'activité d'échange entre le bitcoin et les monnaies étatiques, ce qu'on appelle formellement le change, et l'arrivée des acteurs traditionnels dans l'écosystème. Elle s'accompagne d'une croissance du prix sans précédent, d'une plus grande liquidité du marché, mais aussi d'un resserrement des contraintes réglementaires et d'une mutation du discours dominant au sein de la communauté.

Le besoin de disposer de services de change se fait ressentir très rapidement. En effet, de manière générale les gens possèdent, gagnent et dépensent de la monnaie fiat comme du dollar ou de l'euro, et non du bitcoin. Ainsi, même si Bitcoin est un système théoriquement indépendant du système traditionnel, il est essentiel qu'il existe des passerelles entre les deux univers, au moins de manière temporaire.

À partir de l'année 2011, on assiste de ce fait à un essor sans précédent des places de marché, des bourses en ligne traitant de manière automatisée les ordres d'achat et de vente des clients. C'est en particulier le cas de la plateforme Mt. Gox qui, malgré des débuts houleux, devient rapidement une véritable plaque tournante de la conversion entre bitcoins et dollars, recueillant un volume journalier d'au moins 200 000 $ et dépassant parfois le million de dollars. D'autres plateformes émergent comme Bitstamp, Bitcoin-Central, TradeHill ou BTC-e, mais elles ne parviennent pas à concurrencer Mt. Gox qui continuera de représenter 90 % du volume total échangé sur le marché durant le reste de son existence.

Outre les plateformes où la négociation se fait « au comptant » (les actifs réels sont échangés), on voit aussi apparaître des plateformes de trading sur marge qui permettent de négocier des contrats et ainsi de recourir à l'effet de levier (*leverage*) et de faire de la vente à découvert (*short selling*). La première d'entre elles est Bitcoinica, qui connaît une existence tumultueuse entre septembre 2011 et mai 2012, avant d'être remplacée par la plateforme Bitfinex, qui prend la relève en octobre 2012.

En parallèle se développe un service nommé BitInstant aux États-Unis, cofondé en juin 2011 par Gareth Nelson et Charlie Shrem, dont le rôle est de faciliter les transferts vers et depuis les plateformes de change. L'entreprise sert d'intermédiaire entre les clients et les plateformes et permet de rendre les dépôts (et les retraits) instantanés moyennant une commission. Charlie Shrem, jeune New-Yorkais d'origine juive syrienne, assure le rôle de PDG et devient rapidement la figure principale de l'entreprise, bien que d'autres personnes

soient impliquées dans le projet comme Roger Ver et Erik Voorhees. Dès le début de l'année 2012, BitInstant propose diverses méthodes de transfert d'argent (Liberty Reserve, Dwolla, Paxum, dépôts d'espèces,) pour interagir avec les principales plateformes de l'écosystème, dont notamment Mt. Gox qui est basée au Japon. En avril 2013, l'activité de BitInstant finira par représenter environ 30 % du volume total échangé sur les plateformes de change [1].

Mais les places de marché ne sont pas les seules à fleurir. Premièrement, on constate un développement des applications dépositaires, qui permettent d'envoyer et de recevoir facilement des bitcoins sans devoir en gérer la détention soi-même, dont MyBitcoin était le précurseur entre 2010 et 2011. C'est le cas de Coinbase, fondé en mai 2012 par Brian Armstrong et Fred Ehrsam, qui se développe initialement comme un « portefeuille Bitcoin hébergé [2] ». Coinbase intégrera progressivement les fonctionnalités d'une plateforme de change classique au fil des années.

Deuxièmement, on voit apparaître des processeurs de paiements qui donnent aux commerçants la possibilité de recevoir des bitcoins et de les revendre instantanément pour échapper à la volatilité. L'exemple par excellence de ce type de service est BitPay, un processeur de paiement fondé en mai 2011 par Tony Gallippi et Stephen Pair qui deviendra rapidement la solution de facilité pour de nombreux commerçants.

Troisièmement, les services de change de particulier à particulier se multiplient également. Ceux-ci permettent à deux individus d'échanger du bitcoin via divers moyens de paiement, dont notamment l'échange en personne contre des espèces. La plus connue est la plateforme LocalBitcoins, qui est fondée en juin 2012 par Jeremias Kangas et qui inspirera les autres plateformes du même type. Dans le même esprit, il existe également les marchés de gré à gré (*over the counter*) par lesquels les plus fortunés peuvent procéder à des échanges importants entre eux, en privé, sans affecter instantanément le cours sur les places de marché.

Ainsi, l'offre de services financiers se développe considérablement entre 2012 et 2013. Cela s'explique par une forte demande de la part des clients de plus en plus désireux de se procurer du bitcoin. Cette demande s'illustre par l'apparition de la cryptomonnaie dans la culture populaire, réellement inaugurée par l'épisode de *The Good Wife* diffusé le 15 janvier 2012 aux États-Unis qui est consacré entièrement à Bitcoin [3].

En particulier, l'intérêt des acteurs du monde financier traditionnel fait la différence. On assiste en effet à la venue d'investisseurs très fortunés qui s'intéressent au bitcoin, en raison de son offre limitée (la fameuse limite

des 21 millions) et par son potentiel technologiquement disruptif. Ils placent leur argent non seulement dans le bitcoin, mais aussi dans les entreprises de l'écosystème.

C'est d'abord le cas de Barry Silbert, un aficionado de Wall Street ayant fait fortune grâce à SecondMarket, une société facilitant la négociation d'actifs sur le marché secondaire. Il s'intéresse au bitcoin en 2012 et en achète pour des centaines de milliers de dollars. Il sera à l'origine de la création de Grayscale Investments en 2013 et du Digital Currency Group en 2015.

C'est aussi le cas des frères Tyler et Cameron Winklevoss, qui sont connus pour leur différend avec Mark Zuckerberg concernant la création de Facebook et pour avoir été dédommagés de 65 millions de dollars dans cette affaire. Les jumeaux apprennent l'existence de Bitcoin en août 2012 par le biais de David Azar, un associé de Charlie Shrem. Puis ils rencontrent ce dernier, qui les convainc d'investir dans le bitcoin. Ils finissent également par investir dans sa société BitInstant en mai 2013. Ils seront plus tard à l'origine de la plateforme de change Gemini.

On peut enfin citer l'entrepreneur et philanthrope argentin Wences Casares, qui achète du bitcoin en février 2013. Il fondera sa propre société dans le milieu, Xapo, qui est aujourd'hui l'un des plus importants dépositaires de bitcoin au monde pour les particuliers.

Cette financiarisation apporte ainsi un afflux considérable d'argent, mais elle s'accompagne aussi d'un changement de discours. Grâce à sa politique monétaire fixe, le bitcoin est désormais de plus en plus perçu comme un investissement, comme un actif apportant un profit dû à la croissance de son économie. De ce fait, on le voit de moins en moins comme une monnaie permettant d'échanger de la valeur entre particuliers sans l'intervention des banques ou des États.

Contrairement aux cypherpunks et aux libertariens, les nouveaux investisseurs ne sont en effet pas vraiment des anarchistes, appartenant généralement au monde financier traditionnel très à cheval sur la réglementation. Pour eux, il est nécessaire que les usages les plus controversés disparaissent afin que Bitcoin se développe et s'étende au grand public et aux investisseurs institutionnels. Ils voient en particulier d'un mauvais œil la place de marché Silk Road, qui représente alors 10 à 20 % de l'activité économique sur la chaîne de blocs et qui donne à Bitcoin sa réputation de monnaie de la drogue sur Internet [4]. La tendance est donc à l'amélioration de l'image de la cryptomonnaie, une stratégie par ailleurs initiée en 2010 – 2011 par Satoshi Nakamoto lui-même, comme nous avons pu le constater dans le chapitre 1.

C'est dans cette optique qu'est créée la Fondation Bitcoin en septembre 2012. Conformément au modèle de la Fondation Linux, il s'agit d'un consortium d'entreprises de l'écosystème dont le rôle est de financer l'infrastructure logicielle du protocole, de faire du lobbying auprès du régulateur et d'améliorer l'image publique de Bitcoin [5]. Elle est gérée par des acteurs importants dans l'écosystème : Peter Vessenes, le PDG de CoinLab, Gavin Andresen, le mainteneur principal du logiciel de Bitcoin, Mark Karpelès, le PDG de Mt. Gox, Jon Matonis, cryptographe et économiste, Patrick Murck, un juriste spécialisé dans les monnaies virtuelles, et Charlie Shrem, le PDG de BitInstant.

Le 28 novembre 2012, le premier *halving* se produit : la création monétaire du protocole est réduite de moitié et passe de 50 bitcoins à 25 bitcoins par bloc, ce qui abaisse le taux annualisé d'émission à 12,5 %. La transition se passe parfaitement bien. Quelques jours plus tard, un dénommé Matt Whitlock construit un graphique simple pour visualiser l'évolution de la création de bitcoins dans le temps [6] (voir figure 2.1). Cela confirme le changement de focalisation qui passe de son caractère incensurable à sa rareté.

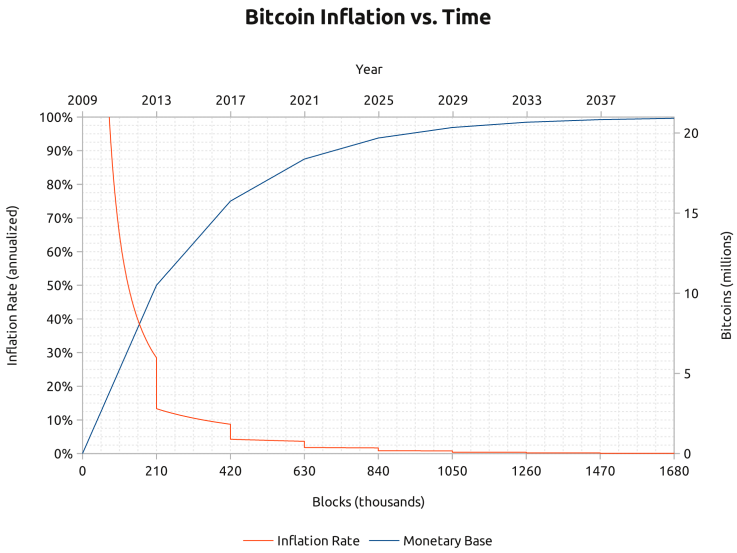

FIGURE 2.1 – Graphique de Matt Whitlock comparant le taux d'émission et la base monétaire du bitcoin en fonction du temps (décembre 2012).

L'augmentation de la demande et la diminution du taux de croissance de l'offre entraînent une hausse sensible du prix du bitcoin. Alors qu'il avoisinait les 5 $ durant la première partie de 2012, il passe à 13 $ en août et se stabilise à ce niveau jusqu'à la fin de l'année. En 2013, sa progression devient parabolique : il dépasse les 20 $ en janvier ; il surmonte l'ancien plus haut des 30 $ en février ; et il finit par atteindre 266 $ sur Mt. Gox en avril.

De façon assez symbolique, un évènement coïncide avec cette hausse : la faillite des banques chypriotes. À cette époque, la crise financière bat son plein sur l'île de Chypre, ce qui pousse le système financier à prendre des mesures drastiques. Le 16 mars 2013, les banques limitent les retraits des comptes de leurs clients. Le 25, le gouvernement chypriote et l'UE décident (sans cadre légal préalable) que la Bank of Cyprus doit être renflouée de manière interne, via une taxation partielle des dépôts de plus de 100 000 euros. La Laiki Bank, deuxième banque du pays, est démantelée suite à sa faillite et les avoirs supérieurs à 100 000 euros sont tout simplement confisqués. Cet évènement vient démontrer l'utilité du bitcoin, cet « or numérique » que l'on peut posséder directement et qui n'est pas soumis aux contraintes des banques à réserves fractionnaires [7].

Du côté de Silk Road, les choses évoluent également. L'enquête des services de renseignement étasuniens, qui a débuté en juin 2011 suite à la publication de l'article d'Adrien Chen sur Gawker et aux injonctions des sénateurs Chuck Schumer et Joe Manchin appelant à fermer la plateforme, commence à porter ses fruits. Après de longues recherches et quelques actions litigieuses de la part des enquêteurs [8], le fondateur de la plateforme, Ross Ulbricht, finit par être suspecté en juin 2013. C'est Gary Alford, un agent de l'*Internal Revenue Service* (le fisc étasunien), qui débusque la piste en retrouvant l'annonce initiale de Ross sur le forum de Bitcoin et en la liant à son adresse de courriel, où figure son nom civil. En juillet 2013, le serveur de Silk Road est saisi par la police islandaise et une copie est partagée aux agences étasuniennes. L'historique contient une connexion depuis une adresse IP située à San Francisco, non loin d'où loge le jeune Texan. En septembre, grâce à cette information, Ross est démasqué.

La chute de Silk Road a lieu au début de l'automne 2013. Le 1er octobre, Ross Ulbricht est maîtrisé par des agents du FBI dans une bibliothèque de San Francisco, avec sa session ouverte sur la plateforme. Le lendemain, le site web est fermé, ce qui provoque l'émoi dans la communauté. Le cours du bitcoin, qui se stabilisait autour des 125 $ lors des jours précédents, chute brutalement pour toucher un niveau bas de 85 $. Entre le 2 et le 25 octobre, près de 174 000

bitcoins appartenant à Ross sont saisis par les agences fédérales, un trésor qui représente alors environ 31 millions de dollars [9].

D'autres personnes liées à Silk Road seront arrêtées et condamnées au cours des années suivantes. Ce sera le cas de Charlie Shrem qui sera interpellé le 27 janvier 2014 par des agents fédéraux (FBI, IRS, DEA) et accusé de facilitation de blanchiment d'argent avec sa société BitInstant. En décembre 2014, il sera condamné à deux ans de prison ferme pour transferts illicites. Ross Ulbricht sera lui condamné à deux peines de réclusion à vie et à 40 ans d'enfermement supplémentaires, pour des charges exclusivement non violentes, dans le but explicite d'en faire un exemple [10].

Bien que la chute de Silk Road représente la destruction d'un pan entier de l'économie de Bitcoin, le cours remonte, conformément aux attentes de certains investisseurs importants. L'engouement pour Bitcoin réapparaît, ce qui provoque une nouvelle flambée du prix qui atteint de nouveaux sommets. Celui-ci, s'étant alors stabilisé au-dessus des 100 $, augmente timidement durant la deuxième moitié d'octobre et dépasse, début novembre, son ancien sommet de 266 $. À partir de là, il monte en flèche et atteint, le 4 décembre 2013, un nouveau plus haut niveau historique sur Mt. Gox à 1 240 $. Cet épisode spéculatif pousse alors beaucoup de médias à parler de Bitcoin pour la première fois.

Cependant, la plateforme Mt. Gox, sur laquelle repose l'essentiel de l'activité spéculative, est beaucoup plus fragile qu'elle ne le paraît. En effet, celle-ci a subi des attaques informatiques tout au long de son existence, entraînant la disparition progressive des fonds. Au début de l'année 2014, il s'avère qu'il manque plus de 650 000 bitcoins dans les caisses de la société, ce qui représente 381 millions de dollars à ce moment-là [11] !

En février 2014, la plateforme Mt. Gox chute. Après avoir suspendu les retraits le 7, le site est mis hors ligne le 25, et la faillite est déclarée le 28. Mark Karpelès présente ses excuses publiques devant les télévisions japonaises. Cette crise est un cataclysme pour Bitcoin : la principale plaque tournante de l'économie ferme ses portes, les détenteurs fortunés qui conservaient leurs bitcoins sur la plateforme perdent tout et la confiance du grand public (qui assimile Bitcoin à Mt. Gox) s'effondre. Cela met fin à l'engouement spéculatif de 2013–2014.

Mark Karpelès est suspecté de détournement de fonds et sa réputation est ternie. Il sera arrêté par la justice japonaise en août 2015, ce qui lui vaudra d'être surnommé le « baron du bitcoin » par les médias français. Plus tard, il sera montré que les pertes de la plateforme provenaient de plusieurs piratages

ayant eu lieu entre 2011 et 2014, et que Mark Karpelès était seulement coupable de négligence et n'avait pas connaissance de la faille qui a permis de retirer la grosse part des bitcoins entre 2011 et 2014.

Néanmoins, cette chute de Mt. Gox aura pour effet d'assainir le marché des plateformes de change. Dorénavant, elles se partageront le marché de manière plus équitable et l'activité se répartira entre des acteurs comme Bitfinex, bitFlyer, Bitstamp, Bittrex, BTCChina, BTC-e, Coinbase, Gemini, OKEx, Kraken ou encore Poloniex.

Le débat sur la scalabilité

La deuxième péripétie qui marque l'histoire de Bitcoin est le débat sur la scalabilité, qui porte sur la capacité du système à passer à l'échelle, c'est-à-dire à continuer de fonctionner de manière équivalente à mesure que le nombre d'utilisateurs augmente. Cette discorde s'amorce au cours de l'année 2013, qui est caractérisée par une forte hausse du prix et de l'activité. Elle dégénère ensuite en une guerre civile en 2015, pour se conclure en 2017 par le schisme en deux communautés distinctes suite à la création d'un nouveau réseau nommé Bitcoin Cash et à l'annulation du projet (artificiel) de compromis SegWit2X. La période constitue une phase d'apprentissage majeure pour la communauté. D'une part, cette dernière prend conscience des imperfections de Bitcoin, qui avait été jusque-là vanté comme un système de monnaie numérique dépourvu d'autorité centrale permettant d'envoyer des paiements instantanés à n'importe qui, n'importe où dans le monde et quasiment sans frais [12]. D'autre part, la communauté se rend compte du mécanisme de gouvernance qui sous-tend l'évolution du protocole, plus complexe qu'elle n'en a l'air (voir ch. 10 et 11).

Le débat sur la scalabilité se concentre sur un paramètre présent dans le protocole qui restreint la capacité transactionnelle du système : la limite de la taille des blocs ou *blocksize limit*. Puisque dans Bitcoin, les transactions sont incluses dans des blocs qui sont ajoutés à la chaîne toutes les 10 minutes en moyenne, limiter la taille de ces blocs revient en effet à instaurer un quota sur le nombre de transactions confirmées.

En 2013, la taille limite est de 1 mégaoctet (1 Mo), ce qui correspond à un flux théorique maximal de 7,37 transactions par seconde. Ajoutée dans le protocole par Satoshi Nakamoto le 12 septembre 2010 sans annonce publique de sa part, cette limite avait initialement pour rôle d'empêcher les attaques par déni de service et devait être augmentée au fil du temps [13]. Néanmoins, après la disparition précipitée du fondateur, la décision a été laissée aux membres de la communauté, ce qui a préparé le terrain pour le conflit.

Dans le débat, deux camps principaux se font face. Le premier est celui des partisans des gros blocs, ou *big blockers*, qui se réclament du projet initial de Satoshi, et qui désirent réaliser des mises à niveau pour accroître la limite, voire la supprimer. Le camp opposé est celui des partisans des petits blocs, ou *small blockers*, qui souhaitent restreindre la taille des blocs, afin de minimiser le coût de gestion d'un nœud.

La première vision, qui est au départ majoritaire, considère que l'augmentation progressive de la taille limite des blocs peut être réalisée sans mettre en danger l'intégrité du système. Cette vision estime que Bitcoin devrait rester un protocole de paiement, qui s'adapte à la demande sans hausse des frais de transaction. Elle favorise de ce fait la facilité d'utilisation par rapport à la sécurité. Elle accepte le recours aux *hard forks*, mises à niveau incompatibles du protocole qui demandent la coordination de tous les membres du réseau pour être réalisées proprement. Il s'agit d'une position plutôt progressiste. De plus, ses partisans jugent généralement que la détermination du protocole est assurée par les mineurs. Cette approche est notamment portée par les développeurs Gavin Andresen, Mike Hearn et Jeff Garzik.

La seconde vision, qui se développe à partir de 2013, se concentre sur la sécurité aux dépens de la facilité d'utilisation. Son but est de minimiser le coût de gestion d'un nœud afin de maximiser la décentralisation du réseau. Cette vision considère que Bitcoin doit être principalement un protocole de règlement, servant de base à des systèmes en surcouche, qui peuvent être centralisés ou décentralisés. Elle prône l'utilisation de *soft forks*, des mises à niveau du protocole rendues rétrocompatibles grâce à l'action des mineurs, et qui peuvent donc être adoptées progressivement par les utilisateurs. Il s'agit d'une position plutôt conservatrice, même si elle admet l'intervention de certains changements essentiels. En outre, ses partisans considèrent généralement que l'intégrité du protocole provient des utilisateurs. Cette approche est notamment soutenue par les développeurs Pieter Wuille, Gregory Maxwell, Wladimir van der Laan et Luke-Jr.

Dans ces deux camps, il existe des nuances et des contradictions. Le sujet de la scalabilité étant complexe et technique, toutes sortes de positions émergent, notamment sur le niveau auquel devrait être fixé la limite de la taille des blocs : 1 Mo, 2 Mo, 8 Mo ?

L'opposition entre les deux tendances se manifeste tout d'abord au sein du projet logiciel de Bitcoin, dont les contributeurs principaux sont majoritairement des partisans des petits blocs. Durant le printemps 2014, le logiciel connaît ainsi un tournant majeur. Au niveau de la forme d'abord, il est re-

nommé « Bitcoin Core » le 19 mars dans le but de « réduire la confusion entre Bitcoin-le-réseau et Bitcoin-le-logiciel [14] ». Puis en ce qui concerne le fond, le dépôt GitHub subit une passation de pouvoir le 7 avril lorsque Gavin Andresen cède son poste de mainteneur principal à Wladimir van der Laan, pour se consacrer à ses activités de scientifique en chef de la Fondation Bitcoin.

Ce changement de gestion se matérialise dans l'année, lorsque Mike Hearn voit sa proposition d'ajout de la requête de réseau `getutxos` être rejetée pour cause de non-unanimité dans l'équipe de Bitcoin Core. L'ingénieur a besoin de cette fonctionnalité pour le développement de son application de financement participatif, Lighthouse. De ce fait, il est contraint de créer Bitcoin XT en décembre 2014, une implémentation alternative issue de Bitcoin Core qui inclut les changements désirés mais qui reste compatible avec le réseau.

Simultanément, la discorde s'étend à l'ensemble de la communauté. La logique des petits blocs se diffuse en particulier grâce à une vidéo produite par le développeur Peter Todd en 2013, qui explique « pourquoi la taille limite des blocs permet à Bitcoin de rester libre et décentralisé [15] ». Un autre argument invoqué est celui du marché des frais, notamment mis en valeur par l'économiste français Nicolas Houy, qui explique dans un article de 2014 que « laisser les frais de transaction résulter d'un marché *et* rendre la taille des blocs non pertinente ou non contraignante conduirait à un niveau de sécurité trop faible pour Bitcoin [16] ». Enfin, les partisans des petits blocs cherchent à justifier leur point de vue en proposant des solutions de passage à l'échelle, permettant d'accroître l'activité économique soutenue par le réseau sans pour autant augmenter significativement la taille des blocs.

La première est la proposition des chaînes latérales, ou *pegged sidechains*, qui sont des chaînes secondaires fonctionnant en parallèle de la chaîne principale, vers et depuis lesquelles des bitcoins peuvent être transférés grâce à un ancrage bilatéral. Cette proposition est présentée pour la première fois dans un document technique le 22 octobre 2014 par les développeurs de l'entreprise Blockstream. Cofondée par Adam Back, des développeurs de Bitcoin Core et des personnalités de la finance, cette société dont la création est annoncée le même jour a pour but de « trouver une manière d'étendre l'utilisation de Bitcoin, qui soit architecturalement solide et qui ne nécessite pas d'autorisation, pour que la cryptomonnaie atteigne son plein potentiel [17] ». Elle se focalisera dans un premier temps sur le développement des sidechains, ce qui donnera naissance au modèle Elements et à sa mise en œuvre, Liquid.

La seconde proposition est celle du réseau Lightning, ou *Lightning Network*, un réseau de canaux de paiements bâti en surcouche de Bitcoin permet-

tant d'effectuer des transferts instantanés et quasi-gratuits de pair à pair. Le concept est présenté en février 2015 par Joseph Poon et Thaddeus Dryja lors d'un séminaire de développeurs à San Francisco. Le 28 février, ils publient le livre blanc de leur invention, qui est intitulé « *The Bitcoin Lightning Network* » et qui présente les éléments de base nécessaires pour construire un tel réseau [18]. En particulier, une implémentation fluide de Lightning demande de modifier le protocole Bitcoin par l'ajout de verrous temporels dans le langage de script et par la correction d'un défaut appelé la malléabilité des transactions [19].

Ces deux propositions font envisager un passage à l'échelle par surcouche, qui ne nécessiterait pas de s'en remettre totalement à un tiers de confiance et qui ne compromettrait pas la sécurité de la chaîne toute entière.

Du côté des partisans des gros blocs, on se concentre surtout sur l'optimisation du logiciel et du protocole afin d'alléger la charge des nœuds. Ainsi, le 6 octobre 2014, Gavin Andresen publie une feuille de route sur le blog de la Fondation Bitcoin dans laquelle il décrit la façon dont les effets de l'augmentation de l'activité du réseau pourraient être compensés par des changements du protocole et par l'évolution exponentielle de la technique décrite par les lois de Moore et de Nielsen [20]. L'article mentionne notamment l'élagage des blocs les plus anciens (*block pruning*) qui permettrait de diminuer la taille de la chaîne à conserver, l'« engagement des UTXO » ayant pour but d'accélérer le téléchargement initial des blocs, ou encore le relai des blocs par *Invertible Bloom Lookup Tables* qui serait plus efficace.

Au printemps 2015, la taille moyenne des blocs approchant les 500 ko, l'idée d'augmenter la capacité transactionnelle du réseau est remise sur le devant de la scène sous l'impulsion de Gavin Andresen qui publie une série d'articles à ce sujet sur son blog personnel. Dans les mois qui suivent, plusieurs propositions apparaissent, notamment celle de Gavin d'augmenter la limite à 8 Mo (BIP-101), conformément aux vœux des coopératives minières chinoises, et celle de Pieter Wuille d'augmenter cette limite de 17,7 % par an (BIP-103). Malheureusement aucune proposition ne satisfait les forces en présence. Cela a pour effet d'intensifier le conflit au sein de la communauté, qui dégénère alors en une véritable guerre civile.

La guerre des blocs

Le conflit sur la taille des blocs prend un tournant majeur au cours de l'été 2015, avec la sortie de la version 0.11A de Bitcoin XT le 15 août, qui inclut une augmentation de la limite de la taille des blocs, changement incompatible

avec les règles du réseau [21]. La mise à niveau intégrée est le BIP-101 qui programme un passage de la limite de 1 à 8 Mo, à condition d'atteindre un signalement suffisant des mineurs, à savoir 75 % de la puissance de calcul du réseau. De ce fait, cette version du logiciel a la possibilité de créer une séparation du réseau et une scission de la chaîne en deux chaînes distinctes.

L'implémentation Bitcoin XT est dirigée par Mike Hearn qui se décrit comme un « dictateur bienveillant » (concept courant dans le monde du logiciel libre). Gavin Andresen participe au projet et a son mot à dire sur la direction prise, mais « Mike prend les décisions finales en cas de litiges graves [22] ». L'augmentation de la taille limite des blocs est soutenue par les grandes coopératives minières chinoises et par une partie des entreprises de l'industrie.

Ce mouvement ressemble grandement à un passage en force aux yeux d'un noyau dur de la communauté, ce qui ne manque pas de provoquer sa réaction épidermique. Dans la nuit du 16 au 17 août, Michael Marquardt (alias Theymos), le modérateur principal du subreddit r/Bitcoin et cogestionnaire du forum Bitcointalk, publie ainsi un long article sur Reddit dans lequel il annonce interdire toutes les discussions à propos de Bitcoin XT [23]. Dans cet article, il explique en particulier pourquoi il considère que Bitcoin XT ne peut pas être Bitcoin, et que les échanges à son sujet n'ont par conséquent pas leur place sur le subreddit. Puisque l'essentiel des conversations se passe sur r/Bitcoin à l'époque, cette décision a un impact non négligeable.

L'apparition de Bitcoin XT marque donc le début d'une guerre civile au sein de la communauté, que l'on appellera la guerre des blocs ou la *block-size war* [24], au cours de laquelle la diplomatie fait progressivement place à l'animosité. Dans la journée du 17 août, le journaliste Alex Hern écrit dans le Guardian : « La guerre des bitcoins a commencé [25]. » Celle-ci sera marquée par une forte propagande des deux côtés, par la censure sur les principaux canaux de communication et par des attaques par déni de service contre les nœuds utilisant Bitcoin XT et ses successeurs.

Toutefois, au début, beaucoup cherchent à apaiser le conflit et appellent à la discussion. C'est le but des conférences appelées *Scaling Bitcoin*, organisées pour présenter les différentes manières de faire passer Bitcoin à l'échelle. La première édition se déroule en septembre à Montréal et parvient à réunir des individus des deux camps dans une bonne foi partagée. La deuxième édition a lieu en décembre à Hong Kong, où la tension est déjà plus palpable.

Durant *Scaling Bitcoin II*, une nouvelle proposition pour Bitcoin est présentée : Segregated Witness ou, plus simplement, SegWit. Imaginée par Gre-

gory Maxwell et Pieter Wuille, celle-ci prévoit de faciliter l'implémentation du réseau Lightning (en corrigeant la malléabilité des transactions) et d'augmenter la capacité transactionnelle de façon rétrocompatible pour les nœuds non miniers. Elle fait partie de la feuille de route de Gregory Maxwell publiée le même jour sur la liste de diffusion [26] et devient rapidement la mise à niveau défendue par les partisans des petits blocs.

Au début de l'année 2016, Bitcoin XT échoue et Mike Hearn quitte la communauté dans un abandon rageur retentissant [27]. Cependant, une nouvelle implémentation émerge du côté des partisans des gros blocs : Bitcoin Classic. Celle-ci intègre une version modifiée du BIP-101 qui porterait une taille limite de 2 Mo en cas d'un signalement de 75 % de la puissance de calcul du réseau. Bitcoin Classic gagne rapidement en popularité au point d'interpeler le camp opposé [28].

Le 20 février 2016, une réunion d'urgence est organisée à Hong Kong. Cette « Table Ronde » réunit les principales coopératives minières, certaines entreprises de l'écosystème et des contributeurs majeurs de Bitcoin Core, dont Matt Corallo, Peter Todd ou encore Luke-Jr. Après de nombreuses heures de discussions sous pression, les participants arrivent à une entente, que l'on appellera l'accord de Hong Kong. D'un côté, les développeurs de Bitcoin Core s'engagent à implémenter SegWit et un doublement de la limite de la taille de base des blocs. De l'autre, les mineurs s'engagent à activer SegWit et à n'utiliser que Bitcoin Core [29].

Mais ce sentiment de compromis ne dure pas, car l'année 2016 amène deux évènements qui changent la donne. Le premier est l'intervention de Craig S. Wright, un informaticien et entrepreneur australien qui prétend être Satoshi Nakamoto. Il est propulsé sur le devant de la scène en décembre 2015 suite à la publication de deux enquêtes indépendantes par Wired et Gizmodo, selon lesquelles il serait probablement le créateur de Bitcoin. Ces enquêtes se fondent sur des éléments qui laissent en effet penser qu'il a pu être impliqué dans la conception de la cryptomonnaie aux côtés de son ami Dave Kleiman, décédé en 2013.

Quelques mois plus tard, le 2 mai 2016, Craig Wright publie un long et tortueux article de blog [30], dans lequel il inclut une signature correspondant à la clé publique utilisée pour recevoir la récompense du bloc 9 et envoyer le premier paiement à Hal Finney en janvier 2009. En outre, un entretien de Craig Wright avec la BBC est mis en ligne ce jour-là, dans lequel l'Australien affirme avoir été « l'élément principal » derrière Satoshi Nakamoto, mais que « d'autres personnes l'ont aidé [31] ». Il prétend également avoir signé un

message en privé devant le journaliste qui l'interroge.

Cependant, il s'avère que les documents fournis dans les enquêtes et les éléments avancés par Craig Wright lui-même ne sont pas probants. En particulier, on découvre très rapidement que la signature présente dans l'article de blog est la signature d'une transaction existante sur la chaîne de Bitcoin qui est simplement encodée différemment [32]. Ce fait incite la communauté à la prudence.

Le même jour, Gavin Andresen publie un article dans lequel il dit croire que Craig Wright est « la personne qui a inventé Bitcoin », ce dernier lui ayant présenté en personne « des messages signés avec les clés que seul Satoshi devrait posséder [33] ». En conséquence, le rôle de mainteneur et le *commit access* de Gavin sur le dépôt de Bitcoin Core sont révoqués dans la foulée, sous prétexte que les membres de l'équipe de Bitcoin Core craignent qu'il ait été piraté. De manière générale, cette affirmation douteuse, confirmée en personne le jour-même lors de la conférence Consensus 2016, a pour effet de le discréditer et son accès au dépôt GitHub ne sera jamais restauré. Il reconnaîtra plus tard avoir été dupé.

Le second évènement qui vient influencer le conflit est un incident qui ne se passe pas au sein de la communauté de Bitcoin, mais sur Ethereum, un système alternatif à Bitcoin dédié aux *smart contracts* lancé en 2015. Il s'agit de la scission entre Ethereum (ETH) et Ethereum Classic (ETC) qui fait suite au piratage de TheDAO.

Le 17 juin 2016, le contrat de TheDAO, une organisation autonome décentralisée ayant pour mission d'investir dans l'écosystème, est piraté et 3,6 millions d'éthers (l'éther est l'unité de compte d'Ethereum) valant 50 millions de dollars sont dérobés, ce qui représente 4,4 % de la quantité totale d'éthers en circulation à l'époque. La décision est alors prise par une grande majorité de la communauté d'annuler purement et simplement ce vol par la modification de l'état du système. Un mois plus tard, le 20 juillet, le changement est appliqué ce qui conduit à une scission de la chaîne en deux chaînes distinctes : celle suivant le protocole modifié (qui est majoritaire et qui prendra le nom d'Ethereum) et celle suivant le protocole initial (qui est minoritaire et qui s'appellera Ethereum Classic). Les détenteurs se retrouvent avec des éthers différents des deux côtés.

Cette séparation n'est pas propre. En particulier, elle n'inclut pas de protection contre la rediffusion des transactions, ce qui signifie que des transferts réalisés sur une chaîne peuvent être répliqués sur l'autre par un tiers, menant à des « attaques par rediffusion » (*replay attacks*). Cela perturbe les plateformes

de change qui doivent composer avec ce problème. Ainsi, même si le prix combiné des deux éthers finit par être supérieur au prix de l'éther initial, tout le monde peut observer les effets négatifs d'une scission créée par un hard fork. Cet exemple conforte de ce fait la position conservatrice des partisans des petits blocs qui recommandent de faire évoluer le protocole par des soft forks tels que SegWit.

À cause de ces deux évènements, le camp des partisans des gros blocs ressort de cette année 2016 particulièrement diminué, tant au niveau réputationnel qu'argumentatif.

C'est ce moment que choisissent les développeurs de Bitcoin Core pour lancer le signalement de SegWit par les mineurs, qui commence le 15 novembre 2016, pour une période d'un an. La mise à niveau exige un taux de signalement de 95 % de la puissance de calcul pour être activée, dans le but d'assurer largement la rétrocompatibilité du changement.

Cependant, les principales coopératives minières refusent SegWit (pour des raisons multiples [34]) et, durant les premiers mois, le taux de blocs en faveur de la mise à niveau stagne autour des 25 %, très loin du seuil demandé. SegWit est bloqué.

Au début de l'année 2017, les blocs commencent à être pleins, ce qui engendre une augmentation significative des frais de transaction et des temps de confirmation sur la chaîne. Mi-février, les frais médians dépassent les 30 centimes de dollar, pour la première fois dans l'histoire de Bitcoin. C'est dans ce contexte que la demande pour un changement s'accroît de part et d'autre du conflit.

D'un côté, nous avons Bitcoin Unlimited, une implémentation qui a gagné en popularité chez les partisans des gros blocs lors de l'été 2016 et qui a pris la relève de Bitcoin Classic. Celle-ci est notamment soutenue par Roger Ver, le PDG de l'entreprise Bitcoin.com qui est alors devenu une personnalité influente de la communauté [35], ce qui permet à Bitcoin Unlimited de disposer d'un large financement. En mars 2017, le signalement pour Unlimited dépasse ainsi celui de SegWit.

Cependant, le 17 mars, la possibilité d'un hard fork contentieux pousse les plateformes de change à considérer la potentielle monnaie créée par Bitcoin Unlimited comme une cryptomonnaie alternative. Fortes de leur expérience avec la scission entre ETH et ETC, elles exigent en outre qu'elle intègre une protection contre la rediffusion, faute de quoi elle ne sera même pas listée. Cette décision est dévastatrice pour les partisans des gros blocs.

De l'autre côté, la pression en faveur de l'activation de SegWit s'intensifie

au sein des partisans des petits blocs, qui commencent à devenir impatients. Ainsi, le 12 mars 2017, un individu se faisant appeler Shaolin Fry publie la proposition d'un UASF (« *User Activated Soft Fork* ») qui permettrait de verrouiller la mise à niveau sans le signalement des mineurs dès le 1er août [36]. Cette mesure, pour le moins audacieuse, est dangereuse et ne fait pas l'unanimité parmi les *small blockers*, comme l'illustre l'opposition de Gregory Maxwell.

Cependant, la menace de l'UASF existe et exerce une influence. Ainsi, devant le désir de la communauté de procéder à SegWit, les gros acteurs de l'écosystème (entreprises et mineurs) sont amenés à signer un accord le 23 mai 2017, en marge de la conférence Consensus 2017 à New York. Cet accord de New York, comme on l'appellera par la suite, représente un compromis théorique dans le conflit qui fait rage : il engage les signataires, d'une part, à activer SegWit avec un seuil de signalement de 80 % de la puissance de calcul, d'autre part, à doubler la taille limite des blocs dans les six mois qui suivent. La mise à niveau implémentant cet accord prendra le nom de SegWit2X. Ce pseudo-compromis est néanmoins rapidement critiqué en raison de l'absence des développeurs de Bitcoin Core à la réunion, qui n'étaient tout simplement pas conviés.

L'accord mène à l'activation de SegWit durant l'été 2017. En juillet, les mineurs commencent à signaler massivement la mise à niveau. Le 21, le processus de verrouillage est enclenché (ce qui rend l'UASF ineffectif). SegWit finit par être activé le 24 août 2017.

La mise à niveau se passe très bien. Cependant, il se produit au même moment une autre scission, pleinement désirée. En opposition à l'UASF, les mineurs décident d'activer un nouveau protocole, incompatible avec le protocole originel, qui n'intègre pas SegWit et qui implémente une taille limite des blocs de 8 Mo : Bitcoin Cash. Le lancement de ce protocole est placé sous l'autorité d'Amaury Séchet, un développeur français.

Le 1er août 2017, avec le bloc 478 559 miné à 18 heures 12, naît ainsi Bitcoin Cash. À la suite de cette scission, les détenteurs de bitcoin se retrouvent avec un montant similaire en bitcoins (BTC) et en bitcoins cash (BCH). Ceux qui désapprouvent SegWit rejoignent Bitcoin Cash.

Durant le mois d'août, alors que SegWit est enfin verrouillé, certains partisans des petits blocs commencent à s'opposer à la deuxième partie de SegWit2X, le doublement de la taille des blocs, via une campagne de communication baptisée « NO2X ». Dans leur argumentaire, ils insistent en particulier sur l'absence de rediffusion des transactions que comporte ce hard fork. En

effet, SegWit2X est pensé comme un changement non contentieux et n'inclut par conséquent pas ce type de procédé qui alourdirait considérablement la charge de la mise à jour pour les portefeuilles.

L'opposition gronde. Les développeurs de Bitcoin Core refusent d'approuver ce changement. Les utilisateurs se mobilisent pour protester, car « la manière dont l'accord a été conclu va à l'encontre de l'essence même de Bitcoin [37] ». Face à cette opposition, les entreprises signataires de l'accord de New York se rétractent peu à peu.

Le projet de doublement de la limite de la taille des blocs est finalement abandonné le 8 novembre 2017, soit une semaine avant son activation programmée. Les promoteurs du projet – Mike Belshe, Wences Casares, Jihan Wu, Jeff Garzik, Peter Smith et Erik Voorhees – déclarent conjointement :

> « Notre objectif a toujours été d'améliorer Bitcoin en douceur. Bien que nous croyons fermement en la nécessité d'augmenter la taille des blocs, il y a une chose que nous croyons encore plus importante : préserver la cohésion de la communauté. Malheureusement, il est clair que nous n'avons pas recueilli un consensus suffisant à l'heure actuelle pour une modification propre de la taille des blocs. Continuer sur la voie actuelle pourrait diviser la communauté et constituer un revers pour la croissance de Bitcoin. Cela n'a jamais été l'objectif de Segwit2x [38]. »

C'est une grande victoire pour la philosophie des petits blocs qui dominera dorénavant la chaîne. Pour ce qui est des solutions de scalabilité sur BTC, le réseau Lightning est lancé en version bêta en mars 2018. Le concept de chaîne latérale est également expérimenté, avec le lancement de Rootstock en janvier 2018 et celui de la sidechain Liquid développée par Blockstream en septembre de la même année.

De l'autre bord, suite à l'annulation de SegWit2X, beaucoup de partisans de l'augmentation de la capacité de la chaîne se dirigent vers d'autres protocoles comme Bitcoin Cash ou Ethereum.

Malgré le dénigrement constant de ses détracteurs, l'évolution de Bitcoin Cash suivra son cours. Néanmoins, sa communauté se délitera progressivement et la cryptomonnaie connaîtra deux scissions majeures avec la création de Bitcoin SV en novembre 2018 puis celle de « eCash » (XEC) en novembre 2020. La part de marché de l'ensemble dégringolera en conséquence : en novembre 2023, la valeur agrégée de ces trois cryptomonnaies représentait moins de 1 % de celle du BTC.

L'essor des cryptomonnaies alternatives

Bitcoin est un projet libre : il se base sur un code source ouvert qui peut être copié et déployé sur un nouveau réseau par n'importe qui. Cette particularité est excellente pour l'innovation : un individu, quel qu'il soit, peut apporter des modifications au code et en faire la base d'une nouvelle cryptomonnaie s'il le désire. La découverte de Bitcoin ouvre ainsi la voie à une vraie concurrence des monnaies sur Internet. Cependant, cette liberté existe aussi pour les personnes mal intentionnées qui peuvent profiter de cette ouverture pour créer des projets douteux, allant de la cryptomonnaie inutile à l'escroquerie pure et simple, en passant par la pyramide de Ponzi ouverte. C'est dans cette dualité entre l'honnêteté de l'innovateur et la cupidité du malfaiteur que se produit l'essor de ce qu'on appelle les « cryptomonnaies alternatives » (ou « *altcoins* » en anglais).

La première idée d'une cryptomonnaie distincte de Bitcoin apparaît alors que Satoshi est encore présent dans la communauté. En novembre 2010, une discussion sur un système distribué de noms de domaine (alors appelé BitDNS) s'engage sur IRC, puis sur le forum de Bitcoin. Il s'agit d'associer des identifiants de site web (DNS) à des pièces créées par le protocole, comme les bitcoins dans Bitcoin. Le registre étant public et difficilement falsifiable, cela améliorerait les choses par rapport au système existant. Satoshi n'est pas hostile à l'idée et suggère de miner la chaîne en combinaison (*merge mining*) avec celle de Bitcoin [39]. Cela donne finalement naissance à Namecoin en avril 2011, créé sous l'impulsion de Vincent Durham.

Par la suite, d'autres cryptomonnaies apparaissent, comme Ixcoin ou Tenebrix. Tenebrix a la particularité d'implémenter l'algorithme de preuve de travail scrypt, mis au point par le mineur ArtForz et supposément résistant aux processeurs graphiques. En octobre 2011, Litecoin est lancé par Charlie Lee, en tant que « version allégée de Bitcoin » dont les blocs sont minés quatre fois plus rapidement, dont l'unité de compte est quatre fois moins rare et qui intègre l'algorithme scrypt. Litecoin a pour but d'être « à l'argent ce que Bitcoin est à l'or [40] ».

En août 2012, Sunny King et Scott Nadal lancent PPCoin, un système introduisant le procédé de preuve d'enjeu, qu'ils présentent comme une alternative à la preuve de travail « économe en énergie à long terme [41] ». La preuve d'enjeu est intégrée de manière hybride aux côtés de la preuve de travail. PPCoin sera progressivement rebaptisé Peercoin au cours des années.

En 2013, avec l'engouement financier résultant du succès du bitcoin, la création de cryptomonnaies originales devient extrêmement rentable. Les nou-

veaux protocoles se multiplient à l'instar de Feathercoin en avril, de Primecoin en juillet ou encore du célèbre Dogecoin en décembre. Le site web coinmarketcap.com est créé en mai 2013 pour recenser l'ensemble des cryptomonnaies et les classer par « capitalisation boursière », c'est-à-dire par leur valeur agrégée (le nombre d'unités multiplié par le prix unitaire).

Cependant, ce foisonnement n'est pas du goût de tout le monde et un mouvement de rejet se forme face à ce qui ressemble à une fragmentation dommageable de l'écosystème. Dès 2011, on voit un certain scepticisme se développer vis-à-vis des premières cryptomonnaies alternatives, scepticisme qui transparaît dans les réactions de Hal Finney et de Gavin Andresen. Puis, le rejet devient plus tranché en août 2013 avec les prises de positions de Gavin Andresen (encore lui), qui assimile la création de nouvelles cryptomonnaies à de l'inflation [42], et de Daniel Krawisz, auteur pour le Satoshi Nakamoto Institute, qui met en lumière la difficulté extrême de surpasser l'effet de réseau de Bitcoin [43].

En parallèle, on assiste à la formation de la tendance contraire : un pluralisme cryptomonétaire qui prône l'ouverture et la tolérance envers cette diversité des cryptomonnaies. Celui-ci est en particulier défendu par le jeune Vitalik Buterin en septembre 2013 [44], qui le mettra en pratique avec l'élaboration de son propre projet, Ethereum.

À partir de 2014, cette tendance est renforcée par l'apparition de systèmes cryptoéconomiques fondamentalement plus pertinents que les simples copies de Bitcoin. Ainsi, pour corriger le manque de confidentialité de la chaîne de blocs de Bitcoin, plusieurs solutions voient le jour. C'est le cas de Darkcoin qui démarre en janvier 2014 (et qui deviendra plus tard Dash). Monero, un protocole intégrant la confidentialité par défaut dont le nom signifie « pièce de monnaie » en espéranto, est lui lancé en avril. En outre, la publication des protocoles Zerocoin et Zerocash par Matthew Green en 2013 mèneront à la création de Zcash en octobre 2016.

Mais la confidentialité n'est pas le seul terrain d'innovation, et d'autres protocoles séparés émergent pour mettre en œuvre un perfectionnement de l'aspect programmable de Bitcoin, conformément à l'idée d'un « Bitcoin 2.0 » qui se diffuse alors dans la communauté. En effet, le protocole de Satoshi est peu adapté pour réaliser des opérations complexes et créer des jetons numériques secondaires, même si cela peut se faire sur des surcouches comme Omni et Counterparty. C'est pourquoi on assiste à la naissance de nouveaux systèmes, à l'instar de Bitshares, une place de marché décentralisée qui a la particularité de fonctionner par preuve d'enjeu déléguée, et de NXT,

une plateforme incluant un grand nombre de fonctionnalités. Mais le système qui se distingue le plus est Ethereum.

Ethereum reprend la programmabilité de Bitcoin et la généralise en constituant une sorte d'ordinateur mondial décentralisé, fonctionnant en parallèle sur tous les nœuds d'un réseau pair à pair. Ce projet est, comme on l'a dit, issu de l'esprit de Vitalik Buterin, qui en dresse les contours à la fin de l'année 2013. Avec ses 7 cofondateurs, il réalise une prévente de jetons en juillet-août 2014, qui recueille 31 529 bitcoins [45] (soit plus de 15 millions de dollars à l'époque) pour en financer le développement. Ethereum est un système volontairement plus progressiste, plus innovant et plus flexible que Bitcoin. La chaîne sera officiellement lancée un an plus tard, le 30 juillet 2015.

L'année 2014 est enfin l'année où apparaît le premier *stablecoin*, le Tether USD (ou USDT), qui est lancé sur la chaîne de Bitcoin le 6 octobre sous le nom de Realcoin. Ce jeton numérique est adossé au dollar grâce à la garantie de l'entreprise Tether Limited, qui s'engage à racheter chaque unité contre un dollar réel. Cette cryptomonnaie « stable » permet aux individus et aux plateformes de change de bénéficier de la faible volatilité du dollar, sans avoir à en subir les inconvénients légaux.

Face à ce développement, le mouvement de rejet à l'égard de ces nouveaux projets continue de croître. Il s'illustre le 22 octobre 2014 par la publication du document de Blockstream sur les sidechains, qui vient décrire comment Bitcoin pourrait être à la base de tous les cas d'utilisation, et d'un article complémentaire, expliquant la démarche derrière la fondation de la société. Dans ce dernier, les développeurs travaillant pour Blockstream écrivent ainsi :

> « L'approche des altcoins, qui consiste à créer une nouvelle cryptomonnaie uniquement pour introduire de nouvelles fonctionnalités, crée une incertitude pour tous ceux qui observent les cryptomonnaies de l'extérieur. Il ne semble pas y avoir de point d'arrêt naturel, chaque copie pouvant être copiée à nouveau, à l'infini. Cela crée à la fois une fragmentation du marché et une fragmentation du développement. Nous pensons que pour que les cryptomonnaies réussissent dans leur ensemble, nous devons favoriser l'effet de réseau, et non la fragmentation [46]. »

Au fil des années, ce rejet prend progressivement le nom de maximalisme du bitcoin (*bitcoin maximalism*), par réappropriation du terme utilisé péjorativement par Vitalik Buterin à l'encontre de ceux qui dénigrent systématiquement les cryptomonnaies alternatives [47]. Le mouvement prône la maximisation de la dominance économique du bitcoin par rapport à ses concurrents proches et prescrit à ses partisans d'agir dans ce sens. Il s'agit de mettre en valeur l'ef-

fet de réseau, non seulement parce que c'est techniquement nécessaire mais aussi parce que c'est moralement désirable [48].

Cependant, devant les limites de Bitcoin mises en exergue durant la guerre des blocs, le phénomène de substitution des autres systèmes cryptoéconomiques va en s'intensifiant au fur et à mesure du temps. Ainsi à partir de mars 2017, la dominance du BTC par rapport aux autres cryptomonnaies décroche du niveau des 85 % où elle se maintenait jusqu'alors pour rejoindre les 40 % en juin. Cela vient en particulier de l'essor d'Ethereum, qui constitue un moyen simple d'émettre des jetons programmables sur sa chaîne de blocs. Cette fonctionnalité permet notamment de lever des fonds en réalisant une prévente de jetons, nommée *Initial Coin Offering* ou ICO, pour financer des projets dans lesquels interviendront les jetons en question. Le nombre de levées de fonds de ce type explose en 2017 – 2018, à tel point que l'on parle de « folie des ICO ». La plus importante d'entre elles, celle d'EOS, lève 4,1 milliards de dollars sur une période d'un an.

En 2019, un autre enthousiasme se dessine : celui de la finance décentralisée, appelée *decentralized finance* ou DeFi en anglais. L'objectif de la DeFi est de reproduire les outils du système financier traditionnel de manière numérique, décentralisée, ouverte et transparente. Il s'agit de minimiser l'intermédiation (souvent de manière imparfaite) intervenant dans l'exécution de diverses opérations financières : les échanges, le prêt sur gage (aussi appelé crédit lombard), la création de produits dérivés, les marchés prédictifs, etc. Ce développement a principalement lieu sur Ethereum et est notamment incarné par l'émergence du protocole Maker qui permet l'existence du premier stablecoin décentralisé : le dai. Dans la DeFi, le BTC est utilisé comme un collatéral de premier choix. À côté de cela, il se crée une nouvelle mode autour des jetons non fongibles ou NFT (pour *non-fongible tokens*), un engouement qui finit par toucher le grand public à partir de 2021.

Cependant, tous ces projets souffrent de failles techniques et humaines parfois très importantes, de sorte que la critique reste pertinente. À certains projets, il manque bien souvent la fameuse « décentralisation » qu'ils prétendent posséder. D'autres sont des doublons, qui n'apportent rien et disparaissent à cause de l'effet de réseau de leurs concurrents. D'autres enfin sont tout simplement des escroqueries, dans le sens où leurs promoteurs principaux mentent pour vendre leur jeton. Tout ceci explique pourquoi le maximalisme du bitcoin subsiste encore à l'écriture de ces lignes.

L'intégration institutionnelle

L'ouverture à la finance traditionnelle initiée en 2012 se traduit au fil du temps par une intégration dans le système légal existant. Cette tendance est naturelle : pour que Bitcoin existe, il doit jouir d'une certaine tolérance de la part de la population et, *in fine*, des autorités qui « représentent » cette dernière.

L'institutionnalisation passe en premier lieu par la réglementation (ou « régulation ») du secteur, qui consiste à l'assujettir à un cadre légal généralement défini et appliqué par l'État. En pratique, il s'agit de soumettre les acteurs financiers importants à des normes plus ou moins drastiques. La réglementation est donc synonyme de contrôle, chose à quoi Bitcoin s'oppose fondamentalement, d'où la tension qui en découle.

Dès les premières années d'existence de Bitcoin, les agences de renseignement s'y intéressent, aux États-Unis comme en France. Ainsi, en avril 2011, la CIA invite Gavin Andresen à venir parler de Bitcoin, chose qu'il fait en juin. Le 9 mai 2012, un rapport interne du FBI sur Bitcoin fuite sur Internet : on peut y lire que « si Bitcoin se stabilise et gagne en popularité, il deviendra un outil de plus en plus utile pour diverses activités illégales au-delà du cyberespace [49] ». En juillet 2012, un rapport de Tracfin dit que les « monnaies virtuelles » posent un « risque spécifique en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme [50] ».

Ces enquêtes préparent la réglementation financière qui se met en place à partir de 2013, sous l'effet de la hausse du cours du printemps. C'est ainsi que, le 18 mars, le FinCEN (*Financial Crimes Enforcement Network*) publie un document clarifiant sa position sur les monnaies numériques [51]. Il spécifie dans celui-ci que les plateformes de change sont des entreprises de services monétaires (*money services business*) et doivent par conséquent obtenir une licence pour exercer aux États-Unis.

Peu à peu, les normes se durcissent. Les plateformes se mettent à appliquer une procédure de connaissance du client (appelée en anglais *Know Your Customer* ou KYC) en imposant une vérification d'identité pour accéder à leurs services. Elles peuvent également aller plus loin dans le cadre de la « lutte contre le blanchiment des capitaux et le financement du terrorisme » (LCB-FT).

D'autres réglementations financières s'appliquent aux cryptomonnaies, comme la taxation des plus-values. En France par exemple, l'utilisateur est légalement contraint de déclarer ses plus-values réalisées lors des « cessions à titre onéreux d'actifs numériques » et de payer un impôt de 30 % sur celles-ci,

si le total des ventes représente plus de 305 € sur l'année [52].

La réglementation diffère cependant entre les juridictions. Et si certaines sont clémentes, d'autres le sont beaucoup moins. C'est par exemple le cas de l'État de New York qui, en 2015, fait passer une réglementation ultrarestrictive, imposant à une large part des acteurs de l'écosystème d'obtenir une licence d'exploitation appelée la « BitLicence ». Dans le même esprit, l'État français fait passer un décret en novembre 2019 pour assujettir les prestataires de services sur actifs numériques (PSAN) à des conditions strictes. Dans les deux cas, cela a pour effet de faire fuir les acteurs locaux vers des juridictions plus accomodantes.

Outre cette réglementation, le discours des acteurs traditionnels est au départ ouvertement hostile à la conception originelle de Bitcoin. On peut le voir en 2014 – 2015 avec l'apparition du terme « *blockchain technology* », dont le but caché est de nier le côté rebelle de la cryptomonnaie, en amalgamant l'ensemble des techniques de consensus distribué au sein d'une même appellation. Cet appel à la blockchain est popularisé en 2015 par Blythe Masters, une ancienne opératrice de marché de JPMorgan Chase, connue pour avoir conçu les contrats de couverture de défaillance (CDS), à l'origine de la crise des subprimes [53]. Cependant, le discours s'adoucit au fur et à mesure que les années passent.

La réglementation amène ainsi de nouvelles contraintes, en opposition frontale au principe d'absence d'autorisation intrinsèquement lié à Bitcoin. Mais elle permet peu à peu à de plus gros investisseurs, comme les fonds d'investissement, d'entrer sur le marché avec de la liquidité, de légitimer la cryptomonnaie aux yeux du grand public, qui a besoin d'une approbation officielle pour oser s'y intéresser. Cela pousse ainsi certains acteurs de la communauté à chercher à coopérer avec le régulateur.

En 2017, un nouvel engouement spéculatif apparaît, durant lequel le prix du bitcoin connaît une forte hausse en passant de 1 000 $ en janvier à 20 000 $ en décembre. Cette nouvelle bulle attire à nouveau l'attention des médias. Bitcoin est désormais pris beaucoup plus au sérieux. En décembre 2017, il entre même à la bourse de Chicago pour faire l'objet d'un contrat à terme, ce qui correspond à une avancée notable.

Après la guerre des blocs, le BTC est en effet vu comme une sorte d'or numérique au sens strict, comme un actif décorrélé des autres marchés financiers qui constituerait une valeur refuge, à tel point que certains analystes en viennent à considérer les crypto-actifs comme une nouvelle classe d'actifs. Pour une part croissante d'utilisateurs, le bitcoin est même perçu comme une

réserve de valeur qui pourrait servir d'étalon au système monétaire mondial et s'intégrer au système légal des différentes instances étatiques.

Ce changement de vision cause un conflit croissant entre ceux qui considèrent le bitcoin comme un intermédiaire d'échange dédié au marché noir et ceux qui le voient comme une monnaie de réserve. D'un côté, les partisans de l'aspect libre et sans autorisation de Bitcoin refusent catégoriquement toute réglementation, considérant cela comme une compromission des valeurs originelles du projet. De l'autre, les partisans de la monnaie de réserve perçoivent bien qu'il faut coopérer avec les autorités en charge pour que les entités les plus fortunées (fonds d'investissement, grandes entreprises, États) puissent en acheter. Pour cela, ils parient sur la représentation d'intérêts (lobbying) et sur le contexte géopolitique (diplomatie).

En 2020, la réaction mondiale à la pandémie de Covid-19 vient accélérer les choses. Les États occidentaux imposent des confinements durs à leurs populations et paralysent leurs économies, ce qui provoque le début d'une crise déflationniste. Les banques centrales réagissent en conséquence par une injection de liquidités record. Comme en 2008, le but est de sauver l'économie en créant de l'argent et en l'injectant sur le marché : 2 300 milliards de dollars sont émis aux États-Unis et 1 850 milliards d'euros dans l'Union Européenne [54]. De plus, les taux directeurs sont abaissés autour de zéro pour stimuler le crédit, ce qui contribue à accroître la masse de monnaie scripturale disponible.

À cause de cette création monétaire démesurée, la menace d'une inflation élevée reparaît en Occident, alors même qu'elle avait disparu depuis des décennies. Ce risque pousse les gens à acheter du bitcoin, qui, en tant qu'actif indépendant de la création monétaire, prend tout son sens. En particulier, de grandes sociétés cotées en bourse aux États-Unis, ayant des réserves non négligeables en dollars, entrent dans la danse. Le 11 août 2020, l'entreprise Microstrategy, dirigée par Michael Saylor, annonce ainsi adopter le bitcoin comme principal actif de réserve et s'être procuré 21 454 BTC, pour un montant d'achat total de 250 millions de dollars. En octobre, Square, une entreprise américaine spécialisée dans le paiement mobile cofondée par Jack Dorsey, suit le mouvement et acquiert 4 709 bitcoins. En février 2021, le constructeur automobile de voitures électriques Tesla, dirigé par Elon Musk, annonce avoir acheté près de 43 000 BTC pour 1,5 milliards de dollars.

De ce fait, un nouvel engouement spéculatif apparaît et le prix du bitcoin s'envole à nouveau. Alors qu'il oscillait autour des 10 000 $ depuis 2019, il monte rapidement à l'automne 2020, pour dépasser son ancien sommet en

décembre et atteindre les 64 000 $ en avril 2021.

FIGURE 2.2 – Évolution du prix du BTC entre le 19 juillet 2010 et le 30 novembre 2023 (source : buybitcoinworldwide.com).

Mais cette tendance va plus loin que les entreprises et l'engouement atteint un petit État d'Amérique centrale : le Salvador. Cette croissance du prix attire en effet l'attention du jeune président, Nayib Bukele, qui décide de faire du bitcoin une monnaie ayant cours légal dans son pays, aux côtés du dollar étasunien. Le président est inspiré par Jack Mallers, le PDG énergique de Strike, ainsi que par l'expérience de Bitcoin Beach, un projet de développement d'une économie durable basée sur le bitcoin autour de la plage d'El Zonte, au sud de la capitale San Salvador.

La mesure imposant le cours légal est annoncée le 5 juin 2021 par Nayib Bukele dans une vidéo diffusée lors de la conférence *Bitcoin Miami 2021* et est mise en place le 7 septembre. Elle exige en particulier que les commerçants acceptent le bitcoin en tant que moyen de paiement et de règlement de dette, bien que des exceptions existent et que la loi ne soit pas strictement appliquée.

L'utilisation de Bitcoin apporte théoriquement de nombreux avantages pour la population : assurer la réception de fonds transférés depuis l'étranger, créer une culture de l'épargne, attirer des capitaux, rendre le pays plus attractif notamment au niveau du tourisme, apporter des opportunités à l'international,

créer un nouvel espoir dans une société rongée par la pauvreté, la criminalité et la corruption, etc. De plus, cette adoption permet au pays, qui repose exclusivement sur le dollar depuis l'abandon du colón en 2001, d'échapper partiellement au seigneuriage de la Réserve Fédérale des États-Unis, en accumulant du bitcoin dans ses réserves de changes. La banque centrale du Salvador se procure ainsi quelques centaines de bitcoins lors de l'entrée en vigueur du cours légal.

Cet évènement est applaudi par un certain nombre de bitcoineurs qui y voient une formidable opportunité et qui se rendent sur place dans les mois qui suivent. Entre autres, il a pour effet d'asseoir encore un peu plus la légitimité institutionnelle du bitcoin qui devient une devise protégée par un État. Cela coïncide avec le sommet de l'épisode spéculatif, qui amène le prix du bitcoin jusqu'aux 69 000 $ en novembre 2021.

Cependant, les avis ne sont pas unanimes et de nombreuses critiques sont émises, que ce soit à l'égard des pratiques autoritaires du président, de l'implémentation de Lightning (via l'application Chivo) ou bien de l'imposition du cours légal elle-même qui va à l'encontre de la philosophie de Bitcoin. Et comme la suite le montrera, l'expérience du Salvador est mitigée : l'adoption est loin d'être un succès, la population reste méfiante, et la chute du cours (divisé par trois en l'espace d'un an) décourage toute épargne à moyen terme.

D'une manière générale, Bitcoin acquiert tout de même au fil des années une légitimité certaine [55], ce qui pousse ses adversaires à profiter de son succès pour développer leurs propres projets.

C'est le cas des grandes sociétés avec l'initiative Libra, portée par Facebook et annoncée le 18 juin 2019. Il s'agit d'un projet d'une monnaie numérique adossée à un panier de devises et d'autres actifs, qui serait géré par un consortium d'une centaine d'entreprises provenant du monde financier traditionnel (comme Visa, Mastercard ou PayPal), de la sphère de la cryptomonnaie (comme Coinbase ou Xapo) ou du secteur technique en général (comme Iliad).

Cette annonce provoque une levée de boucliers, tant du côté du grand public, qui s'inquiète du potentiel de surveillance que représente ce système, que des États, qui craignent la perte de leur souveraineté monétaire. C'est donc tout naturellement que le projet est repoussé par les régulateurs du monde entier, à commencer par le Congrès américain. En décembre 2020, Libra prend le nom de Diem, devenant alors un projet de stablecoin adossé au dollar étasunien. Il finira par être définitivement abandonné en janvier 2022.

Les instances étatiques s'organisent aussi de leur côté en envisageant de

déployer leurs propres monnaies électroniques dont elles gèreraient l'émission et les transactions. Durant cette période, on assiste ainsi au début du développement des monnaies numériques de banque centrale (MNBC). L'idée, qui s'inspire directement du succès de Bitcoin et des stablecoins, se veut être une modernisation de la monnaie fiat traditionnelle, notamment dans le but de favoriser la fluidité des échanges et l'inclusion financière.

Ce type de monnaie pérenniserait les transferts numériques qui forment déjà l'essentiel des transactions dans les pays occidentaux. Mais elle offrirait également un levier de contrôle supplémentaire pour le pouvoir et, ce faisant, introduirait un danger inédit : celui d'une surveillance et d'une censure bancaire généralisées. Couplée à une disparition contrôlée de l'argent liquide, une telle monnaie pourrait de ce fait constituer la base d'un régime dystopique et totalitaire.

Les projets de MNBC mettent ainsi en exergue l'apport essentiel de Bitcoin : un outil de résistance à la censure permettant de rester libre dans un monde qui ne l'est pas. Le concept découvert par Satoshi Nakamoto en 2007, déjà très utile, pourrait donc devenir la solution à un problème qui ne serait que sur le point d'émerger.

Un déploiement fait de divisions

Bitcoin a donc évolué depuis ses premiers développements sur Mt. Gox et sur Silk Road. Durant son existence, il a été la source de nombreux clivages internes concernant la vision qu'il est censé incarner. Ces clivages ont donné lieu à des conflits qui ont profondément marqué l'histoire de la cryptomonnaie.

Tout d'abord, l'arrivée d'acteurs financiers dans l'écosystème a mis l'accent sur la résistance à l'inflation du bitcoin (21 millions) et sur son caractère déflationniste, aux dépens de sa résistance à la censure, ce qui a créé une opposition de principe entre les nouveaux investisseurs et les anciens cypherpunks. Puis, la guerre des blocs a divisé la communauté à partir de 2015 sur le rôle de la chaîne de blocs, entre les partisans d'un protocole destiné à effectuer des paiements et les défenseurs d'un protocole de règlement. Ensuite, l'émergence des cryptomonnaies alternatives (et notamment d'Ethereum) a fait naître un enthousiasme pluraliste, mais les pratiques douteuses qui accompagnaient le lancement des nouveaux projets ont donné naissance à un mouvement de rejet, le maximalisme du bitcoin. Enfin, une dernière opposition s'est faite au niveau de l'assimilation institutionnelle, entre d'une part les personnes désireuses de coopérer avec les autorités en charge et les régulateurs, et d'autre part celles

prônant la confrontation et dénigrant la soumission et la conformité.

Bitcoin est aujourd'hui pluriel et il est encore en proie à ces tensions de manière plus ou moins diffuse. Mais ce sont précisément ces tensions qui lui ont permis de devenir le système organique et antifragile qui a su se faire une place dans notre société. La découverte de Satoshi Nakamoto est en effet toujours vivante et continue, bloc après bloc, de servir ses utilisateurs.

3

Des racines monétaires

Bitcoin constitue un protocole de transfert de valeur qui gère l'émission et les échanges d'une unité de compte numérique du même nom, le bitcoin. Comme son nom l'indique (bitcoin est la fusion de *bit*, chiffre binaire, et de *coin*, pièce de monnaie), le bitcoin a vocation à être une monnaie. Il a ainsi été présenté comme tel dès ses débuts, comme l'atteste le titre du livre blanc qui en faisait « un système d'argent liquide électronique pair à pair ». C'est pourquoi il est nécessaire de comprendre l'économie et la monnaie afin de saisir correctement Bitcoin.

En particulier, le bitcoin est une nouvelle forme de monnaie. Il s'agit en effet d'une monnaie entièrement numérique qui se base sur un réseau décentralisé et qui ne nécessite pas d'autorité centrale pour fonctionner, ce qui constitue un véritable tour de force technique. Ce modèle original permet au bitcoin d'être résistant à la censure, dans le sens où il est difficile d'empêcher une transaction d'avoir lieu, et résistant à l'inflation, dans le sens où il est dur de créer de nouvelles unités. Grâce à cette proposition de valeur double, il représente une alternative viable au système monétaire et bancaire moderne.

Dans ce chapitre, nous nous proposons d'explorer les racines monétaires de Bitcoin, en expliquant d'abord ce qu'est la monnaie, en décrivant ensuite la conception qu'en a l'école autrichienne d'économie, avant de montrer en quoi le modèle du bitcoin est unique et où réside son utilité.

Qu'est-ce que la monnaie ?

La monnaie est un sujet ardu à appréhender et la conception que s'en font les gens est souvent floue et inexacte. Pourtant, il s'agit d'un instrument utilisé massivement dans nos sociétés modernes, caractérisées par la marchandisation et par la division du travail. Il est donc crucial d'appréhender cet objet de manière fine et pertinente.

L'importance concrète de la monnaie se retrouve dans la diversité des termes qui existent pour la désigner en français. D'abord, l'appellation la plus répandue pour parler de la monnaie est l'argent, si bien qu'on doit aujourd'hui préciser quand on veut parler du métal précieux. Ensuite, l'argot regorge de termes variés : le blé, en référence à la céréale ; l'oseille, désignant originellement une plante potagère ; le flouze, venant d'un mot arabe signifiant pièce de cuivre ; le pèze, qui viendrait peut-être du breton ; le pognon, qu'on échange de main à main ; la maille et le sou, qui sont les noms d'anciennes pièces de monnaie. Puis, pour sa forme liquide, on parle de numéraire ou d'espèces, ou bien de *cash*, un anglicisme venant de l'ancien français *casse*, qui a donné caisse. Enfin, il y a le mot « monnaie » lui-même, qui provient du latin *moneta*, issu du nom de temple de Juno Moneta (« Junon la Prévenante ») où se frappait la monnaie de Rome.

Une monnaie est un intermédiaire d'échange généralement accepté au sein d'un groupe de personnes donné. Il s'agit d'un outil utilisé dans l'échange indirect de biens et de services : une personne *vend* des biens et des services contre de la monnaie, qui lui sert ensuite à *acheter* d'autres biens et services.

La monnaie résout en cela le problème de la double coïncidence des besoins, qui se poserait dans une économie de troc où deux personnes doivent simultanément désirer le bien de l'autre dans la proportion souhaitée pour que l'échange puisse se faire d'une manière directe. Par exemple, si un boulanger souhaitait acquérir une pièce de viande contre quelques-unes de ses baguettes de pain, il devrait trouver un boucher désirant obtenir ces baguettes à cet endroit-là, à ce moment-là et pour ce montant-là. La monnaie est donc un bien intermédiaire que les gens acquièrent en vue de le céder contre autre chose, et qui fluidifie grandement leurs échanges.

Ce qui fait qu'un bien est utilisé comme monnaie plutôt qu'un autre, c'est ce qu'on appelle sa cessibilité [1], c'est-à-dire la facilité avec laquelle ce bien peut être échangé sur le marché dès que son détenteur le désire et en encourant le moins de perte de valeur possible. Le bien servant de monnaie doit pouvoir être obtenu facilement sans que cela ne provoque une pénurie de monnaie. Cette propriété est similaire à la liquidité d'un marché, qui représente la

capacité à acheter ou à vendre rapidement les biens qui y sont cotés sans que l'opération n'ait d'effet majeur sur les prix. C'est en ce sens qu'on décrit parfois la monnaie comme *le bien le plus liquide* au sein d'une économie donnée, et qu'on emploie le terme d'*argent liquide* en français pour parler de la monnaie physique composée des pièces et des billets, échangeables facilement et sans contrainte.

La monnaie n'est pas un concept dont les contours sont fixes et rigides. Un bien peut être plus ou moins une monnaie selon son niveau de cessibilité dans le groupe humain où il est échangé, de sorte qu'on peut parler de degré de monétarité ou de liquidité [2]. L'or et le bitcoin disposent ainsi d'un degré de monétarité moindre que les devises étatiques en général, mais cela ne les empêche pas d'être considérés comme des monnaies au sens large. L'or est même mondialement perçu comme la réserve de valeur par excellence et comme le fondement historique de la monnaie, ce qui se retrouve dans la culture et en particulier dans les jeux vidéos.

De plus, la cessibilité d'un bien peut varier selon la situation. Le dollar n'est pas forcément utile en Europe où l'euro est bien plus cessible. L'or est un piètre instrument pour les paiements quotidiens, mais constitue une bonne manière de déplacer de la valeur dans le temps. Le bitcoin est peu utilisé dans le commerce physique, mais l'est beaucoup plus sur Internet. Les cigarettes ne servent pas de monnaie dans la population générale mais ont pu l'être dans certaines prisons. Le statut de monnaie dépend aussi du contexte.

La cessibilité élevée nécessaire pour que le bien soit sélectionné comme monnaie se retrouve dans les trois fonctions monétaires classiques, souvent citées par les économistes et dont l'origine est attribuée au philosophe Aristote. Ces fonctions de la monnaie sont les suivantes : premièrement, c'est un moyen de paiement, permettant de régler des échanges de manière directe ou différée (dette) ; deuxièmement, c'est une réserve de valeur, permettant d'épargner de la richesse pour l'utiliser plus tard ; troisièmement, c'est une unité de compte, servant de moyen standard d'exprimer la valeur des autres biens, sous la forme de prix. Autrement dit, la monnaie doit posséder une cessibilité qui s'adapte à la fois à l'espace, au temps et à l'échelle.

De ces trois *fonctions* fondamentales, on dérive usuellement les *qualités* essentielles de la monnaie, qui sont :

— La portabilité : la monnaie doit être facilement transportable pour être transmise d'une personne à une autre, ou pour le dire autrement, le coût pour la déplacer doit être minimal ;

— La durabilité : elle doit se conserver dans le temps, ne pas s'altérer, ne

pas pourrir ;
— La rareté : sa disponibilité doit être restreinte et ne pas être modifiée ;
— La divisibilité : elle doit pouvoir être scindée en sous-parties plus petites ;
— La fongibilité : chaque unité doit être interchangeable avec une autre ;
— La vérifiabilité : la conformité de la monnaie doit pouvoir être vérifiée aisément et rapidement (les espèces doivent être « sonnantes et trébuchantes ») ;
— La résistance à la censure : il doit être difficile d'empêcher une transaction de se faire (ce qui peut être remis en cause dans les solutions numériques) ;
— L'historicité : la monnaie doit présenter une utilisation ancienne (et donc bénéficier de l'effet Lindy [3]).

Ces qualités se sont retrouvées, de manière partielle ou totale, dans les différentes monnaies qui ont émergé et se sont imposées au cours de l'histoire.

Les différentes monnaies

On peut regrouper les monnaies qui ont existé en différentes catégories. Cinq formes plus ou moins distinctes se dégagent ainsi : la monnaie-marchandise, la monnaie représentative, le papier-monnaie, la monnaie-crédit et la monnaie numérique. Ces formes ont toutes des qualités singulières, qui sont le résultat de l'évolution monétaire mondiale.

Une monnaie-marchandise est, comme son nom l'indique, une marchandise qui est amenée à servir d'intermédiaire d'échange au sein d'un groupe donné. Une marchandise, dans le sens où nous l'entendons ici [4], est un produit standardisé, essentiel et courant, dont les qualités sont parfaitement définies et connues des acheteurs, comme une matière minérale, un produit agricole ou un produit manufacturé. De ce fait, le bien utilisé possède originellement une utilité intrinsèque autre que monétaire : industrielle, alimentaire ou esthétique.

Les marchandises utilisées comme intermédiaire d'échange ont été nombreuses au cours de l'histoire de l'humanité. On a pu utiliser des restes d'animaux comme les coquillages et les ossements, des produits artisanaux comme les pagnes ou les couteaux, des denrées alimentaires comme le blé, les épices, les graines de cacao ou le sel [5], des produits de l'élevage dont notamment le gros bétail, ou des matières naturelles comme les pierres ou les métaux.

Toutes ces marchandises possédaient de plus ou moins bonnes qualités monétaires, mais certaines souffraient de gros défauts, ce qui les rendaient

moins adéquates à l'utilisation comme intermédiaire d'échange que d'autres. Le bétail avait une très mauvaise portabilité et n'était pas divisible. Les céréales comme le blé ou le riz étaient peu durables. La rareté des coquillages pouvait être élevée dans les terres, mais l'était peu près des côtes. Les produits artisanaux et les bijoux différaient légèrement les uns des autres ce qui nuisait à leur fongibilité.

De manière générale, ce sont les métaux précieux, et tout particulièrement l'or, l'argent et le cuivre (sous forme de bronze), qui ont été sélectionnés au fil du temps pour finir par devenir la base monétaire mondiale. Cette convergence peut s'expliquer par le fait que ces trois métaux (de symboles chimiques respectifs Au, Ag et Cu) appartiennent tous les trois au groupe 11 de la classification périodique des éléments et qu'ils possèdent par conséquent des propriétés chimiques similaires, dont notamment une grande résistance à la corrosion et à l'oxydation, et une malléabilité élevée. L'utilisation de métaux multiples s'explique par leur portabilité imparfaite : l'or permet de déplacer beaucoup de valeur, mais n'est pas adapté aux petits paiements quotidiens, contrairement à l'argent et au cuivre.

Les métaux précieux ont pu être utilisés à l'état brut, sous la forme de lingots plus ou moins gros. Cependant, ils ont surtout été frappés sous la forme de pièces de monnaie, sur lesquelles une institution de confiance (généralement un État) inscrivait sa marque et certifiait le poids et la teneur en métal. Cette inscription constituait entre autres choses un certificat, intégré à la monnaie, qui avait pour but de faciliter l'échange par la non-nécessité de procéder à une vérification à chaque paiement.

Cette certification peut également être déconnectée de la monnaie, auquel cas on parle de monnaie représentative. Une monnaie représentative est une monnaie constituée de certificats, imprimés ou numériques, qui sont convertibles à vue contre une marchandise de base, comme de l'or ou de l'argent, auprès d'un tiers de confiance. L'aspect central d'une telle monnaie est qu'elle est théoriquement adossée à une réserve intégrale de monnaie de base, détenue par une ou plusieurs institutions. Les certificats sont par essence des substituts monétaires, c'est-à-dire des créances juridiquement exécutoires sur un débiteur pour un montant de monnaie de base déterminé.

L'archétype de la monnaie représentative est le système de l'étalon-or classique, qui était en vigueur durant la Belle Époque dans le monde occidental, où la monnaie était constituée de pièces d'or et de billets de banque convertibles en or. Cependant, avec le temps, la convertibilité a été progressivement abandonnée et les billets ont été transformés en une simple monnaie fiduciaire

papier.

Une monnaie fiduciaire est une monnaie dont la valeur d'usage est négligeable par rapport à sa valeur nominale. La valeur initiale de la monnaie fiduciaire provient de la confiance (*fiducia* en latin) accordée à d'autres acteurs plutôt que de ses propriétés intrinsèques, comme c'est le cas des monnaies-marchandises. Cette confiance peut être placée dans un État, dans une firme ou bien dans une communauté. Elle se fonde non seulement sur la conviction que le dépositaire n'en dégradera pas les propriétés (dont notamment la rareté), mais aussi, dans le cas de l'État, sur l'assurance qu'il fera usage de la violence pour en contraindre l'utilisation, auquel cas on parle de monnaie fiat (du latin *fiat*, « qu'il soit fait », qui véhicule l'idée de décret). Contrairement à la monnaie représentative, la monnaie fiduciaire ne représente pas une marchandise ou une autre monnaie de base : *c'est* la monnaie de base.

L'exemple type de monnaie fiduciaire est le papier-monnaie, qui est une monnaie basée sur un support physique, dont la valeur d'usage est largement inférieure à la valeur nominale ou faciale indiquée sur le support. Le support peut être fabriqué à partir de papier, de tissu ou de plastique (billets) ou bien d'alliages de métaux composés par exemple de cuivre, de zinc et de nickel (pièces). Le maintien de sa valeur est garanti par la limitation de la production et la répression du faux-monnayage : sans cela, la monnaie deviendrait une monnaie-marchandise et la valeur d'échange des supports tendrait rapidement vers leur coût de production, généralement inférieur à leur valeur nominale.

Cette forme de monnaie a été expérimentée par les États à de multiples reprises au cours de l'histoire conduisant la plupart du temps à des inflations dramatiques, comme l'illustrent la tentative d'instauration d'une monnaie fiat par la dynastie Song entre le XI^e^ et le XII^e^ siècle en Chine ou l'épisode des assignats durant la Révolution française. Ce n'est que depuis le XX^e^ siècle et l'abandon de l'étalon-or que ce modèle s'est généralisé.

Une monnaie-crédit, aussi appelée monnaie scripturale, est une monnaie qui se rapporte à l'écriture (*scriptura* en latin) d'une dette dans un registre bancaire. Elle se distingue de la monnaie représentative par le fait qu'elle n'oblige pas le dépositaire à conserver le bien représenté en réserve. Les banques sont en effet des organismes de crédit, et pas des entrepôts de monnaie : lorsqu'une personne « dépose » des fonds sur un compte en banque, elle prêtent en réalité son argent à la banque qui « crédite » son compte en conséquence (d'où l'adage « les dépôts font les crédits »).

Tout comme la monnaie représentative, la monnaie-crédit est un substitut monétaire. La monnaie-crédit doit se fonder sur une unité de compte de base,

issue d'une monnaie-marchandise (comme l'or) ou d'une monnaie fiduciaire (comme le dollar), qui sert à régler la dette lorsqu'elle arrive à échéance.

Aujourd'hui, le crédit est largement monétisé dans les sociétés occidentales, comme l'illustrent les moyens de paiement modernes que sont les chèques, les virements et les cartes bancaires. La monnaie scripturale compose plus de 90 % de la quantité en circulation de la monnaie au sens large.

Une monnaie numérique est une forme particulière de monnaie fiduciaire dont l'existence repose sur un registre géré informatiquement. Elle se distingue de la monnaie scripturale par le fait que l'entrée dans le registre n'est pas une créance en monnaie sur un tiers, mais *est la monnaie*. La monnaie est ainsi stockée sur une mémoire électronique, d'où le fait qu'on parle parfois de monnaie électronique [6]. Une conséquence de la nature particulière de cette forme de monnaie est qu'elle est généralement programmable, dans le sens où on peut inscrire les conditions de dépense dans le système informatique qui la soutient.

Le premier exemple de monnaie numérique est celle qui est gérée de manière centralisée par une banque centrale. Elle constitue, avec les pièces et les billets, la base monétaire, qui est aussi appelée « monnaie de banque centrale » ou « monnaie centrale ». Plus précisément, il s'agit des avoirs monétaires détenus par les titulaires de comptes auprès de la banque centrale (c'est-à-dire des banques commerciales). Ce type de monnaie a permis de ne plus reposer uniquement sur des supports physiques, qui rendaient le règlement difficile et risqué. À l'avenir, la monnaie numérique étatique devrait être étendue à une monnaie numérique de banque centrale (MNBC) disponible pour les organismes financiers et, probablement, pour les particuliers.

Le second exemple de monnaie numérique est la cryptomonnaie, gérée de manière décentralisée par un réseau pair à pair, dont l'archétype est le bitcoin. Il s'agit d'une monnaie numérique de marché dans le sens où son existence n'est pas dépendante de l'intervention (ou de l'absence d'intervention) de l'État. C'est la monnaie sur laquelle se focalise cet ouvrage.

L'école autrichienne et la valeur de la monnaie

Puisque Bitcoin est un système monétaire, la compréhension de son fonctionnement et de ses enjeux passe par la connaissance de l'économie. Il existe de multiples manières d'aborder le sujet mais nous adoptons ici la perspective du courant économique dit « autrichien », qui est probablement la plus pertinente pour décrire Bitcoin, car elle a inspiré, au moins indirectement, sa

création et son développement.

L'école autrichienne d'économie, parfois aussi appelée école de Vienne, est une école de pensée économique créée en Autriche au XIXe siècle autour de la figure de Carl Menger. Elle s'est initialement développée dans ce pays d'Europe centrale avec des penseurs comme Eugen von Böhm-Bawerk et Friedrich von Wieser. Après la Première Guerre mondiale et le démantèlement de l'Autriche-Hongrie en 1918, elle s'est exportée à l'étranger, dont notamment aux États-Unis, avec des économistes d'origine autrichienne comme Ludwig von Mises et Friedrich Hayek (ce dernier ayant reçu le prix « Nobel » d'économie en 1974). Par la suite, elle s'est étendue à des penseurs de toutes origines, dont les principales figures sont Murray Rothbard, Jesús Huerta de Soto et Hans-Hermann Hoppe.

L'école autrichienne se caractérise par son approche méthodologique – l'individualisme méthodologique – qui se fonde sur la praxéologie, c'est-à-dire l'étude rationnelle de l'action humaine. Cette méthode est aprioriste (ou axiomatique) dans le sens où elle repose sur un certain nombre d'axiomes qui ont trait au comportement humain. Elle part donc de la partie (l'individu) pour en déduire des conséquences logiques sur le tout (l'économie). L'école autrichienne s'oppose de ce fait aux écoles de pensée économiques qui se basent essentiellement sur l'observation et qui cherchent à modéliser « mathématiquement » l'économie, comme le néokeynésianisme, aujourd'hui majoritaire.

L'école autrichienne a en particulier une analyse fine de la valeur, c'est-à-dire l'intérêt ou l'importance qu'une personne porte à une chose.

Plusieurs conceptions de l'origine de la valeur existent. Certains considèrent que la valeur provient de la terre et de l'activité s'y rapportant, une thèse défendue par les économistes physiocrates du XVIIIe siècle. D'autres postulent que la valeur tire son origine du travail, à l'instar d'Adam Smith, de David Ricardo, et surtout de Karl Marx, dont les partisans soutiennent cette théorie depuis le XIXe siècle.

L'école autrichienne d'économie diffère de ces conceptions en prônant une conception subjective de la valeur. Pour les autrichiens en effet, la valeur n'est pas un phénomène objectif et dépend du point de vue individuel. Selon Carl Menger :

> « La valeur n'est pas inhérente aux biens, elle n'en est pas une propriété, elle n'est pas une chose qui existe en soi. C'est un jugement que les sujets économiques portent sur l'importance des biens dont ils peuvent disposer pour maintenir leur vie et leur bien-être. Il en résulte que la valeur n'existe pas en dehors de la conscience des hommes [7]. »

Ainsi, un individu peut accorder une immense valeur à un bien (un tableau par exemple) tandis qu'un autre ne lui en accordera aucune. De même, la valeur prodiguée peut varier selon le contexte : une personne vivant dans le désert ne portera pas le même intérêt à un litre d'eau que quelqu'un résidant dans une région humide.

La valeur d'un même bien peut être différente aux yeux d'un individu selon sa consommation antérieure. S'il est affamé, il accordera une grande valeur à une pomme ; mais à mesure qu'il se sustentera, la valeur qu'il donnera aux pommes suivantes décroîtra. C'est ce qu'on appelle l'utilité marginale.

La valeur que l'individu tire d'un bien est appelée la « valeur d'usage » par les économistes. Le sens porté à ce terme est différent selon les personnes qui l'utilisent. Ainsi, il renvoie souvent à la valeur d'usage objective, qui est la relation entre une chose et l'effet qu'elle a la capacité d'entraîner, comme par exemple le pouvoir de chauffage du bois. Mais le terme peut également, dans le contexte autrichien, faire référence à la valeur d'usage subjective, qui n'est pas toujours fondée sur un critère objectif d'évaluation.

L'estimation de la valeur des biens et des services permet à l'individu de savoir comment orienter sa production et sa consommation. Mais cette appréciation intervient également dans le commerce : un échange a lieu seulement si les deux parties de cet échange donnent *plus de valeur* au bien économique possédé par autrui. De ce fait, si un bien appartenant à autrui vaut pour moi plus que quatre pièces d'argent et que cette autre personne accorde plus de valeur à deux pièces d'argent qu'à ce bien, alors un échange à un prix de trois pièces d'argent sera bénéfique pour nous deux. C'est pour cette raison qu'à long terme le marché libre *crée* de la richesse. Le prix ainsi obtenu dans le commerce est parfois appelé « valeur d'échange ».

Même si la valeur est subjective, cela n'empêche pas les êtres humains d'accorder de la valeur aux mêmes choses. D'abord, en tant qu'ils sont semblables, ils valorisent naturellement les biens qui leur permettent de satisfaire leurs besoins physiologiques primaires (eau potable, nourriture, vêtements, abris, etc.). Ensuite, ils ont tendance à copier le désir d'autrui pour des choses non nécessaires, conformément à la nature mimétique du désir, ce qui a pour effet de créer les engouements et les effets de mode autour d'objets communs. Enfin, ils accordent de la valeur aux biens d'ordre supérieur, que ce soient des outils (capital) ou des matières premières, qui permettent de fabriquer les biens de consommation désirés.

La monnaie est un cas particulier dans l'analyse de la valeur. Elle repose sur un phénomène intersubjectif : une construction psychologique qui se fait

au sein de chaque personne et qui se renforce à mesure qu'elle s'enracine dans l'esprit des autres. Chacun acquiert de la monnaie parce qu'il pense qu'il pourra l'échanger contre un autre bien plus tard, ce qui affermit la conviction des autres que la monnaie peut effectivement être utilisée. C'est un cercle vertueux conforme à l'effet de réseau.

De ce fait, même si la valeur est évaluée subjectivement, la valeur de la monnaie converge nécessairement vers une valeur d'échange objective commune à tous, qu'on appelle le pouvoir d'achat. Ce pouvoir d'achat peut varier selon la période et selon la localité, au gré des variations naturelles du marché et des distorsions causées par l'État. Lorsqu'il baisse durablement (ce qui se manifeste par une augmentation généralisée des prix), on parle d'inflation. Lorsqu'il augmente durablement (ce qui se traduit par une baisse généralisée des prix), on parle de déflation.

Au sein de la valorisation du bien utilisé comme monnaie, il est donc possible de distinguer deux valeurs mutuellement exclusives : sa valeur non monétaire, c'est-à-dire l'utilité alimentaire, industrielle, esthétique, etc. que la personne en retire ; et sa valeur strictement monétaire, qui découle de l'avantage provenant de l'utilisation du bien comme intermédiaire d'échange. Pour les monnaies-marchandises par exemple, on peut distinguer la demande dite « intrinsèque » de la demande monétaire : l'or ne tire pas sa valeur uniquement de sa demande esthétique (bijoux) et industrielle (microprocesseurs), mais aussi, et surtout, de sa demande en tant qu'intermédiaire d'échange, qui provient notamment des banques centrales.

Les économistes autrichiens minimisent le rôle de l'État dans la création de la monnaie, postulant qu'elle a largement émergé de l'échange économique, du moins en ce qui concerne sa forme la plus primitive. Ils s'opposent en cela aux chartalistes et aux partisans de la théorie monétaire moderne, qui affirment que la monnaie est née de l'intervention étatique et que sa valeur provient de son emploi pour le paiement de l'impôt [8]. Tel que l'écrivait Carl Menger :

> « L'origine de la monnaie (qu'il faut distinguer des pièces de monnaie, qui n'en sont qu'une variété) est [...] tout à fait naturelle, et elle n'est donc qu'en de très rares circonstances le résultat d'une influence de la législation. La monnaie n'est ni une invention de l'État, ni le produit d'un acte législatif, et la sanction d'un tel acte par l'autorité de l'État est donc étrangère à la notion même de monnaie [9]. »

Dans cette perspective, la monnaie tire son origine de l'échange entre les groupes d'individus qui ne se faisaient pas confiance, mais qui étaient désireux de coopérer. Ainsi les protomonnaies (ou paléomonnaies) ont émergé, non pas

au sein des tribus humaines, dont le fonctionnement interne reposait largement sur le don et le crédit, mais *entre* ces tribus. Cela pouvait concerner l'échange simple de marchandises, la résolution de conflits, le règlement de mariages et le paiement de tributs [10].

Avec la mondialisation progressive de la planète, les protomonnaies ont subi une sélection : beaucoup d'entre elles ont disparu au profit de celles qui satisfaisaient les propriétés d'une bonne monnaie. En particulier, le bien sélectionné devait être facile à cacher (résistance à la censure), difficile à produire (rareté) et sa valeur devait pouvoir être aisément approximée (vérifiabilité). La monnaie a convergé vers les pièces de métal précieux, le plus souvent d'or et d'argent, de préférence frappées par une autorité reconnue. Les premières pièces frappées sont vraisemblablement apparues au VII^e^ siècle avant Jésus-Christ en Asie Mineure sous l'impulsion des Lydiens, et étaient constituées d'électrum, un alliage naturel d'or et d'argent. Par la suite, de nombreuses pièces différentes se sont succédées : la darique perse, la drachme grecque, le denarius romain, le solidus byzantin (besant), etc.

L'utilisation de pièces s'est faite pendant des siècles et s'est généralisée à la planète entière. Néanmoins, cet usage a progressivement reculé à partir de la Renaissance avec l'émergence des billets de banque, qui se sont généralisés au cours du XIX^e^ siècle grâce à l'action des États. Le passage au papier-monnaie fiduciaire a eu lieu durant le XX^e^ siècle avec l'abandon total de toute référence aux métaux précieux dans le système monétaire en 1971. Nous avons assisté à une véritable corruption de la monnaie, qui a apporté quelques bénéfices mais qui a surtout permis aux autorités de davantage profiter de la création monétaire par le biais de la fameuse « planche à billets ».

Pour les partisans de la liberté, il est crucial de procéder à une rédemption de la monnaie [11], en revenant à ce que les économistes autrichiens appellent une monnaie saine. Une monnaie saine est une monnaie librement choisie par le marché qui reste à l'abri des ingérences coercitives. Tel que l'écrivait Ludwig von Mises dans sa *Théorie de la monnaie et du crédit* en 1912 :

> « Le principe de la monnaie saine comporte deux aspects. Il est positif en ce qu'il approuve le choix par le marché d'un intermédiaire d'échange couramment utilisé. Il est négatif en ce qu'il fait obstacle à la propension du gouvernement à s'immiscer dans le système monétaire [12]. »

Plusieurs projets politiques ont émergé dans le but de rétablir un système monétaire mondial basé sur une monnaie saine. Le premier était celui de Mises (et de Rothbard) visant à restaurer l'étalon-or. En effet, pour Mises, « une monnaie saine signifie un étalon métallique » et l'étalon-or « rend la

détermination du pouvoir d'achat de l'unité monétaire indépendante des États et des partis politiques ».

Le second projet était celui de Friedrich Hayek, développé plus tard, qui prônait une concurrence de monnaies (représentatives ou fiduciaires) qui seraient émises par des banques privées [13]. Cela a inspiré le modèle de la banque libre, dans lequel les organismes financiers pourraient agir librement sans intervention d'une banque centrale ou d'une autre instance, un modèle notamment soutenu par les économistes Lawrence White, George Selgin et Kevin Dowd.

Aucun de ces deux projets politiques n'a jamais abouti, malgré des décennies d'évènements démontrant la validité des thèses autrichiennes. Comme l'a montré l'histoire, le contrôle étatique sur la monnaie s'est progressivement étendu jusqu'à devenir ce qu'il est aujourd'hui, un contrôle tendant vers le totalitarisme. Cependant, il existe une alternative, une solution non pas politique, mais économique : Bitcoin.

Une nouvelle forme de monnaie

Si l'on parle autant de Bitcoin, c'est qu'il apporte quelque chose de nouveau, non seulement d'un point de vue technique, mais aussi et surtout dans une perspective économique. La découverte de ce système par Satoshi Nakamoto en 2008 représente en effet un véritable bouleversement dans le domaine monétaire. Le bitcoin constitue une forme de monnaie inédite : une monnaie *sui generis* (pour reprendre l'expression de Jacques Favier), de son propre genre, qu'il est difficile de placer dans les cases existantes.

Premièrement, il s'agit comme on l'a évoqué d'une monnaie entièrement numérique. Le bitcoin se base sur un registre de propriété public (la chaîne de blocs) qui définit la monnaie : les entrées de ce registre ne correspondent pas à des créances, comme c'est le cas pour la monnaie-crédit, mais à la monnaie elle-même.

Deuxièmement, cette monnaie numérique innove par le fait qu'elle ne nécessite pas de tiers de confiance pour fonctionner. Le contenu du registre ne dépend pas d'une institution financière comme une banque centrale, mais d'un ensemble d'acteurs agissant par le biais d'un réseau distribué d'ordinateurs.

Troisièmement, sa sécurité est assurée de manière économique : elle ne repose pas sur un bénévolat altruiste (même s'il joue évidemment un rôle), mais sur les incitations économiques des différents acteurs impliqués. Cela donne au système une stabilité à long terme dont n'ont jamais disposé les

différentes monnaies privées qui l'ont précédé.

Ces propriétés permettent au bitcoin de constituer une monnaie fiduciaire distribuée, dans le sens où il ne possède pas d'utilisation non monétaire significative et où sa valeur provient de la confiance accordée à une économie de commerçants plutôt qu'à un tiers. On peut également le qualifier de monnaie réticulaire (du latin *reticulum*, « filet à petites mailles », « réseau ») dans la mesure où la confiance est répartie sur le réseau des nœuds des commerçants plutôt qu'être concentrée sur un serveur central.

Bien que le bitcoin semble se rapprocher par ses caractéristiques des monnaies-marchandises [14], il ne s'agit aucunement d'une marchandise. Les propriétés de Bitcoin émergent d'un accord atteint par l'ensemble de ses utilisateurs, pas de caractéristiques intrinsèques du monde physique comme c'est le cas pour l'or ou l'argent. Il est ainsi possible de modifier les règles de consensus du système, même si un tel changement est très difficile.

En réalité, une monnaie est toujours un accord concernant un intermédiaire mutuellement acceptable dans le commerce. Dans le cas de la monnaie-marchandise, cet accord converge naturellement vers une denrée qui est déjà échangée au sein de la société. Dans le cas de la monnaie fiat, l'agrément est maintenu par un décret étatique disposant du respect de la population. Dans le cas de Bitcoin, la coordination est réalisée de manière volontaire autour de règles de consensus spécifiques.

C'est l'étendue de cet accord qui donne sa force à la monnaie, par effet de réseau : son utilité augmente en effet de manière superlinéaire par rapport à la taille de l'économie l'utilisant. C'est ce qui fait qu'une monnaie peut difficilement être remplacée par une autre, et c'est aussi ce qui rend difficile l'altération des règles de consensus du système, comme nous le verrons dans le chapitre 11 sur la détermination du protocole.

L'avantage premier de la monnaie-marchandise n'est pas de disposer d'une valeur intrinsèque, mais d'exiger un coût infalsifiable pour sa production, de façon à éviter qu'une création monétaire excessive ne détruise son pouvoir d'achat. En effet, dans le cas d'une monnaie fiduciaire étatique ou privée, la détermination de la monnaie se trouve entièrement entre les mains de l'émetteur, qui peut bénéficier de la situation en créant plus d'unités à son avantage, surtout s'il jouit d'un privilège légal.

Bitcoin est différent et n'est pas soumis à un tel risque : son fonctionnement distribué répartit sa détermination dans l'économie et l'empêche d'être soumis à l'arbitraire d'un tiers. Cette particularité lui permet de disposer d'une caractéristique inédite : une rareté absolue, découlant d'une quantité fixe d'unités

émises selon un programme prédéfini. C'est d'ailleurs l'un des facteurs qui ont construit sa renommée : le fait que l'offre monétaire soit limitée à 21 millions de bitcoins.

La « valeur intrinsèque » n'est donc pas un élément essentiel à la qualité de la monnaie. Le bitcoin, qui est une forme pure de monnaie, valorisée quasi exclusivement pour son rôle de monnaie, en est la preuve. Avec les monnaies-marchandises, les propriétés physiques de la monnaie constituaient un garde-fou contre les interventions privées et étatiques ; dans Bitcoin, c'est le réseau qui possède cette fonction.

Bitcoin et le théorème de régression

Certains économistes autrichiens refusent d'admettre que le bitcoin ait pu émerger sans avoir de valeur d'usage objective. Ils font pour cela référence au théorème de régression de Ludwig von Mises, qui stipule que la valeur d'échange de la monnaie est calculée par rapport à sa valeur précédente et doit, par régression, être ramenée à sa valeur en tant que marchandise.

L'essentiel de ce théorème se trouve dans la *Théorie de la monnaie et du crédit*, un ouvrage publié en 1912, où Mises écrit :

> « La théorie de la valeur de la monnaie en tant que telle peut faire remonter la valeur d'échange objective seulement jusqu'au point où elle cesse d'être la valeur de la monnaie et devient uniquement la valeur d'une marchandise. À ce point, la théorie doit laisser cours pour toute investigation ultérieure à la théorie générale de la valeur, qui n'a alors plus aucune difficulté à résoudre le problème. Il est vrai que l'évaluation subjective de la monnaie présuppose une valeur d'échange objective existante, mais la valeur qui a besoin d'être présupposée n'est pas la même que la valeur qu'il faut expliquer. Ce qui est présupposé est la valeur d'échange d'*hier* et il est parfaitement légitime de l'utiliser pour expliquer celle d'aujourd'hui. La valeur d'échange objective de la monnaie qui s'établit sur le marché d'aujourd'hui découle de celle d'hier sous l'influence des évaluations subjectives des individus fréquentant le marché, tout comme celle d'hier découlait à son tour, sous l'influence des évaluations subjectives, de la valeur d'échange objective de la monnaie d'avant-hier.
>
> Si de cette façon nous retournons de façon continuelle en arrière, nous devons arriver à un point où nous ne trouvons plus aucune composante dans la valeur d'échange objective qui provienne des évaluations basées sur la fonction de la monnaie comme moyen d'échange commun ; un point où la valeur de la monnaie n'est rien d'autre que la valeur de l'objet qui est utile d'une autre façon que comme monnaie [15]. »

Le théorème comporte deux éléments : la régression et la première valorisation.

Concernant la régression, le raisonnement se tient : la valeur attribuée à la monnaie se base sur sa valeur précédente, de sorte qu'on peut remonter à une valeur entièrement non monétaire. Il n'y a pas besoin que cette première valeur se maintienne : une fois que la monnaie a été établie, sa valorisation peut reposer uniquement sur la mémoire des prix précédents.

Cette régression se vérifie historiquement. La valeur de nos billets fiduciaires actuels en Occident peut être retracée de proche en proche jusqu'à la valeur des billets en tant certificats or, qui est issue de la valeur des pièces de monnaies, qui provient elle-même de la valeur de l'or sous forme brute. Cet or a été valorisé premièrement pour des motifs ornementaux et religieux avant de commencer à servir d'intermédiaire d'échange.

Concernant la première valorisation, ce qu'affirme Ludwig von Mises est plus inexact. Il parle d'une « marchandise » (*commodity* en anglais, *Ware* en allemand) qui est initialement valorisée pour son utilité « industrielle [16] » (*industrial* en anglais, *industriell* en allemand), donc d'un produit standardisé et courant dont les qualités sont définies et connues. À un autre endroit, il s'oppose explicitement à la théorie lockéenne de l'origine de la monnaie qui, selon ses termes, fait « découler l'origine de la monnaie d'un accord général qui aurait attribué des valeurs fictives à des choses intrinsèquement sans valeur [17] ». Il semble ainsi que Mises exclut qu'un bien intangible sans valeur d'usage objective puisse devenir un intermédiaire d'échange sans être adossé à une monnaie précédente.

Pourtant c'est exactement ce qui s'est passé avec le bitcoin, dont le succès constitue un contre-exemple limpide au théorème de régression dans son acception la plus stricte. L'erreur de Mises semble venir de son biais en faveur des métaux précieux lié à la période durant laquelle il écrivait, c'est-à-dire le début du XX^e^ siècle. Il était en effet difficile d'imaginer un système monétaire aussi fantaisiste que Bitcoin, des décennies avant la révolution technique de l'ordinateur personnel et d'Internet. Comme l'expliquait Satoshi Nakamoto en août 2010 :

> « Je pense que les critères traditionnels de la monnaie ont été décrits en partant du principe qu'il y avait tellement d'objets rares en concurrence dans le monde, qu'un objet bénéficiant de l'amorce automatique d'une valeur intrinsèque l'emporterait sûrement sur ceux sans valeur intrinsèque. Mais s'il n'y avait dans le monde rien qui ait de valeur intrinsèque et qui puisse être utilisé comme monnaie, s'il y avait seulement des objets rares mais sans valeur intrinsèque, je pense que les gens opteraient quand même pour quelque chose [18]. »

Toutefois, malgré cette conception erronée, le théorème de régression reste valide dans une acception plus large. Pour pouvoir servir d'intermédiaire d'échange, toute monnaie a dû *nécessairement* posséder en premier lieu une valeur d'usage non monétaire. Il a par conséquent fallu que quelqu'un donne une valeur au bitcoin « pour une raison ou pour une autre [19] » avant qu'une utilisation monétaire, comme par exemple « transférer de la richesse sur une longue distance », devienne possible.

Il existait donc un problème d'amorçage. Le cryptographe Hal Finney, qui avait expérimenté les systèmes d'argent liquide numérique au début des années 1990, en était notamment conscient. Dès les débuts de Bitcoin en janvier 2009, il écrivait :

> « Un des problèmes immédiats avec n'importe quelle nouvelle monnaie est de savoir comment lui donner une valeur. Même en ignorant le problème pratique lié au fait que quasi personne ne l'acceptera au début, il est toujours difficile de trouver un argument raisonnable justifiant l'attribution d'une valeur non nulle pour les pièces [20]. »

Mais cet amorçage a fini par avoir lieu.

L'émergence de la valeur du bitcoin

Selon le théorème de régression, le bitcoin a dû posséder une valeur d'usage non monétaire (objective ou subjective) avant d'être valorisé en tant qu'intermédiaire d'échange. Au cours des années, différentes hypothèses de première valorisation ont été proposées pour expliquer l'émergence de la valeur du bitcoin sur le marché. Examinons-en les principales, en commençant par les moins plausibles pour finir par les plus vraisemblables.

Tout d'abord, une hypothèse malheureusement trop souvent citée est la valeur qui découlerait de l'énergie utilisée pour sa production. Cette hypothèse provient notamment sur l'estimation de NewLibertyStandard, qui, à partir d'octobre 2009, vendait et achetait des bitcoins à un taux basé sur le coût énergétique de sa production personnelle. Il s'agit essentiellement d'une version revisitée de la théorie de la valeur-travail des marxistes. Cette explication était déjà critiquée par Satoshi Nakamoto en février 2010, qui écrivait que le coût de production était une conséquence du prix, et non pas une cause :

> « En l'absence d'un marché pour établir le prix, l'estimation de NewLibertyStandard basée sur le coût de production est une bonne estimation et un service utile (merci). Le prix de toute marchandise tend à graviter vers le coût de production. Si le prix est inférieur au coût, alors la production ralentit. Si le prix

> est supérieur au coût, il est possible de réaliser des bénéfices en produisant et en vendant davantage. Dans le même temps, l'augmentation de la production accroîtrait la difficulté, poussant le coût de production vers le prix [21]. »

Certaines personnes ont également suggéré que la valeur proviendrait du fait que le bitcoin a été échangé contre du dollar, avançant l'idée que la régression se transmettrait avec cette conversion. Cependant, le change avec le dollar a toujours été réalisé à taux variable, selon l'offre et la demande, sans aucune entité pour garantir un taux fixe. De ce fait, cette hypothèse ne peut pas être valide.

Une autre hypothèse de première valorisation évoquée est celle qui fait résider la valeur initiale du bitcoin dans sa capacité à être un système de paiement. Mais cet argument doit être écarté car il est circulaire : nul ne peut payer en bitcoins si ce dernier n'a de valeur pour personne. De plus, même si le réseau avait permis de traiter des transferts en dollars ou en euros, les paiements réalisés n'auraient pas été sécurisés du tout, en raison du caractère économique de la sécurité minière de Bitcoin, que nous décrirons dans le chapitre 8.

Une hypothèse apparentée est que des individus auraient attribué de la valeur au bitcoin pour sa capacité à servir pour l'horodatage, c'est-à-dire l'association d'une date et d'une heure à une information spécifique. Bitcoin permet en effet d'écrire des données arbitraires sur sa chaîne de blocs, ce qui garantit leur authenticité notariale, et on peut par exemple publier l'empreinte d'un document dans une transaction pour montrer que ce document existait antérieurement à la date de confirmation de la transaction. Néanmoins, pour que cet ancrage sur la chaîne possède une quelconque utilité, il faut qu'il soit difficile de modifier le registre. Puisque la sécurité de Bitcoin est essentiellement économique, cet usage ne peut donc pas avoir permis de première valorisation. De plus, cela ne s'est pas passé d'une telle manière : si on met de côté le message contenu dans le premier bloc (ayant pour but d'empêcher l'antidatage du lancement), aucune donnée arbitraire n'a été inscrite sur la chaîne avant 2011.

S'il faut chercher des raisons à la première valorisation du bitcoin, on doit les trouver dans les préférences strictement subjectives de l'individu, non pas dans une hypothétique valeur d'usage objective. Au vu de l'histoire de Bitcoin durant ses premières années d'existence, on peut observer qu'il a existé deux raisons principales derrière une telle valorisation : la dimension culturelle et l'aspect spéculatif.

La première raison derrière la valorisation initiale est la motivation cultu-

relle. Selon cette hypothèse, le bitcoin a été un objet de collection, représentant les principes en lesquels croyaient les individus qui lui ont porté de l'intérêt. C'est ce qui a poussé les gens à s'en procurer alors même qu'ils n'en avaient aucun avantage matériel à en retirer. Cela rejoint en un sens l'idée de valorisation en tant que système de paiement, à une nuance près : l'individu ne donne pas de la valeur au bitcoin parce que le système est un bon système de paiement à un instant précis, mais parce qu'il souhaite que ce projet réussisse.

Dans cette logique, l'économiste autrichien Konrad S. Graf parlait en 2013 de « composantes de la valeur de consommation directe » qui seraient « psychologiques ou sociologiques dans le sens où elles se rapportent à des facteurs tels que l'attrait inhérent pour les geeks, le défi professionnel lancé aux spécialistes, la curiosité et le signal d'appartenance [22] ». Dans le même ordre d'idées, Ross Ulbricht, le créateur de la place de marché Silk Road, expliquait dans un essai rédigé en 2019 :

> « C'est comme par magie que le bitcoin a pu en quelque sorte provenir de rien et, sans valeur préalable ni décret autoritaire, devenir une monnaie. Mais Bitcoin n'a pas émergé du vide. C'était la solution à un problème sur lequel les cryptographes butaient depuis de nombreuses années : Comment créer une monnaie numérique sans autorité centrale qui ne puisse pas être contrefaite et qui soit digne de confiance.
>
> Ce problème a persisté si longtemps que certains ont laissé sa résolution aux autres et ont rêvé à la place de ce que serait notre avenir si la monnaie numérique décentralisée devenait réalité d'une manière ou d'une autre. Ils rêvaient d'un avenir où le pouvoir économique du monde serait accessible à tous, où la valeur pourrait être transférée n'importe où en appuyant sur un bouton. Ils rêvaient de prospérité et de liberté, qui ne dépendraient uniquement que des mathématiques du chiffrement fort [23]. »

C'est donc le rêve d'une monnaie numérique libre qui a en partie motivé la valorisation initiale du bitcoin. L'objectif était, dès le début, de créer une monnaie, et le bitcoin a été valorisé pour cette propension.

Bitcoin était notamment conforme à l'idéal libertarien étasunien, représenté à l'époque par l'homme politique Ron Paul, qui proposait notamment d'« abolir la Fed » et qui a brigué l'investiture républicaine pour l'élection présidentielle de 2008 puis celle de 2012. Les cypherpunks, majoritairement originaires des États-Unis, se rapprochaient largement de cette idéologie. Satoshi lui-même était conscient de cette proximité, déclarant dès novembre 2008 que le concept de Bitcoin était « très attrayant pour le point de vue libertarien [24] ». C'est donc tout naturellement que les premières personnes à

apporter de la valeur au bitcoin ont été ces libertariens, à l'instar de Martti Malmi, de NewLibertyStandard ou, plus tard, de Ross Ulbricht.

La deuxième raison derrière la première valorisation du bitcoin est la valeur spéculative qui provenait de sa potentielle utilisation en tant que monnaie. La promesse de Bitcoin faisait qu'il pouvait être intelligent de parier là-dessus. En particulier, le bitcoin devait devenir au fil du temps une monnaie à quantité fixe (21 millions), dont la rareté était absolue.

Cette caractéristique unique a bouleversé l'imagination des gens. S'il y avait un nombre limité de bitcoins et que l'utilité monétaire du réseau augmentait, alors leur prix unitaire subirait théoriquement une forte hausse. C'est sur quoi se sont basées les engouements spéculatifs successifs qui ont jalonné l'histoire de la cryptomonnaie.

Cette idée est apparue en janvier 2009, lorsque Hal Finney a estimé dans un courriel que le prix unitaire du bitcoin pourrait atteindre la coquette somme de 10 millions de dollars :

> « En guise d'expérience de pensée amusante, imaginons que Bitcoin soit un succès et devienne le système de paiement dominant utilisé dans le monde entier. Alors, la valeur totale de la monnaie devrait être égale à la valeur totale de toutes les richesses du monde. Les estimations actuelles de la richesse totale des ménages dans le monde que j'ai trouvées varient entre 100 et 300 milliers de milliards de dollars. Pour un nombre de pièces de 20 millions, cette prévision donnerait à chaque pièce une valeur d'environ 10 millions de dollars [25]. »

Cette estimation était plus que contestable (la monnaie n'est pas censée représenter toute la richesse du monde), mais elle portait en elle la notion que chacun pouvait profiter de la hausse du cours.

Par la suite, Satoshi a lui-même utilisé cette logique pour attirer les utilisateurs potentiels. Il déclarait ainsi le 16 janvier qu'« il pourrait être judicieux de s'en procurer au cas où le phénomène prendrait de l'ampleur » et que « si suffisamment de gens [pensaient] la même chose, on [pourrait] assister à une prophétie autoréalisatrice [26] ». Le 18 février, il écrivait qu'« à mesure que le nombre d'utilisateurs [croissait], la valeur par pièce [augmentait] » et que cela pouvait « attirer davantage d'utilisateurs », ce qui constituerait une « boucle de rétroaction positive [27] » pour le système.

Ainsi, ce sont ces deux raisons – culturelle et spéculative – qui ont principalement contribué à la première valorisation du bitcoin. Si les premiers mineurs ont daigné utiliser leur ordinateur et dépenser de l'énergie, c'est parce que l'idée de Bitcoin correspondait à leurs valeurs morales et qu'ils avaient « le sentiment d'apporter une contribution bénéfique au monde [28] »

ou bien parce qu'ils entrevoyaient le potentiel profit [29]. Les personnes prêtes à accepter du bitcoin contre quelque chose d'autre l'ont fait pour les mêmes raisons. NewLibertyStandard, qui a été le premier individu à accepter d'échanger des dollars contre des bitcoins en octobre 2009, était notamment convaincu que Bitcoin était « une révolution économique » et « la référence de la monnaie numérique [30] ».

Comme l'a écrit un internaute anonyme en 2012, « les premiers adeptes de Bitcoin étaient le genre de personnes (du fait de leur intérêt pour les crypto-monnaies) à considérer Bitcoin comme quelque chose de beau [31] ». Et c'est cette beauté qui a été à l'origine de la réalité monétaire qu'on connaît aujourd'hui.

La monnaie de la désobéissance

Quand on présente Bitcoin, la question de sa proposition de valeur se pose immédiatement. Pourquoi Bitcoin ? Qu'est-ce qui le démarque des monnaies étatiques qui sont ses principales concurrentes ? Quel est l'intérêt d'utiliser le bitcoin comme monnaie, et pas le dollar ou l'euro ?

Car le bitcoin est, de par son aspect décentralisé et libre, une moins bonne monnaie que le dollar ou l'euro dans de nombreux cas : il est largement moins accepté, son utilisation est plus difficile, il implique de payer des frais de transaction, son pouvoir d'achat fluctue davantage et il pose plus de risques légaux. Toutes ces raisons font que les monnaies fiat et les solutions centralisées sont (et resteront) plus efficaces que Bitcoin dans la grande majorité des situations.

Cela ne veut pas dire que Bitcoin est inutile, mais seulement qu'il doit être appréhendé d'un point de vue particulier. Bitcoin est un système de monnaie « sans permission », *permissionless*, qui peut être utilisé sans avoir à demander l'autorisation de qui que ce soit. C'est un argent liquide électronique permettant l'échange direct et confidentiel entre particuliers, sans avoir recours à un intermédiaire. Il offre la possibilité d'exercer un contrôle total sur ses unités et de réaliser des transferts sans crainte d'être observé ou censuré, vers n'importe quel destinataire, n'importe où dans le monde et à n'importe quel moment.

Sa proposition de valeur découle de ces simples caractéristiques. En étant pour ainsi dire incontrôlable, Bitcoin constitue un instrument de *désobéissance* aux normes sociales et, surtout, au pouvoir politique. En particulier, il retire aux banques et aux États leur pouvoir de contrôle et de sélection des tran-

sactions, qui leur permet de superviser l'activité économique, ainsi que celui sur l'émission monétaire, qui leur permet de tirer un revenu de seigneuriage. Bitcoin constitue donc un concept de monnaie résistante à la censure, dans le sens où il est difficile d'empêcher une transaction, et résistante à l'inflation, dans le sens où il est difficile de créer plus d'unités qu'initialement prévues.

Bitcoin se construit en opposition aux autorités en charge, et s'inscrit dans la lutte ancienne contre l'asservissement des hommes. Par son existence, il affirme la primauté du droit naturel sur la loi positive, la supériorité de la propriété individuelle par rapport à la collectivité. Il s'intègre par là dans la tradition libérale du droit de résistance (*jus resistendi*), justifiant la sécession d'un individu ou d'un groupe d'individus face aux lois injustes, droit reconnu par deux grandes révolutions du XVIII^e^ siècle, qu'ont été la révolution américaine et la révolution française.

Il est un outil de désobéissance civile, conception ébauchée par Étienne de La Boétie au XVI^e^ siècle, théorisée par Henry David Thoreau en 1849 et mise en pratique par Gandhi dans sa démarche du *satyāgraha* en Inde et par Martin Luther King dans le cadre du mouvement des droits civiques contre la ségrégation raciale aux États-Unis. Il est un message envoyé au souverain terrestre, refusant ses décrets et affirmant : « Je n'utiliserai plus votre monnaie. »

Bitcoin a été créé en vue de gagner en indépendance individuelle. Bitcoin est issu du mouvement cypherpunk, un mouvement de désobéissance technique prônant l'utilisation proactive de la cryptographie sur Internet afin de protéger la confidentialité et la liberté. Lorsque Satoshi Nakamoto a lancé le réseau, il l'a fait sans demander l'autorisation au pouvoir en place, dans le but explicite d'accroître la liberté. Le 6 novembre 2008, en réponse à une personne qui lui disait qu'il ne « [trouverait] pas de solution aux problèmes politiques dans la cryptographie », il déclarait ainsi :

> « Oui, mais nous pouvons remporter une bataille majeure dans la course aux armements et conquérir un nouveau territoire de liberté pour plusieurs années [32]. »

De ce fait, il est naturel que le noyau dur de l'activité construite sur Bitcoin se situe à la marge de ce qui est généralement approuvé par le grand public. Bitcoin implique de reprendre sa souveraineté individuelle contre l'autorité, une démarche qui peut être impopulaire quand les lois émanent d'une acceptation majoritaire. Il sert donc à combler une niche de marché plus ou moins grande, dont la taille évolue selon la proportion de la population qui est prête à désobéir.

Parmi les utilisations centrales de Bitcoin, il y a notamment l'opposition

politique. En effet, ce dernier peut constituer un moyen alternatif de financement (réception) et de paiement (envoi) pour les organisations politiques, souvent classifiées à l'extrême-droite ou à l'extrême-gauche, dont l'intégrité financière est mise à mal par le pouvoir.

L'exemple de Julian Assange et de WikiLeaks est particulièrement illustratif. En effet, suite aux révélations publiées en 2010 sur les pratiques de l'armée étasunienne en Afghanistan et en Irak, l'organisation a subi un blocus financier de la part de Mastercard, Visa, Western Union, Bank of America et d'autres, qui a fait disparaître 95 % de ses revenus [33]. Cet épisode l'a poussé à accepter les dons en bitcoins en juin 2011 qui, à défaut d'être substantiels sur le moment, le sont devenus avec la hausse du cours quelques années plus tard.

On peut également citer le cas du lanceur d'alerte Edward Snowden, l'ancien employé de la CIA et de la NSA, qui a révélé en 2013 l'existence d'une surveillance de masse par la NSA d'Internet et du réseau téléphonique aux États-Unis. Celui-ci est depuis poursuivi par les États-Unis pour « espionnage, vol et utilisation illégale de biens gouvernementaux » et s'est exilé en Russie, dont il a acquis la nationalité en 2022. Snowden est un soutien solide de Bitcoin, en ayant fait usage en 2013 pour payer les serveurs qui ont servi à partager les informations de manière anonyme [34]. Il a également fait la promotion de la cryptomonnaie ZCash pour son modèle de confidentialité, dont il a participé à la cérémonie d'initialisation en 2016.

Un troisième exemple est celui d'Alexeï Navalny, le principal opposant à Vladimir Poutine en Russie, fondateur de la Fondation anti-corruption (FBK) dont les comptes en banques se sont faits geler en 2019 avant qu'elle soit liquidée en 2021. L'activiste a notamment utilisé Bitcoin pour se financer depuis 2017 et l'équivalent de plusieurs millions de dollars ont transité par son adresse [35]. Selon son bras droit, Leonid Volkov, cet apport en bitcoins aurait représenté 10 % de leur financement total. Navalny a été incarcéré en Russie en janvier 2021 et l'était toujours en novembre 2023 [36].

Une autre utilisation de Bitcoin se situant aussi dans la démarche de désobéissance est le financement de la plateforme de partage d'articles scientifiques Sci-Hub, fondée en 2011 par Alexandra Elbakyan, une jeune femme kazakhe inspirée par les idéaux communistes. Le but du site (toujours en ligne) est de fournir un libre accès au savoir, par la partage gratuit d'articles et d'œuvres en tous genres, au mépris des lois sur le droit d'auteur. En raison de son caractère illégal, la plateforme a accepté les donations en bitcoins dès ses débuts et a reçu des centaines de milliers de dollars par ce moyen [37]. Elle a également eu des soucis récurrents avec PayPal, sa seule autre source de revenu, qui a

clôturé définitivement son compte en 2020.

De manière plus large, Bitcoin est utile dans le contexte géopolitique. Le système n'est pas lié à une juridiction particulière et n'est pas concerné par la notion de frontière. Il permet par conséquent d'envoyer des fonds à l'étranger en échappant aux diverses contraintes et réglementations en vigueur.

C'est pourquoi il peut servir aux personnes émigrées pour envoyer de l'argent à leurs proches restés dans leur pays d'origine. Ces transferts monétaires, appelés *remittances* en anglais, reposent en effet généralement sur des solutions centralisées comme Western Union et MoneyGram, qui facturent souvent des frais élevés pour leurs services.

Dans le même ordre d'idées, Bitcoin peut aussi être utilisé pour contourner les sanctions économiques qu'imposent les différents États à leurs populations respectives dans le contexte de leurs rapports de force. Toute l'utilité de la cryptomonnaie a par exemple pu être constatée suite au début du conflit russo-ukrainien en 2022, lorsque le bloc occidental a décidé d'instaurer des sanctions financières lourdes à l'encontre de la Russie. Bitcoin a ainsi pu servir tant du côté des citoyens russes, qui ne pouvaient plus recevoir de fonds de l'étranger, que des ressortissants ukrainiens habitant dans les régions occupées.

Ainsi, toute personne vivant sous un régime autoritaire et désireuse de contourner ses lois ou de se révolter contre l'ordre établi trouvera un intérêt à Bitcoin. C'est là où se situe le cœur de l'utilisation de Bitcoin : dans ce qui est interdit et dans ce qui peut facilement le devenir.

La monnaie du marché noir

Bitcoin est un système d'argent liquide électronique qui peut être utilisé de manière confidentielle, sans requérir d'autorisation, avec peu de risques de censure. Il est par conséquent particulièrement adapté pour l'activité économique qui échappe à la supervision de l'État et à ses prélèvements, c'est-à-dire ce que nous appelons communément le marché noir.

Le terme « marché noir » est apparu dans la langue française au cours de la Seconde Guerre mondiale sous l'occupation allemande. Il s'agit d'une traduction littérale du mot allemand du même sens, *Schwarzmarkt*, qui daterait de la Première Guerre. Dès l'origine, le terme désignait un marché clandestin où la réglementation du commerce était contournée.

L'expression n'était pas employée auparavant car la réglementation n'était pas assez présente pour donner un nom à ce concept : l'échange de marchandises se faisait sur le marché tout court. Seul existait le terme « au noir » qui servait à qualifier l'activité réalisée de façon non déclarée, cachée au sou-

verain. Mais avec le développement d'une société de plus en plus policée et réglementée reposant sur des lois explicites plutôt que des normes sociales implicites, la nécessité de distinguer le marché réglementé du marché libre s'est fait ressentir, d'où l'émergence de l'appellation.

La notion de marché noir est floue : elle peut recouvrir à la fois l'activité commerciale exercée par des particuliers et celle des trafiquants de grande envergure, la vente de biens et services légitimes comme celle de produits issus de l'exploitation criminelle. C'est pourquoi il est nécessaire de la clarifier. Ici, nous entendons par marché noir l'économie libre où s'échangent, de manière non réglementée et non taxée, des biens et des services, légaux et illégaux, qui ne sont pas des produits directs de l'agression. Cette définition du marché noir inclut le « marché gris » où s'échangent des biens et services légaux par ailleurs (comme le travail au noir) et exclut le « marché rouge » où se monnaie le crime (comme le meurtre, l'extorsion ou l'esclavage).

Pour désigner l'ensemble des activités marchandes qui échappent au contrôle de l'État et à l'impôt, il arrive aussi que les gens parlent d'économie souterraine, d'économie clandestine ou d'économie parallèle. Cette économie rentre dans le cadre plus large de l'économie informelle, qui n'est pas nécessairement marchande et qui comprend des activités comme le travail domestique [38]. Cette dernière représente une part énorme de l'économie dans les pays en voie de développement.

Le marché noir profite toujours des circonstances restrictives qui pèsent sur l'économie. Durant la Seconde Guerre [39], son succès provenait des grandes pénuries créées par la guerre, par le contrôle des prix et par les conditions sévères imposées par l'occupant allemand. La population française était en effet soumise à des rationnements drastiques (la ration alimentaire officielle d'un adulte représentait 1 100 calories par jour en 1942) et à des prélèvements outranciers, sous forme de pillages, de taxes ou de réquisitions. Le recours au marché noir est alors devenu une question de nécessité. L'économie souterraine a également prospéré au sein des régimes les plus répressifs : c'était notamment le cas du marché noir en Union Soviétique qui représentait une « seconde économie [40] » sur laquelle reposait la survie du pays.

Mais le marché noir n'est pas qu'un phénomène controversé ; c'est aussi la pierre angulaire d'une véritable doctrine, appelée l'agorisme. L'agorisme (terme dérivé du grec ancien ἀγορά, *agora*, signifiant « place de marché ») est une philosophie politique dérivée du libertarianisme, qui préconise la pratique de l'économie souterraine comme moyen pacifique de réduire l'influence de l'État. Cette doctrine a été théorisée dans les années 1970 par Samuel

Edward Konkin III[41], un canadien vivant aux États-Unis, grand lecteur de Mises et Rothbard, qui cherchait à radicaliser la vision développée par l'école autrichienne d'économie. Après avoir pratiqué lui-même sa philosophie, il l'a mise sur papier en 1980 dans un long essai, le *Manifeste néo-libertarien*.

L'idée derrière l'agorisme était de joindre le geste à la parole, en unifiant la théorie libertarienne, fondée sur le principe de non-agression[42], et la pratique du marché noir (que Konkin appelait la « contre-économie[43] »), fondée sur la recherche du profit. Il s'agissait d'une stratégie visant à éradiquer l'agression (dont celle de l'État) de manière progressive et à créer une société libre (« l'agora ») par le biais d'actions individuelles intéressées.

L'idée de Konkin était d'appliquer les analyses de Mises et Rothbard à l'économie souterraine. Il suivait une démarche raisonnée qui consistait notamment à prendre en compte le risque lié à l'activité illégale (se manifestant par les amendes, l'emprisonnement et les dommages physiques) comme un risque entrepreneurial. Il écrivait :

> « Pourquoi les gens s'engagent-ils dans la contre-économie sans protection ? parce que le gain par rapport au risque qu'ils prennent est plus grand que la perte attendue. Cette affirmation est vraie au sujet de toute activité économique, bien sûr, mais concernant la contre-économie, elle mérite une attention particulière :
>
> Le principe fondamental de la contre-économie est d'échanger du risque contre du profit[44]. »

Ainsi, l'agorisme consistait bien plus à passer entre les mailles du filet étatique pour améliorer sa vie qu'à jouer les barons de la drogue. Si les activités les plus controversées et moralement sensibles du marché noir sont utiles pour illustrer le mécanisme, elles n'en sont pas moins inenvisageable pour la plupart des gens, qui ont une aversion au risque élevée. Il ne s'agit pas non plus d'un appel à violer la loi sans aucune restriction : le jeu n'en vaut souvent pas la chandelle.

Contrairement aux autres théories politiques qui ne font qu'énoncer des principes, l'agorisme fournissait à la fois une fin à viser – l'*agora*, la société sans État – et un moyen permettant d'y parvenir. La cohérence du processus reposait sur les incitations économiques des individus : les actions clandestines amélioraient directement leur vie à court terme, et contribuaient à réduire la place de l'État à long terme en le privant de son revenu fiscal.

Mais quel rapport avec la monnaie et avec Bitcoin ? La monnaie a toujours été une préoccupation de Samuel Konkin. L'idée agoriste a été développée dans les années 1970 aux États-Unis soit précisément au moment de l'abandon définitif de l'étalon-or et de l'inflation qui s'est ensuivie. Konkin imaginait

alors résoudre le problème par l'utilisation d'une banque illégale permettant d'échanger de l'or de manière pratique, mais cette idée comportait des risques trop élevés, comme nous le verrons dans le chapitre 4.

Le marché noir a ainsi manqué d'une monnaie endogène vraiment efficace. Depuis les années 70, l'essentiel de l'économie souterraine a fonctionné grâce aux monnaies fiat disponibles sous forme liquide, et en particulier aux billets verts américains répandus aux quatre coins du monde. L'utilisation des espèces est très pratique, car elles sont acceptées quasi partout, mais elle a pour effet de permettre aux autorités de bénéficier indirectement des activités illégales grâce au prélèvement caché du seigneuriage, issu du privilège de création monétaire. De plus, au vu des récentes évolutions, le contrôle sur la monnaie a tendance à s'accroître et l'argent liquide étatique est voué à devenir de plus en plus anecdotique, ce qui représente une menace existentielle pour le marché noir et la liberté en général.

Les métaux précieux comme l'or et l'argent semblent être des candidats acceptables. Cependant, ils possèdent deux défauts majeurs : leur coût de vérification élevé, ce qui explique le succès de la certification étatique au moyen des pièces frappées ; et leur portabilité réduite, ce qui explique le développement du crédit et l'apparition subséquente des monnaies fiat.

Bitcoin corrige ces insuffisances. Le coût de vérification est celui de l'entretien d'un nœud, qui peut être réparti entre plusieurs personnes, et sa portabilité est supérieure, notamment en ce qui concerne les paiements à distance.

Bitcoin constitue un concept de monnaie numérique particulièrement bien adapté pour le marché noir grâce à sa résistance à la censure et à l'absence de seigneuriage. Bitcoin est une manière pour les agoristes de littéralement « rendre à César ce qui est à César, et à Dieu ce qui est à Dieu » par l'abandon de la monnaie fiat, étroitement liée au prélèvement de richesse de l'État, et par l'utilisation exclusive d'une monnaie libre, neutre et décentralisée par essence.

C'est tout naturellement que les premiers contributeurs à Bitcoin s'inscrivaient dans cette démarche, voire y souscrivaient complètement. Martti Malmi, le jeune développeur finlandais qui a aidé Satoshi Nakamoto au début, avait typiquement ce genre de motivation. En avril 2009, dans une courte introduction présentant Bitcoin sur le forum anarcho-capitaliste de Freedomain Radio, il écrivait :

> « Le système est anonyme, et aucun État ne pourrait possiblement taxer ou empêcher les transactions. Il n'y a pas de banque centrale qui puisse déprécier la devise avec la création illimitée de nouvelle monnaie. L'adoption généralisée d'un tel système ressemblerait à quelque chose qui pourrait avoir un effet dévastateur sur la capacité de l'État à se nourrir à partir de son bétail [45]. »

Cette capacité a été illustrée par l'émergence de la place de marché Silk Road en 2011, qui utilisait le bitcoin comme unique intermédiaire d'échange. Les vendeurs y postaient des annonces, les acheteurs payaient et les produits étaient envoyés par voie postale. La plateforme garantissait la confidentialité des deux parties par l'utilisation du réseau Tor, et protégeait les acheteurs en intégrant un système de réputation pour la sélection des vendeurs et un procédé de dépôt fiduciaire pour arbitrer les échanges. Les produits disponibles sur la plateforme étaient divers mais il s'agissait essentiellement de drogue illicite, et notamment de cannabis. Cet « Amazon de la drogue » générait plus d'un million de dollars de volume mensuel en bitcoins à partir de 2012.

Silk Road a été créée par Ross Ulbricht qui a ouvertement admis avoir été influencé par l'école autrichienne d'économie et par la philosophie agoriste [46]. Sa place de marché en ligne était dans son esprit un moyen de détruire les structures agressives, et en particulier les cartels de la drogue dont l'influence nuisait aux trafiquants individuels. De manière générale, les initiatives comme Silk Road devaient mettre à bas l'État tel que nous le connaissons. Comme Ross le déclarait dans son entrevue avec Adrien Chen publiée le 1er juin 2011 :

> « L'État est la principale source de violence, d'oppression, de vol et de toute forme de coercition. Arrêtez de financer l'État avec l'argent de vos impôts et dirigez votre énergie productive vers le marché noir [47]. »

Néanmoins, son orgueil et les risques inconsidérés qu'il a pris l'ont mené là où on finit généralement lorsqu'on défie frontalement l'État : en prison. Il a été arrêté en 2013 et condamné à l'emprisonnement à perpétuité sans possibilité de libération conditionnelle en 2015.

Silk Road a été un élément essentiel du développement de Bitcoin, le premier cas d'utilisation majeur de la cryptomonnaie, et son héritage est toujours présent. De nombreux utilisateurs ont ainsi découvert Bitcoin soit en recherchant une mise en application des idées libertariennes (à l'instar de Roger Ver ou de Vitalik Buterin [48]), soit en cherchant à se procurer de la drogue sur Silk Road (comme Peter McCormack [49]). Cette particularité est une incarnation de la vision de Konkin, qui voulait réconcilier les « libertariens de bibliothèque » et les « contre-économistes » de l'économie souterraine.

La proposition de valeur de Bitcoin

Bitcoin est un concept de monnaie numérique fonctionnant sur Internet, résistante à la censure et résistante à l'inflation. Il diffère de ses alternatives que sont le dollar (et les monnaies fiat en général) et l'or (et les métaux

précieux en général), par ses propriétés nouvelles, liées à son absence de tiers de confiance.

Bitcoin est par essence un outil qui donne à l'individu le pouvoir de préserver sa liberté et sa richesse. Grâce à la résistance à la censure, il vise à permettre à quiconque de décider comment il veut dépenser son argent et, par conséquent, de choisir s'il veut le céder à autrui ou non. Grâce à la résistance à l'inflation, il permet à ses utilisateurs de ne pas subir le seigneuriage de l'État, en disposant d'une monnaie dont l'émission est prédéterminée et dont la quantité maximale est limitée.

De ce fait, le cœur de l'utilisation de Bitcoin se situe aux confins de ce qui est autorisé par les puissances de ce monde. Il est principalement, et restera, une monnaie de désobéissance, utilisée dans l'économie parallèle, pour acheter des biens et des services et pour conserver de la valeur à long terme. Avec l'inéluctable numérisation de la monnaie, il pourrait devenir un « territoire de liberté » équivalant à ce qui est aujourd'hui offert par l'argent liquide physique. Il a, après tout, été présenté au monde comme un « argent liquide électronique ».

4

La nécessité de décentralisation

Bitcoin donne aux individus une propriété entière et souveraine sur leur argent. D'une part, il leur permet de l'envoyer à n'importe quelle personne, n'importe où dans le monde, à n'importe quel moment et quel que soit le motif, en empêchant le gel des transactions. D'autre part, il leur permet de préserver pleinement leur pouvoir d'achat en interdisant la création arbitraire d'unités supplémentaires. Par cette double proposition de valeur, Bitcoin s'inscrit dans un rapport antagoniste avec l'État, qui revendique une prérogative exclusive sur la monnaie et un contrôle inquisitorial sur son utilisation.

Souvent présenté comme l'institution qui possède le « monopole de la violence légitime », l'État se caractérise plutôt par le transfert de richesse non consenti qu'il assure. Ce transfert se manifeste de deux manières principales que sont l'impôt, c'est-à-dire le prélèvement direct du contribuable, et le seigneuriage, à savoir la spoliation indirecte de l'épargnant par l'émission de monnaie. Et ces moyens de prélèvement reposent tous deux sur le contrôle monétaire : le premier est facilité par la surveillance et le blocage des transactions ; le second est issu de la maîtrise sur la définition de l'unité de compte.

De ce fait, l'État ne tolère aucune concurrence sérieuse en matière monétaire. En tant qu'outil de liberté, Bitcoin remet ce contrôle en question et constitue en ceci une menace du point de vue étatique. C'est la raison d'être de son architecture distribuée, fondamentale dans sa conception.

Dans ce chapitre, nous étudierons d'abord le transfert de richesse organisé par l'État et ses conséquences. Puis, nous verrons comment le contrôle monétaire a pu se renforcer au cours de l'histoire, et comment il menace de s'accroître à nouveau par l'intermédiaire de la monnaie numérique de banque centrale. Enfin, nous expliquerons en quoi les systèmes alternatifs centralisés ne sont pas viables et pourquoi la décentralisation constitue une nécessité.

L'État et l'impôt

Du point de vue sociologique, l'État se définit classiquement comme une autorité souveraine qui s'exerce sur un territoire déterminé et sur un peuple qu'elle représente officiellement. Il en ressort trois éléments qui le caractérisent : un pouvoir sur une population, un territoire et une certaine acceptation.

Premièrement, la nature de l'État est d'utiliser la force physique : son existence repose sur la contrainte, imposée par la violence ou la menace de violence, par l'intermédiaire d'une police et d'une armée. Cette violence s'exerce sur un groupe de personnes sous sa domination, appelées des sujets ou des citoyens, dont il restreint la liberté naturelle, le plus souvent au moyen de lois et de décrets délimitant les interdictions. En particulier, il lève un impôt (terme venant du latin *impōnō*, « charger », « faire peser sur ») qui est, dans les faits, un prélèvement de richesse ne disposant pas du consentement individuel [1].

Deuxièmement, l'autorité de l'État s'exerce au moyen de la domination sur un territoire donné. Cette caractéristique lui permet de consolider son prélèvement au sein de frontières déterminées : puisque les êtres humains ont besoin de la terre (ou de la mer) pour exercer leurs facultés, le contrôle du territoire facilite énormément leur soumission. C'est la domination sur la terre qui explique l'organisation féodale (du latin médiéval *feodum*, « fief ») de l'État dans les sociétés agraires.

L'impôt est aujourd'hui levé grâce à une multitude de contrôles réalisés par l'État. Ces contrôles passent en premier lieu par la surveillance financière, qui s'applique notamment dans le domaine bancaire : les banques et autres institutions financières sont responsables devant l'administration fiscale, à qui elles doivent transmettre les informations douteuses concernant leurs clients. Cette surveillance est facilitée par un certain nombre de lois, comme par exemple les restrictions sur l'utilisation de l'argent liquide. À l'intérieur du territoire, la collecte de l'impôt se base sur le contrôle fiscal, c'est-à-dire l'ensemble des méthodes d'intervention permettant d'examiner les déclarations,

de les confronter à la réalité des faits et de réhausser, le cas échéant, les bases d'imposition. La préservation du revenu fiscal de l'État repose également sur l'entrave des flux de richesse sortant du territoire, par le biais des contrôles douaniers et des contrôles de capitaux. Tous ces contrôles sont étroitement liés à la question de la censure financière, traitée dans le chapitre 9 du présent ouvrage.

La collecte de l'impôt sur le territoire se fait principalement par l'intermédiaire des acteurs économiques établis, même lorsqu'ils ne sont pas directement taxés. En France, la taxe sur la valeur ajoutée, prélevée sur la vente des biens et services, est ainsi payée par le client, mais versée par le commerçant qui doit l'ajouter à son prix de vente. De même, de nombreuses charges fiscales sont retenues à la source par les entreprises mais payées par leurs employés, comme la contribution sociale généralisée et (aujourd'hui) l'impôt sur le revenu. Ce recours à l'impôt « indirect » permet de réduire le nombre de personnes à surveiller et de rendre le prélèvement « indolore » pour ceux qui le paient réellement.

Troisièmement, l'État bénéficie d'une *large acceptation* de la part de la population, qui peut aller de l'approbation active à la résignation passive. C'est cet élément qui le différencie des groupes criminels organisés qui ne bénéficient pas en général d'une telle aura. Bien que temporaire et partielle, cette acceptation est à l'origine de l'idée de « contrat social », qui n'a rien d'un réel contrat juridique, mais qui forme une constatation de la situation existante. L'État tire ainsi son nom du fait qu'il incarne l'état actuel du rapport de force au sein de la société.

L'acceptation de l'État assure la pérennité du prélèvement fiscal, en faisant en sorte que son pouvoir n'ait pas pas besoin d'être maintenu par la force pure. L'État affirme sa légitimité en prétendant représenter les intérêts du peuple qui vit sur son territoire, au moyen d'idéologies diverses, de façon à rendre les contributeurs dociles et à limiter les révoltes.

En particulier, l'État revendique un monopole sur la violence défensive [2], et garantit le maintien de l'ordre intérieur (par l'intermédiaire de la police) et la défense contre les ennemis extérieurs (par le biais de l'armée). Ce service réel n'est pas réalisé de manière purement altruiste : l'intérêt de l'État est de défendre les forces productives contre les perturbations internes et externes, tout en les empêchant d'organiser elles-mêmes leur propre protection, dans le but de stabiliser son revenu fiscal. Ce monopole s'apparente ainsi à un chantage à la protection accepté par la population comme un moindre mal.

Puisque l'impôt est la pierre angulaire de la construction étatique, son

paiement possède un caractère sacré. C'est ce qui explique pourquoi son évitement est systématiquement dénigré, y compris lorsqu'il est légal. C'est aussi la raison derrière la répression sévère de la résistance fiscale, qui passe notamment par la limitation de la liberté d'expression dans le domaine. En France, il est par exemple interdit d'appeler à arrêter de payer l'impôt, sous peine d'une amende de 3 750 € et d'un emprisonnement de six mois [3].

La capacité de prélèvement de l'État n'est cependant pas infinie. D'abord, il existe une pondération subtile entre le niveau effectif du prélèvement de richesse et la destruction économique induite, qui varie selon la préférence temporelle des bénéficiaires [4]. Ensuite, le niveau de prélèvement dépend du niveau d'acceptation de la population et il existe nécessairement un point au-delà duquel l'accroissement du taux de prélèvement se traduit par un amoindrissement du prélèvement total, phénomène illustré par la courbe de Laffer. Enfin, la capacité de prélèvement dépend des moyens techniques possédés par l'appareil étatique, notamment en ce qui concerne la surveillance, et des outils à la disposition de la population pour résister fiscalement, ce qui inclut bien entendu Bitcoin.

L'État est donc l'incarnation de la violence institutionnalisée, qui a pour fonction primaire d'assurer un transfert de richesse non consenti individuellement. Plus qu'un groupe de personnes identifié, il doit être bien plus compris comme un ensemble d'actions réalisées par des individus dans un contexte spécifique. Ainsi, nous nous référerons ici à l'État au singulier en tant que concept pouvant se manifester dans des instances particulières plus ou moins indépendantes, mais toujours selon les mêmes principes.

La monnaie et le seigneuriage

Si nous parlons de l'État, c'est parce qu'il entretient une relation étroite avec la monnaie. Comme nous l'avons vu dans le chapitre 3, celui-ci s'est arrogé une prérogative de plus en plus grande sur la définition de l'intermédiaire d'échange, en garantissant d'abord sa certification, puis en contrôlant aujourd'hui son émission. Cet état de fait a conduit certains théoriciens, dont notamment les chartalistes, à adopter une approche fiscale de la monnaie qui fait du paiement de l'impôt la source originelle de la valeur de cette dernière.

Ce lien étroit s'explique par le fait que l'État en tire un bénéfice considérable, le seigneuriage [5], qui est l'avantage financier direct qui découle de l'émission de monnaie pour l'émetteur. Le seigneuriage constitue en effet la seconde source principale de revenu de l'État, aux côtés de l'impôt, permet-

tant de financer la dépense publique. Il est par nature une spoliation indirecte du détenteur de monnaie, beaucoup plus efficace à court terme que le prélèvement direct du contribuable. L'endettement, souvent cité comme un troisième moyen, n'est en réalité qu'un impôt différé ou un seigneuriage déguisé.

Le seigneuriage est ainsi le fait de tirer profit d'une industrie particulière : la production de monnaie. Il est le résultat de quatre mesures légales fondamentales que sont la contrefaçon légalisée, le monopole sur la production, l'imposition du cours légal et la suspension des paiements [6]. Comme dans le cas de l'impôt, ces actions sont largement acceptées dans la mesure où elles émanent de la puissance publique.

La contrefaçon légalisée consiste à faire circuler de la monnaie dont le certificat ne correspond pas à ce qui est attendu par la population générale. Typiquement, il s'agit de faire circuler des pièces possédant une teneur moindre en métal que les pièces similaires existantes ou bien de billets représentatifs dont la monnaie de base de garantie est en réalité conservée de manière fractionnaire.

Le monopole sur la production de monnaie est le privilège exclusif d'émission monétaire accordé à une entité, la dédouanant de toute concurrence et lui permettant de vendre sa monnaie à un prix supérieur à ce qu'il aurait été sur le marché libre. Ce privilège est habituellement délégué à une entité contrôlée par l'État comme un hôtel de la Monnaie ou une banque centrale.

Le cours légal est l'obligation imposée aux acteurs économiques d'accepter une monnaie à la valeur nominale dictée par l'État. L'imposition du cours légal peut être restreinte et ne concerner que les paiements différés (c'est le sens de la *legal tender* anglo-saxonne) ou bien être plus large et se rapporter à tous les paiements (comme c'est souvent le cas en Europe continentale [7]). Il s'agit d'avantager la monnaie dont l'État dispose d'un monopole d'émission en la surestimant par rapport aux monnaies concurrentes.

Ce cours légal a pris plusieurs formes au cours de l'histoire. Il se retrouvait dans le bimétallisme (double étalon) où le ratio entre l'or et l'argent était fixé à une valeur arbitraire, avantageant l'un ou l'autre des deux métaux. Il se manifestait pendant la période de l'étalon-or classique lorsque les certificats représentatifs devaient être échangés au même cours que le numéraire. Il était également institué par l'étalon de change-or qui imposait que les monnaies nationales des pays secondaires aient cours à un taux déterminé par rapport à la livre ou au dollar, le taux du marché étant maintenu artificiellement haut par le contrôle des changes. Aujourd'hui, le cours légal se définit par rapport au cours sur le marché des changes et il se manifeste par l'interdiction de

proposer systématiquement un prix différent selon l'intermédiaire d'échange utilisé.

La suspension des paiements consiste, pour une banque centrale, à interrompre momentanément le remboursement de ses clients, auquel cas on parle de cours forcé. Dans le cas des billets représentatifs, la possibilité de recourir à cette mesure légale permettait de ne pas conserver l'intégralité de l'or en réserve, en empêchant les retraits dans le cas d'une chute de confiance.

Depuis l'Antiquité jusqu'au XIXe siècle, la monnaie était constituée de pièces de métaux précieux, essentiellement de l'or, de l'argent et parfois du cuivre. Il était donc impossible pour le souverain de créer de nouvelles unités à partir de rien. Cependant, il pouvait dévaluer les pièces existantes en réduisant leur teneur en métal.

À l'époque romaine, le *denarius* d'argent (qui a donné son nom au denier) a été dévalué à de nombreuses reprises, lentement d'abord, avant de voir sa teneur en métal être réduite à l'excès au cours de la crise du IIIe siècle. Le seigneuriage retiré a permis à l'Empire romain de continuer à financer sa domination, sans pour autant continuer son expansion territoriale. De même, tous les souverains européens ont procédé à ce type de manipulation au cours du Moyen Âge. Ces pratiques ont notamment été observées par le philosophe chrétien Nicolas Oresme au XIVe siècle.

De plus, cette manipulation des pièces de monnaie a un effet autrement malencontreux : celui de chasser de la circulation la monnaie sous-estimée, qui se retrouve thésaurisée ou exportée à l'étranger. Ce phénomène porte le nom de loi de Gresham, loi économique faisant référence à Sir Thomas Gresham, un grand marchand et financier anglais du XVIe siècle, qui avait établi le lien causal entre la disparition des meilleures pièces d'argent de la circulation et les mesures légales du pouvoir de l'époque [8]. Cette loi, couramment résumée par l'expression proverbiale « la mauvaise monnaie chasse la bonne », stipule qu'en l'existence d'un taux de change légal fixe entre deux monnaies, la mauvaise monnaie (c'est-à-dire celle qui est surestimée) a tendance à remplacer la bonne monnaie (c'est-à-dire celle qui est sous-estimée) en tant que moyen de paiement dans le commerce. Cette loi s'applique également, dans une moindre mesure, pour la monnaie représentative et pour la monnaie fiat.

Le développement des banques modernes à partir de la Renaissance a provoqué l'apparition des billets de banque convertibles à vue, bien plus pratiques pour déplacer de la valeur dans l'espace. Le pouvoir a repris cette invention à son compte en monopolisant l'émission des billets et en faisant des instruments supposés représentatifs.

Dans ce cas, le seigneuriage consiste à créer plus de billets qu'il n'y a de métal précieux en réserve, c'est-à-dire réaliser une fraude financière. Mais une contrainte subsiste : une grande partie du métal doit être conservée, sous peine de voir les créanciers vider les coffres. L'État peut choisir de suspendre les paiements (ce qu'il a fait dans l'histoire), mais une telle mesure s'accompagne alors d'une baisse drastique de confiance dans les billets par rapport au métal qu'ils sont censés représenter. C'est pourquoi le régime de l'étalon-or est resté relativement stable au niveau monétaire. Il a cependant pavé la voie à un régime autrement plus inflationniste : celui du papier-monnaie.

Le seigneuriage a acquis un rôle majeur avec l'apparition du papier-monnaie, qui est une monnaie fiduciaire basée sur un support physique. Le seigneuriage consiste alors juste à créer plus de billets dont l'usage est imposé sur le territoire, ce qui est considérablement plus efficace que la dévaluation des pièces en métal précieux et la fraude sur les billets représentatifs.

Dès l'origine, le papier-monnaie a permis de financer les projets pharaoniques des États. Il est notamment indissociable de la guerre moderne. L'émission des *greenbacks* américains, désignés comme tels à cause de l'encre verte utilisée pour imprimer le verso, entre 1861 et 1865 a permis de soutenir la guerre de Sécession aux États-Unis. De même, la Première Guerre mondiale a été majoritairement financée par la création monétaire et par la réduction de la dette liée à l'inflation.

Pour éviter une fuite trop importante vers des monnaies concurrentes jugées plus fiables, les États ont également mis en place des mesures de contrôle des changes qui réglementaient l'achat et la vente de devises étrangères. Ces mesures servaient à maintenir la valeur de la monnaie à un niveau artificiellement haut, alors même que la confiance dans celle-ci s'effondrait. Le prétexte invoqué était souvent la « lutte contre la spéculation ».

Toutefois, même si l'émergence du papier-monnaie constituait une manne inédite, la capacité de profiter de la monnaie n'est pas devenue illimitée : la production de pièces et de billets fiduciaires et la lutte contre la contrefaçon privée ont un coût incompressible réduisant le seigneuriage. C'est en partie pourquoi il existe aujourd'hui une volonté de remplacer cet argent liquide par une monnaie intégralement numérique.

Enfin, tout comme l'impôt, le seigneuriage repose sur l'acceptation de la population, qui est soutenue en particulier par une limitation de l'expression. En France, il est ainsi interdit de faire douter le public de la solidité de la monnaie, celui qui désobéit à cette loi s'exposant à une amende de 9 000 € et à deux ans de prison [9].

L'inflation des prix

La principale conséquence du seigneuriage est l'inflation des prix. Ce terme, qui vient du latin *inflatio* signifiant « gonflement », « enflure », « dilatation », désigne la perte du pouvoir d'achat de la monnaie qui se traduit par une augmentation générale et durable des prix. Il s'agit ainsi d'un phénomène qui touche l'économie dans son ensemble à long terme.

Contrairement à ce qui est parfois supposé, toute hausse des prix n'est pas une manifestation de l'inflation. À cause de son caractère durable, l'inflation est par nature structurelle et non conjoncturelle. Les mesures temporaires imposées par un État peuvent faire augmenter les prix, mais cet effet ne constitue pas en soi de l'inflation.

L'inflation des prix est un phénomène qui a pu être observé dans de nombreuses économies. Elle était déjà présente à l'époque de l'Empire romain, dont elle a accompagné l'effondrement à partir du IIIe siècle, en culminant sous le règne de l'empereur Dioclétien. Elle a également pu être observée dans nos économies modernes suite aux deux guerres mondiales, dans les années 1970 et plus récemment dans les années 2020.

L'inflation peut provenir d'une augmentation générale de la demande ou d'une diminution de l'offre de biens et de services. Elle peut théoriquement être le fait de plusieurs facteurs comme l'inflation monétaire, la raréfaction de l'énergie, la destruction de richesse par la guerre ou la fuite des capitaux. En pratique, c'est-à-dire dans le cas d'une économie croissante, pacifiée et indépendante, l'inflation des prix à long terme est, en règle générale, une conséquence de l'inflation monétaire.

L'inflation monétaire est l'excédent de production de monnaie par rapport à la production naturelle sur le marché libre [10]. Elle résulte de la manipulation de la monnaie par le pouvoir en place, qui cherche à en tirer profit par le biais du seigneuriage. Il arrive ainsi régulièrement que l'État sacrifie le pouvoir d'achat de sa monnaie à long terme pour obtenir un revenu à court terme, par exemple dans le contexte d'une crise militaire, politique ou sanitaire.

Le phénomène de l'inflation est souvent mal appréhendé car il n'est pas le phénomène uniforme et instantané que l'on a tendance à se représenter. Une injection de monnaie dans l'économie exerce un effet progressif et différencié sur les prix au fur et à mesure que la monnaie se diffuse par les échanges. C'est ce qu'on nomme l'effet Cantillon, qui a été observé en 1730 par l'économiste physiocrate Richard Cantillon dans son *Essai sur la Nature du Commerce en Général* où il déclarait qu'« une augmentation d'argent effectif [causait] dans un État une augmentation proportionnée de consommation, qui [produisait]

par degrés l'augmentation des prix [11] ».

Cet effet Cantillon s'applique à l'espace et au temps. La monnaie produite peut se retrouver dans des espaces spécifiques (les aires urbaines par exemple), se concentrer dans certaines régions du monde (hors du territoire national notamment) ou se concentrer dans certains secteurs économiques particuliers (comme la finance). La propagation peut être ralentie par certaines pratiques, comme le paiement de salaires mensuels. Cependant, l'effet de la hausse de la quantité finit par se répercuter progressivement sur l'ensemble de l'économie.

Entretemps, les personnes proches de l'émission monétaire s'enrichissent. Le producteur de monnaie la dépense en apportant une demande supplémentaire, quitte à proposer un prix supérieur pour obtenir le bien désiré. Le commerçant qui la reçoit, devenu momentanément plus riche, réitère cette dépense plus généreuse auprès d'un autre commerçant. Et ce phénomène se poursuit jusqu'à atteindre les confins de la société économique, de telle sorte que les personnes les plus éloignées de l'émission monétaire s'en retrouvent les plus lésées.

L'inflation des prix est donc une manifestation différée de l'inflation monétaire résultant du seigneuriage excessif de l'État. Si le phénomène s'emballe, celui-ci peut conduire *in fine* à la destruction de l'unité de compte, ce qu'on appelle une hyperinflation. Dans ce cas, l'inflation n'est plus nourrie par la production de monnaie (qui peine à suivre le rythme), mais par la fuite de la valeur vers d'autres monnaies jugées plus fortes ou vers des biens liquides.

Les banques centrales

De nos jours, le système monétaire mondial repose sur le modèle de la banque centrale. Une banque centrale est une institution qui possède un monopole d'émission de la monnaie ayant cours légal sur un territoire donné. Tous les États du monde ont recours à une telle institution pour gérer leur monnaie fiat.

La banque centrale est le résultat de la prise de contrôle sur l'activité bancaire par le pouvoir central. La banque moderne, consistant à faire commerce de la monnaie et du crédit, s'est développée au cours de la Renaissance. Elle se basait sur deux innovations majeures : le dépôt à vue et la lettre de change, qui sont devenus le compte courant et le billet de banque, lorsque le crédit s'est popularisé en tant que substitut monétaire.

Le pouvoir a peu à peu centralisé cette activité en créant des banques publiques qui bénéficiaient d'avantages par rapport à leurs concurrentes privées. Ces banques publiques étaient initialement cantonnées à une ville. C'était par

exemple le cas de la Banque du Rialto créée à Venise en 1587, de la banque d'Amsterdam fondée en 1609 avec la bénédiction des Provinces-Unies ou bien de la Banque de Stockholm créée en 1656 par Johan Palmstruch. Puis, des banques nationales ont été formées, comme la banque des États du royaume de Suède (plus tard renommée *Sveriges Riksbank*) qui a été fondée en 1668, la Banque d'Angleterre qui a vu le jour en 1694, ou encore l'éphémère Banque générale, qui s'est développée en France de 1716 à 1720 sous la supervision de l'écossais John Law.

Les banques centrales ont émergé de ces banques publiques en acquérant le monopole d'émission des billets. La Banque d'Angleterre a acquis ce privilège grâce au *Bank Charter Act* de 1844. En Prusse, le décret du 11 avril 1846 a permis à la Banque royale de Prusse de bénéficier d'un monopole d'émission sur le même modèle que le Royaume-Uni. La Banque de France, fondée en 1800 par Napoléon Bonaparte, a vu son privilège d'émission (à l'origine limité à Paris) être étendu à l'ensemble du territoire en 1848. Aux États-Unis, la banque centrale n'a été créée que tardivement avec la fondation de la Réserve Fédérale en 1913.

Contrairement à ce qui est communément affirmé par les responsables politiques, la banque centrale n'est pas indépendante de l'État. Elle repose sur la force de l'État pour assurer son monopole et l'application du cours légal ; et ce dernier dépend de la banque centrale pour prélever un seigneuriage. La banque centrale n'est ainsi qu'une institution qui joue un rôle dans l'appareil étatique.

Cette implémentation des banques centrales a mené à une installation durable de la monnaie fiat papier. D'abord, les billets étaient adossés à une quantité de métal précieux, et notamment à l'or durant la période de l'étalon-or classique de 1873 à 1914. Ensuite, leur convertibilité directe a été interrompue, au début de manière temporaire au cours d'épisodes de cours forcé plus ou moins longs, puis de manière définitive à partir de la Première Guerre mondiale en 1914 pour l'Europe et de la Nouvelle donne de Franklin Roosevelt en 1933 pour les États-Unis. Enfin, toute référence à l'or dans le système monétaire mondial a été abandonnée en 1971, avec l'abrogation de l'étalon de change-or de Bretton Woods par Richard Nixon.

La banque centrale possède aujourd'hui un rôle prépondérant. Elle intervient largement dans l'économie par sa politique monétaire. Ses missions principales sont la limitation de l'inflation des prix, qui se traduit souvent par un objectif de hausse de l'IPC à 2 % par an, et le prêt en dernier ressort [12], consistant à fournir de la liquidité aux banques en difficulté lors d'un res-

serrement du crédit. Elle peut avoir d'autres missions secondaires comme le soutien à la baisse du chômage.

Pour réaliser ces missions, trois leviers d'action lui sont généralement octroyés : la production de la monnaie physique, le rachat de titres sur les marchés financiers et l'influence sur l'émission du crédit par le biais de taux directeurs. Tout d'abord, la banque centrale peut avoir pour tâche de fabriquer le papier-monnaie. Mais cette tâche peut également être déléguée. La Fed délègue cette tâche au Bureau de la gravure et de l'impression, la BCE aux banques nationales des États-membres de l'Union Européenne.

Ensuite, la banque centrale peut se rendre sur les marchés financiers afin d'y intervenir. Elle réalise traditionnellement des opérations d'open market, c'est-à-dire des achats et des ventes de titres, en particulier d'obligations publiques (bons du Trésor), sur le marché interbancaire. Les politiques monétaires non conventionnelles lui permettent également de mener des opérations d'assouplissement quantitatif (QE), plus longues et plus agressives, ce qui permet d'apporter de la liquidité pour soutenir l'économie en cas de crise. Mais ces achats permettent surtout de financer la dette de l'État : puisque la taille du bilan est strictement croissante, on peut considérer qu'une partie de ces achats représente un pur seigneuriage.

Enfin, la banque centrale influence l'émission du crédit bancaire, à l'aide de ses taux directeurs. Ces taux, appelés différemment selon les pays, sont généralement au nombre de trois : le taux de refinancement, qui est taux usuel pour lequel les banques commerciales peuvent obtenir de la monnaie centrale, le taux du prêt marginal, qui est le taux de prêt à courte échéance servant à obtenir des fonds en cas d'urgence, et le taux de rémunération des dépôts, le taux d'intérêt payé par la banque centrale pour la conservation de monnaie centrale en réserve. Le premier, le plus important, sert à limiter la création de crédit bancaire ; le deuxième, qui est nécessairement le plus élevé, permet de maintenir le système bancaire en place en cas de crise grave ; le troisième, qui doit être le moins élevé, a pour rôle de décourager ou d'encourager le prêt commercial à court terme. La banque centrale fixe également un niveau de réserves obligatoires. Ces taux ne sont pas des taux d'intérêt issus du marché et peuvent donc être négatifs.

Le fonctionnement des taux directeurs permet à la banque centrale, et donc à l'État, de prélever un seigneuriage en prêtant à intérêt la monnaie centrale aux banques commerciales. Ces dernières peuvent ensuite prêter ces fonds à leurs emprunteurs qui, par leurs actions économiques comme l'investissement et la consommation, les diffusent dans l'économie toute entière.

Dans ce fonctionnement pyramidal, les banques commerciales tirent aussi profit de leur position. Le système bancaire, formé comme un cartel, bénéficie d'un privilège d'émission de crédit et est protégé des conséquences économiques par la banque centrale, qui constitue un prêteur en dernier ressort, et par le Trésor, qui peut procéder à un renflouement externe [13]. Ce privilège lui permet, dans la mesure où la banque centrale l'autorise, de prélever elles-aussi un seigneuriage sur le crédit qu'elles émettent. De plus, cette situation encourage l'expansion du crédit et stimule les cycles économico-financiers haussiers et baissiers, qui ont des effets terriblement néfastes sur l'économie comme le malinvestissement et les crises récessionnistes.

Ce système banco-monétaire a été largement critiqué au cours des décennies qui ont suivi l'abandon définitif des accords de Bretton Woods en 1971. Satoshi Nakamoto s'est lui-même joint à la critique en février 2009 lorsque, soucieux d'amener les gens à s'intéresser à Bitcoin, il a mis en avant les conséquences de ce fonctionnement bancaire :

> « Le problème fondamental de la monnaie conventionnelle est toute la confiance nécessaire pour la faire fonctionner. Il faut faire confiance à la banque centrale pour qu'elle ne déprécie pas la monnaie, mais l'histoire des monnaies fiat est pleine de violations de cette confiance. Il faut faire confiance aux banques pour détenir notre argent et le transférer par voie électronique, mais elles le prêtent par vagues de bulles de crédit avec à peine une fraction en réserve [14]. »

Les banques centrales sont ainsi issues de la centralisation de l'activité bancaire. Cependant, ce ne sont plus aujourd'hui des banques, dans le sens où elles n'émettent plus des substituts monétaires, mais la monnaie elle-même. Elles sont en effet devenues des institutions de création monétaire, prenant la place des hôtels de la Monnaie qui frappaient les pièces.

Il est intéressant de constater que c'est l'adoption du billet de banque et la prise de contrôle totale sur celui-ci qui ont mené à l'installation durable de la monnaie fiat. En garantissant sa convertibilité, l'État lui a d'abord octroyé un avantage par rapport aux espèces sonnantes et trébuchantes, le billet offrant une portabilité largement supérieure aux pièces de métaux précieux. Une fois le billet devenu monnaie courante, la puissance publique n'a ensuite eu qu'à suspendre progressivement la convertibilité pour conclure la transformation.

De même, une telle prise de contrôle sur les comptes bancaires est aujourd'hui en cours. Avec la monétisation générale du crédit bancaire numérique soutenue par la garantie étatique des dépôts, tous les ingrédients sont présents pour l'accomplissement d'une nouvelle mutation. C'est l'objet du développement de la monnaie numérique de banque centrale.

La monnaie numérique de banque centrale

Une monnaie numérique de banque centrale (MNBC), de l'anglais *central bank digital currency* (CBDC), est une monnaie fiduciaire numérique émise par une banque centrale. Il s'agit d'une sorte de monnaie entièrement numérique qui ne représente pas une créance. Les systèmes informatiques de MNBC sont actuellement en phase de conception tout autour du monde. Leur déploiement pourrait constituer une évolution majeure dans l'histoire de la monnaie via l'appropriation indirecte des dépôts bancaires par l'État.

Disposer d'une monnaie qui serait gérée intégralement par une banque centrale et qui concurrencerait la monnaie scripturale des banques commerciales n'est pas une idée nouvelle. Cette idée remonte en effet à une période antérieure à la démocratisation d'Internet. On la retrouve sous la plume de l'économiste keynésien James Tobin, lauréat du prix Nobel, qui faisait une suggestion approchante en 1987 en écrivant :

> « Je pense que l'État devrait mettre à la disposition du public un intermédiaire de paiement offrant la commodité des dépôts et la sécurité des espèces, qui serait essentiellement de la monnaie sous forme de dépôt, transférable pour tout montant par chèque ou autre ordre [15]. »

Avec l'émergence de Bitcoin dans les années 2010, l'idée d'une monnaie numérique gérée par une banque centrale et mise à disposition des particuliers a été remise au goût du jour. Elle est tout d'abord venue de l'intérieur de la communauté de Bitcoin : elle a été évoquée par un utilisateur le 26 mars 2013 sous la forme de « Fedcoin », un concept satirique d'une « une alternative centralisée aux monnaies pair-à-pair » qui serait contrôlée par la Réserve fédérale des États-Unis [16]. Du côté de l'Europe, l'idée d'un Eurocoin a été évoquée par Bitcoin.fr le 1er avril 2014 [17]. Bien qu'initialement ironique, cette idée a mené à diverses réflexions sur la pertinence d'un tel système et sur les conséquences de sa potentielle implémentation [18].

Le sujet est devenu plus sérieux au début de l'année 2015 lorsque David Andolfatto, alors vice-président de la Federal Reserve Bank de Saint-Louis, en a fait la promotion dans une présentation donnée durant la *P2P Financial Systems Conference* à Francfort, puis dans un article publié sur son blog [19]. Sa proposition était de faire en sorte que, contrairement à Bitcoin, le système d'émission monétaire soit contrôlé par la Réserve fédérale, qui se chargerait d'assurer la convertibilité de l'unité numérique en dollars. Son modèle restait néanmoins mesuré : pour Andolfatto, Fedcoin devrait être un système ouvert et anonyme.

Le concept de monnaie numérique de banque centrale a pleinement émergé avec le discours du 2 mars 2016 de Ben Broadbent, gouverneur adjoint pour la politique monétaire à la Banque d'Angleterre, prononcé à la London School of Economics, qui donnait naissance au terme « *central bank digital currency* » [20]. Dans ce discours, le banquier expliquait comment un registre distribué pouvait permettre de remplacer l'actuel modèle de compensation et de règlement interbancaire, d'en élargir l'accès aux acteurs financiers et aux particuliers en leur permettant de posséder un compte auprès de la banque centrale, et de faire ainsi concurrence à l'argent liquide et aux dépôts dans les banques commerciales.

Depuis, le concept a été mis en œuvre de manière expérimentale. La Banque populaire de Chine, qui a monté un programme de recherche (appelé *Digital Currency Electronic Payment* ou DCEP) dès 2014, a commencé à déployer progressivement son yuan numérique (*digital renminbi*) en 2020. La Riksbank suédoise a envisagé de mettre en place une couronne électronique (ou e-Krona) en novembre 2016, qui est toujours en phase de tests.

Aux États-Unis, l'effort est pris en charge par la *Digital Currency Initiative* du MIT Media Lab, une initiative créée en 2015 dans le but « de réunir les esprits les plus brillants [...] pour mener les recherches nécessaires au développement des monnaies numériques et de la technologie blockchain [21] » et qui a notamment financé certains développeurs de Bitcoin Core comme Gavin Andresen, Wladimir van der Laan et Cory Fields. Cette initiative a abouti au projet Hamilton en février 2022, un prototype de monnaie numérique développé conjointement avec la *Federal Reserve Bank* de Boston [22].

Du côté de la Grande-Bretagne, la Banque d'Angleterre a annoncé former un groupe de travail en avril 2021 en collaboration avec le trésor de Sa Majesté. En Europe continentale, la BCE a annoncé en juillet 2021 vouloir développer un euro numérique.

Le concept de monnaie numérique de banque centrale se fonde sur un modèle déjà existant : celui de la monnaie numérique interbancaire composée des avoirs monétaires détenus par les banques commerciales auprès de la banque centrale. Cette monnaie est destinée à fluidifier les règlements entre les banques, plutôt que de passer par des espèces. Elle constitue, avec les pièces et les billets en circulation, ce qu'on appelle la monnaie centrale ou monnaie de base. Celle-ci est fiduciaire par nature, dans le sens où elle tire essentiellement sa valeur de la confiance que ses utilisateurs accordent à l'entité qui l'émet et non pas à une propriété physique intrinsèque.

L'idée derrière la monnaie numérique de banque centrale est d'étendre

l'accès de cette monnaie interbancaire aux autres entreprises et aux particuliers. Les banques centrales parlent parfois de « MNBC de détail » (*retail CBDC*) pour différencier ce projet de celui d'une modernisation de la monnaie interbancaire existante, qui constituerait une « MNBC de gros [23] » (*wholesale CBDC*). Nous parlerons ici uniquement de la MNBC de détail.

D'un point de vue technique, une monnaie numérique de banque centrale serait basée sur un registre de compte, distribué entre quelques serveurs grâce à un mécanisme de consensus de type classique, très bien adapté pour traiter un volume transactionnel élevé. La réplication des données financières à différents endroits permettrait d'éviter toute perte liée à une panne ou une cyberattaque.

Le système serait accessible via une identification de l'utilisateur, probablement grâce un système d'identité numérique, dans le but de satisfaire les exigences de lutte contre le blanchiment et le financement du terrorisme. Les transactions des utilisateurs seraient cachées au public, mais pourraient être observées par une autorité homologuée.

Comme tout système informatique, un tel dispositif serait programmable, et des conditions de dépenses pourraient être ajoutées aux fonds. De plus, ce modèle pourrait être modifié au cours du temps pour inclure de nouvelles fonctionnalités.

Les apports directs de la monnaie numérique pour l'utilisateur seraient multiples. D'abord, elle éliminerait le risque de contrepartie lié au crédit : l'utilisateur pourrait jouir théoriquement de tous les avantages apportés par un compte bancaire sans subir le risque de faillite de la banque. Ensuite, elle fournirait une plus grande accessibilité et favoriserait l'inclusion financière en permettant de « bancariser les non-bancarisés » à moindre frais. Enfin, elle automatiserait les opérations financières de façon à améliorer considérablement la qualité des services en ligne.

Grâce à ces avantages, la monnaie numérique de banque centrale paraît représenter un progrès, une modernisation de la monnaie physique dépassée par la numérisation de la société. Toutefois, c'est ignorer son potentiel majeur pour le pouvoir et les inconvénients majeurs pour l'utilisateur individuel.

Pour l'État, le potentiel des monnaies numériques de banque centrale est double. Premièrement, la monnaie numérique de banque centrale a le potentiel d'apporter un contrôle financier total.

D'une part, la généralisation de la monnaie de banque centrale formerait une base légale à partir de laquelle supprimer l'argent liquide. En effet, contrairement au crédit bancaire, la MNBC constituerait une monnaie de base dont il serait aisé de définir le cours légal sur le territoire. On pourrait donc

assister à une disparition progressive des supports physiques de la monnaie.

D'autre part, elle permettrait d'améliorer la surveillance financière et offrirait une possibilité d'intervention supérieure, notamment grâce au traitement automatisé par intelligence artificielle. En particulier, une MNBC faciliterait la collecte de l'impôt, en généralisant le prélèvement direct sur le compte du contribuable. Cet aspect est traité dans la section apparentée du chapitre 9 sur la résistance à la censure.

Deuxièmement, la monnaie numérique de banque centrale possède un potentiel inflationniste non négligeable. D'une part, le remplacement de l'argent liquide permettrait d'éliminer les coûts de production, de distribution et de destruction des supports monétaires (pièces et billets). Cela améliorerait le seigneuriage sur la monnaie de base, en diminuant largement le coût de production. C'est déjà le cas avec la monnaie centrale interbancaire.

D'autre part, le remplacement progressif du crédit bancaire permettrait de récupérer le seigneuriage réalisé sur le crédit par les banques commerciales, comme cela se fait déjà partiellement grâce au taux de refinancement. Cette capture se ferait aux dépens des banques, qui verrait leur capacité à prêter être réduite voire annihilée. C'est pourquoi elles devraient gagner quelque chose au change, par exemple en obtenant à la place un rôle d'intermédiaire dans le système.

Les banques commerciales pourraient être pleinement absorbées par la banque centrale, dont elles deviendraient les succursales. Ainsi, le vieux rêve marxiste de centraliser le crédit entre les mains d'une seule banque serait réalisé [24]. À l'instar de la Gosbank, la banque centrale de l'Union soviétique et seule banque autorisée 1932 et 1987, cette banque unique suivrait les directives du pouvoir central en accordant des prêts financés par création monétaire, non aux emprunteurs solvables, mais aux entités favorisées par la planification économique.

Tout ceci constitue une prospective qui semble peu probable au premier abord. Quand on voit les dangers que crée la généralisation d'un tel système, on peut penser que la population ne pourrait pas accepter cette mutation. Ces systèmes ne sont en effet pas naturellement adoptés par les citoyens, comme en témoigne l'échec de l'eNaira au Nigéria en 2023. En Occident, une réaction de rejet existe, notamment à droite, et des personnalités publiques attachées aux libertés ont déjà affirmé leur opposition, comme le lanceur d'alerte Edward Snowden qui a qualifié cette potentielle monnaie numérique de « monnaie cryptofasciste [25] » en octobre 2021.

L'acceptation promet donc d'être complexe, mais elle est loin d'être im-

possible. Elle pourrait reposer sur des incitations légales encourageant l'utilisation de la MNBC et pénalisant son refus, par la récompense et la punition. La récompense serait constituée de diverses subventions pour encourager l'usage, versées aux commerçants et aux consommateurs, comme cela est déjà fait en Chine dans le cadre du yuan numérique. La punition, qui arriverait dans un second temps, pourrait se composer de l'imposition d'un cours légal qui contraindrait les commerçants à accepter la monnaie numérique centrale, du refus d'accès aux services publics aux personnes ne disposant pas d'un compte à la banque centrale, et de la censure des opinions anti-MNBC, jugées complotistes.

Quoi qu'il en soit, la monnaie numérique de banque centrale repose, comme pour toute mesure étatique, sur l'acceptation de la population générale. L'opinion publique est donc le champ de bataille ici, mais on est en droit d'imaginer que l'État l'emportera au bout d'une période plus ou moins longue, comme il l'a fait avec le papier-monnaie. Dans ce cas, Bitcoin deviendrait la seule porte de sortie monétaire viable pour la résistance.

L'arbitrage juridictionnel

Un concept régulièrement invoqué comme un moyen de protéger sa liberté individuelle face au contrôle de l'État est celui d'« arbitrage juridictionnel », terme calqué sur l'anglais *jurisdictional arbitrage*. Il s'agit, pour une personne, de tirer parti des divergences qui existent entre des juridictions concurrentes pour optimiser ses conditions de vie. La forme la plus simple de cet arbitrage est l'expatriation fiscale qui consiste à émigrer pour bénéficier d'un taux de prélèvement moins élevé. Cette méthode aurait aussi pour conséquence d'inciter les États, par l'effet de la concurrence, à respecter la liberté de leurs citoyens, et serait de ce fait une forme de « vote avec ses pieds ».

L'arbitrage juridictionnel est un phénomène qui a émergé avec la baisse drastique du coût de changement de juridiction ayant eu lieu au cours des siècles passés, par l'assouplissement des restrictions migratoires, la baisse des frais de voyage et l'accroissement de la liquidité des actifs. De plus, la facilitation de la communication liée à l'arrivée d'Internet a amplifié cet effet en fournissant aux individus un moyen de se soustraire partiellement à l'influence de leurs autorités locales. C'est pourquoi cette stratégie est aujourd'hui beaucoup mise en avant.

La notion d'arbitrage juridictionnel a été notamment décrite par les auteurs à succès Rees-Mogg et Davidson dans leur ouvrage *The Sovereign In-*

dividual publié en 1997, dont la thèse principale était de prédire le recul des États-Nations face à l'innovation technique. Ils y formulaient un « théorème d'inéquivalence » qui, en opposition à l'équivalence ricardienne, postulait que les acteurs économiques ne réduiraient pas leur consommation par anticipation d'une hausse d'impôt due à une relance budgétaire, mais changeraient de juridiction :

> « À l'Ère de l'Information, [...] la personne rationnelle ne réagira pas à la perspective d'une augmentation des impôts pour financer les déficits en augmentant son taux d'épargne ; elle déplacera son domicile ou effectuera ses transactions ailleurs. [...] Il faut donc s'attendre à ce que les Individus Souverains et les autres personnes rationnelles fuient les juridictions ayant d'importants engagements non financés [26]. »

Cette vision était également partagée par les cypherpunks, dont beaucoup voyaient le cyberespace émergent comme une juridiction indépendante à part entière, hors d'atteinte de l'État [27]. Ils envisageaient en particulier l'émission d'une cybermonnaie échappant au contrôle des États. C'était le cas d'Eric Hughes, qui confiait au journaliste Kevin Kelly en 1994 :

> « La question la plus importante est la suivante : quelle est l'ampleur des flux monétaires sur les réseaux avant que l'État n'exige la déclaration de chaque petite transaction ? Car si les flux peuvent devenir suffisamment importants, au-delà d'un certain seuil, il pourrait y avoir suffisamment de fonds agrégés pour inciter économiquement un service transnational à émettre une monnaie, et les actions d'un État n'auraient pas d'importance [28]. »

Une des conséquences de l'arbitrage juridictionnel généralisé est l'émergence naturelle d'une monnaie saine. Puisque, dans l'acception naïve du concept, les États sont en concurrence et que les individus peuvent se déplacer librement, ces derniers finiront par favoriser la monnaie la moins taxée, c'est-à-dire celle empêchant le plus le prélèvement involontaire. On pourrait ainsi voir des États émettre une monnaie basée sur l'or, ou sur le bitcoin, pour faire concurrence aux autres devises et bénéficier d'un attrait supplémentaire pour prospérer [29].

Cependant, cette théorie séduisante résiste difficilement à l'épreuve de la réalité, car elle néglige les rapports de domination qui existent entre les États dans le cadre de leur interaction géopolitique. Les États ne sont en effet pas des entités indépendantes : ils sont sans cesse en lutte pour prélever un revenu sur des populations, principalement par leur contrôle du territoire, un conflit qui peut se manifester, au niveau le plus extrême, par la guerre. Ces rapports

de domination s'exercent aujourd'hui au niveau mondial, car la baisse du coût du transport et des télécommunications a non seulement amplifié l'arbitrage juridictionnel, mais a aussi étendu l'interaction des États entre eux.

Cette théorie fait en particulier abstraction d'un phénomène appelé l'impérialisme, qui est la volonté d'un État d'étendre son pouvoir au-delà de ses frontières naturelles, et qui se manifeste actuellement par les actions des États-Unis, de la Russie et de la Chine dans leurs sphères d'influence respectives. En effet, un État qui s'affaiblit en renonçant à une partie de son revenu fiscal (même si la relation n'est pas exactement proportionnelle) devient plus sensible à une ingérence étrangère impérialiste. C'est pour cette raison que la concurrence entre les États est beaucoup moins économique que ce qu'on imagine, celle-ci étant soumise à des interventions politiques comme l'application de sanctions qui restreignent les flux commerciaux, financiers et migratoires vers et depuis l'État concerné.

L'une des facettes de l'impérialisme est l'impérialisme monétaire, qui consiste à favoriser, par la violence ou la menace de violence, l'usage d'une monnaie sur un territoire étranger pour en retirer un avantage [30]. L'avantage visé ordinairement est le revenu de seigneuriage supplémentaire rendu possible grâce à une plus grande utilisation de la monnaie, quelque chose qui est parfois schématisé par l'idée que l'État dominant « exporte son inflation ». C'est précisément ce qu'ont pratiqué les États-Unis avec le dollar depuis le début du xx^{e} siècle, notamment au moyen du système d'étalon de change-or de Bretton Woods.

Il est ainsi illusoire de croire qu'un État dominant puisse tolérer qu'un État sous son influence émette, ou autorise ses citoyens à émettre, une meilleure monnaie utilisable à grande échelle. L'arbitrage juridictionnel ne s'applique ici qu'à la marge, c'est-à-dire dans la mesure où il n'affaiblit pas le pouvoir central de manière significative. La réelle façon de changer les choses dans le domaine monétaire à moyen terme repose sur la désobéissance individuelle.

Les monnaies alternatives centralisées

Face à cet ordre monétaire imposé par la force de façon plus ou moins directe, certaines personnes ont tenté de construire des systèmes alternatifs. Nous ne parlons pas de monnaies locales complémentaires sans ambition ; nous parlons de monnaies dont le but était de représenter un véritable contrepoids à la monnaie étatique. Et les exemples les plus représentatifs de ces réelles alternatives nous viennent des États-Unis.

Les États-Unis possèdent en effet une grande culture des monnaies privées, conformément à l'esprit de liberté individuelle qui les a caractérisés. Pendant la période coloniale et durant la première moitié du XIXe siècle, la frappe privée de pièces était tout à fait autorisée et pratiquée. De même, l'activité bancaire a été relativement libre à partir de 1837, année de fin du mandat de la *Second Bank of the United States*, la banque nationale de l'époque.

Cette liberté monétaire et bancaire a été cependant interrompue par les mesures prises à la suite de la guerre de Sécession. D'une part, une loi du Congrès du 8 juin 1864 a interdit la frappe privée des pièces [31]. D'autre part, les *National Banking Acts* de 1863 et 1864 ont définitivement mis fin à l'horizontalité et l'indépendance des banques.

C'est à cette occasion qu'a été fondé le *Secret Service*, une agence étatique ayant pour mission de lutter contre le faux-monnayage et la fraude financière en général. Créé le 14 avril 1865, le jour de l'assassinat d'Abraham Lincoln, il servait, d'une façon détournée, à affermir le monopole sur la production de monnaie.

Cette transition a été finalisée avec la création de la Réserve Fédérale en 1913 et la prohibition de la détention d'or promulguée par l'ordre exécutif 6102 signé par F.D. Roosevelt le 5 avril 1933.

Après l'abandon de toute référence à l'or dans le système monétaire mondial (et l'abrogation consécutive de l'ordre exécutif en 1975) et le développement d'Internet, l'idée de déployer une monnaie privée est réapparue. Puisque l'État fédéral pouvait gérer arbitrairement sa monnaie, pourquoi ne pouvait-il pas en être autant des individus ? C'est ainsi que des individus ont entrepris, dans une démarche purement hayekienne, de déployer leur propre monnaie sur le marché. Parmi ces projets de monnaie privée, nous pouvons en citer quatre : ALH&Co, le Liberty Dollar, e-gold et Liberty Reserve.

Le premier était ALH&Co, une banque libre offrant la possibilité à ses clients d'avoir des comptes bancaires libellés en or ou en dollars [32]. Cette banque a été créée par Anthony L. Hargis, un libertarien proche de Samuel Edward Konkin et de son idée agoriste. Bien que la banque elle-même faisait toutes les démarches pour rester légale, elle n'empêchait pas l'évasion fiscale. Konkin lui-même a décrit le fonctionnement de ALH&Co dans son ouvrage *Counter-Economics* publié à titre posthume [33].

Les clients pouvaient rédiger des « ordres de transfert » qui fonctionnaient comme des chèques bancaires entre les différentes entreprises qui les reconnaissaient, ou bien les soumettre à ALH&Co et recevoir en retour un chèque bancaire classique ou demander à ALH&Co de payer leurs factures régulières.

ALH&Co a existé pendant près de 30 ans, entre 1976 et 2004, du fait de son caractère confidentiel. À un moment donné, la banque avait 253 clients et utilisait 9 comptes bancaires classiques sur lesquels étaient déposés 7,2 millions de dollars.

En mai 1993, les locaux d'ALH&Co ont subi une descente des agents fédéraux, suite à un signalement de suspicion de blanchiment d'argent lié au trafic de drogue. Les agents se sont emparés des dossiers des clients. Cependant, les opérations d'ALH&Co ont pu continuer pendant une décennie.

Hargis a finalement été inculpé en mars 2004, et ALH&Co a définitivement été fermée. L'IRS a estimé que l'évasion fiscale des clients s'élevait à 24 millions de dollars.

Le deuxième exemple contemporain de monnaie privée aux États-Unis est le Liberty Dollar, une monnaie basée sur l'or et l'argent qu'on pouvait retrouver sous forme de pièces d'argent, de billets représentatifs et, un peu plus tard, d'unités électroniques. Le Liberty Dollar a été créé en 1998 par Bernard von NotHaus via son organisation à but non lucratif NORFED.

Ce système a connu un certain succès, notamment après l'introduction du système de monnaie numérique en 2003. Outre les pièces de monnaies en circulation, les coffres de NORFED contenaient environ 8 millions de dollars en métaux précieux pour assurer la convertibilité de la devise, dont 6 pour garantir l'unité numérique [34].

Toutefois, en septembre 2006, la Monnaie des États-Unis, l'institution en charge de frapper et mettre en circulation les pièces de monnaie américaines, a émis un communiqué de presse, écrit conjointement avec le département de la Justice, dans lequel elle concluait que l'utilisation des « médaillons » de NORFED violait la section 486 du titre 18 du Code des États-Unis et constituait « un crime fédéral [35] ». Le communiqué rappelait également que les pièces frappées ressemblaient au dollar ce qui s'apparentait à de la contrefaçon.

Après une descente du FBI dans les locaux de NORFED en 2007, les violations ont été retenues contre von NotHaus et ses associés, qui ont été arrêtés en 2009 et jugés en mars 2011. En conséquence de ce jugement, les pièces pouvaient être considérées comme de la contrebande et être saisies comme telles. Les ventes de ces pièces ont également été interdites sur eBay en décembre 2012, sous la pression du Secret Service. En 2014, Bernard von NotHaus a été condamné à six mois d'assignation à résidence et à trois ans de liberté conditionnelle.

Le Liberty Dollar n'était pas inconnu des premiers utilisateurs de Bitcoin. Ainsi, Dustin Trammell, l'un des premiers opérateurs de nœud sur le réseau,

s'intéressait à ce système avant de découvrir la monnaie de Nakamoto comme en témoigne son article sur le sujet en décembre 2008 [36].

Le troisième cas de monnaie privée est l'e-gold, une « devise en or numérique » (*digital gold currency*) transférée électroniquement et garantie à 100 % par une quantité équivalente en or conservée en lieu sûr. Le système e-gold a été cofondé par Douglas Jackson et Barry Downey en 1996, deux ans avant PayPal. Douglas Jackson était un oncologue américain vivant en Floride. Adepte de Hayek, il souhaitait créer une meilleure monnaie avec e-gold.

L'e-gold était par essence une monnaie représentative, chaque montant d'e-gold pouvant être converti en or réel. La détention et la conversion d'or était administrée par une société créée pour l'occasion et basée aux États-Unis, *Gold & Silver Reserve Inc.* (G&SR). La société garantissait également de l'e-silver, de l'e-platinum et de l'e-palladium sur le même modèle.

Le système informatique était géré par une deuxième entreprise, *e-gold Ltd.*, enregistrée à Saint-Christophe-et-Niévès dans les Caraïbes. Pour l'époque, il était très performant, mettant à profit un système à règlement brut en temps réel inspiré du virement interbancaire. Le système tirait profit des navigateurs web et en particulier de Netscape, de sorte que chaque client pouvait avoir accès à son compte depuis le site web.

Le système e-gold a rencontré ainsi un grand succès, à tel point qu'il représentait à un moment donné le deuxième système de paiement en ligne mondial derrière PayPal. À son apogée en 2006, il garantissait 3,6 tonnes d'or, soit plus de 80 millions de dollars, traitait 75 000 transactions par jour, pour un volume annualisé de 3 milliards de dollars, et gérait plus de 2,7 millions de comptes.

Toutefois, ce succès fulgurant a été de courte durée. Au terme d'une enquête menée par le Secret Service, Douglas Jackson, ses deux sociétés et ses associés ont été inculpés le 27 avril 2007 par le département de la Justice pour facilitation de blanchiment d'argent et activité de transfert d'argent sans licence.

Jackson a été condamné à 3 ans de liberté surveillée, incluant 6 mois d'assignation à résidence sous surveillance électronique, et à 300 heures de travail communautaire. Ses deux entreprises ont dû payer une amende de 300 000 $. Après une tentative infructueuse d'obtenir une licence, e-gold a dû fermer ses portes définitivement en novembre 2009.

Un indicateur du succès d'e-gold est l'émergence de systèmes similaires de devise en or numérique : nous pouvons citer GoldMoney, fondé par James Turk et son fils en février 2001, qui s'est aujourd'hui adapté aux réglementations

financières ; e-Bullion, fondé par James Fayed en juillet 2001 et fermé en 2008 ; et Pecunix fondé par Simon Davis en 2002, entreprise enregistrée au Panama, qui a fermé ses portes en 2015, dans le cadre d'une escroquerie de sortie. Le Liberty Dollar électronique (eLD) lancé en 2003 ne faisait ainsi que suivre la vague.

Ces devises en or numérique étaient encore utilisées du temps de Bitcoin, de sorte que ses premiers utilisateurs en avaient connaissance. Satoshi Nakamoto lui-même savait bien comment ces systèmes fonctionnaient, comme le montre l'un de ses courriels adressé à la *Cryptography Mailing List* [37]. De même, Ross Ulbricht avait envisagé d'utiliser Pecunix pour Silk Road avant de trouver Bitcoin [38].

Le quatrième et dernier exemple de projet de monnaie privée était le système Liberty Reserve, qui permettait de détenir et de transférer des devises indexées sur le dollar étasunien, sur l'euro ou sur l'or. Le système était la création d'Arthur Budovsky, un Américain d'origine ukrainienne, aux côtés de Vladimir Kats. En 2006, Budovsky s'est expatrié au Costa Rica, qui était alors considéré comme un paradis fiscal facilitant le blanchiment d'argent, où il a enregistré sa société, Liberty Reserve S.A.

L'inculpation d'e-gold en avril 2007 a grandement profité à Liberty Reserve qui a pu prendre la relève. Le système a ainsi rencontré un grand succès. En mai 2013, l'acte d'accusation du département de la Justice étasunienne estimait que Liberty Reserve possédait plus d'un million d'utilisateurs dans le monde, dont plus de 200 000 aux États-Unis, et traitait 12 millions de transactions financières annuellement, pour un volume combiné de plus de 1,4 milliards de dollars.

Toutefois, ce succès s'est accompagné de complications sérieuses. En 2009, la *Superintendencia General de Entidades Financieras* (SUGEF) costaricaine s'est intéressée au cas de Liberty Reserve, lui demandant d'obtenir une licence (chose qu'elle n'est pas parvenue à faire). En mars 2011, une enquête a été ouverte. En novembre 2011, le FinCEN a délivré à son tour un avis selon lequel LR était « utilisée par les criminels pour effectuer des transactions anonymes [39] ».

La fin de Liberty Reserve a été retentissante, au terme d'une opération coordonnée de manière internationale. Le 24 mai 2013, Arthur Budovsky et les principaux gestionnaires de Liberty Reserve ont été inculpés et arrêtés, dans des juridictions différentes : en Espagne, aux États-Unis et au Costa Rica. Après environ un an et demi de détention, en octobre 2014, Arthur Budovsky a été extradé de l'Espagne vers New York aux États-Unis, où s'est

déroulé son procès. En 2016, Arthur Budovsky a finalement plaidé coupable pour blanchiment d'argent, et a été condamné à 20 ans de prison ferme.

Liberty Reserve a probablement été la dernière monnaie libre centralisée de grande envergure sur Internet. Le système était encore massivement utilisé lorsque Bitcoin faisait ses premiers pas. Liberty Reserve a ainsi été utilisé pour acheter du bitcoin sur les toutes premières plateformes de change, y compris sur la fameuse plateforme Mt. Gox !

Si l'on tente de récapituler, il est *de facto* interdit de fournir des services bancaires sans licence (ALH&Co), de frapper ses propres pièces de monnaie et d'imprimer ses propres billets (Liberty Dollar), ou de gérer des comptes électroniques en or (e-gold) ou dans la devise nationale (Liberty Reserve), dans la mesure où cela fait concurrence à l'État. Bien qu'il y ait des raisons multiples aux fermetures de ces systèmes, on ne peut que constater que toutes les alternatives sérieuses au système monétaire étatique ont été éliminées [40].

Le monopole monétaire est souvent imposé subtilement excluant les concurrents potentiels du marché par des lois liées à la contrefaçon ou au blanchiment d'argent. C'est pour cette raison qu'il n'y a aujourd'hui aucune alternative légale. C'est pourquoi les innovations dans le domaine financier, comme PayPal ou GoldMoney, se sont conformées aux réglementations existantes : pour survivre [41].

L'intervention étatique est là pour s'immiscer dans le système monétaire et le contrôler, en détruisant au besoin les alternatives. C'est pour résister à cette force inouïe que Bitcoin a été conçu tel qu'il existe aujourd'hui.

Bitcoin contre l'État

L'État est ainsi l'incarnation organisée, territorialisée et institutionnalisée du transfert de richesse non consenti. En tant que tel, le contrôle sur la monnaie constitue logiquement un élément qu'il revendique comme sa prérogative, d'autant plus qu'il en tire un revenu, appelé le seigneuriage. Au fil du temps, ce contrôle sur la monnaie est devenu de plus en plus pernicieux, et il s'est accéléré avec l'émergence de la banque durant la Renaissance. L'usage des billets de banque a progressivement été récupéré par l'État au moyen d'une banque centrale, qui s'est arrogé le monopole exclusif sur leur production, jusqu'à les transformer en papier-monnaie. De même, l'usage des dépôts bancaires, qui est aujourd'hui surveillé et contrôlé minutieusement, pourrait être repris dans un futur proche par l'État par le biais de la monnaie numérique de banque centrale.

À moyen terme, il est illusoire de croire que l'État renoncera à son prélèvement, ou même le rendra plus transparent : il faudrait pour cela que ses bénéficiaires demandent eux-mêmes cette transition. On pourrait croire qu'un petit État aurait la possibilité et l'intérêt géostratégique de le faire, mais ce serait ignorer les velléités impérialistes des puissances dominantes. Il ne suffit donc pas de faire tourner un serveur dans une juridiction accommodante pour gérer une monnaie numérique comme l'a montré le cas de Liberty Reserve.

C'est pourquoi Bitcoin est comme il est. Il est spécifiquement conçu pour résister à l'intervention de l'État et constitue une tentative de construire une alternative robuste au système monétaire actuel. Bitcoin résout cette problématique en distribuant le fonctionnement du système au sein d'un réseau pair-à-pair de nœuds. Cette distribution à égalité permet de partager les risques entre les personnes qui s'en occupent, et de faire en sorte que la sécurité du système repose sur leurs actions économiques combinées plutôt que sur celle d'un seul individu ou d'une seule entreprise.

5

Un mouvement technologique

Bitcoin est un objet technique et doit être pensé en tant que tel. La technique (du grec ancien τέχνη, « habileté », « art », « métier ») est l'ensemble des procédés pratiques issus du savoir humain employés en vue d'atteindre des objectifs concrets, le plus souvent de manière reproductible. Ces procédés peuvent tout aussi bien intervenir dans la fabrication de produits manufacturés que dans la réalisation de services. Ils permettent aussi de construire des biens intermédiaires, appelés outils, servant à produire d'autres biens et services.

L'évolution technique fait partie intégrante de l'histoire du monde, ayant modifié les rapports humains en profondeur à de multiples reprises. Les innovations techniques majeures coïncident en effet avec les grandes mutations historiques : la maîtrise de la métallurgie avec le développement des premières civilisations, l'émergence de l'imprimerie avec la réforme protestante, la révolution industrielle avec l'urbanisation et la planification. À notre époque, le développement des ordinateurs et leur mise en réseau est en train de transformer notre culture comme jamais auparavant.

L'enjeu politique est donc plus que jamais *technologique*, dans le sens où l'étude de la technique devient nécessaire pour appréhender correctement les rapports de domination. Il s'agit essentiellement de choisir quels procédés employer et comment en faire usage. En particulier, cet enjeu est aujourd'hui au centre d'une opposition entre l'individu et l'État, entre la liberté et l'autorité, entre l'émancipation et l'oppression.

En tant qu'assemblage de procédés, Bitcoin s'inscrit pleinement dans cette opposition technique. La guerre pour le contrôle sur la monnaie se transpose de plus en plus dans le monde numérique, avec le développement de la MNBC et l'essor de la cryptomonnaie. Nous nous ne vivons plus à l'heure des pièces de métaux précieux ou des billets de banque (qui conservent malgré tout une certaine utilité), mais à l'époque de la monnaie numérique, bien plus adaptée à nos moyens de communication et d'échange économique modernes. Satoshi en était conscient quand il déclarait dès novembre 2008 que Bitcoin pourrait permettre de « remporter une bataille majeure dans la course aux armements » et de « conquérir un nouveau territoire de liberté pour plusieurs années ».

Dans ce chapitre, nous nous proposons de revenir sur les évolutions techniques et les idées politiques apparentées qui ont amené Bitcoin à exister. Dans un premier temps, nous nous efforcerons de décrire comment la cryptographie, l'ordinateur et Internet ont modifié nos façons de communiquer. Puis, dans un second temps, nous nous concentrerons sur les mouvements des libristes, des extropiens et des cypherpunks, qui ont formé le terreau techno-idéologique au sein duquel Bitcoin a germé.

La cryptographie symétrique et l'ordinateur

Bitcoin est avant tout basé sur la communication, c'est-à-dire le fait de transmettre des informations à autrui. Cette communication a longtemps été restreinte géographiquement, du fait des limitations techniques qui caractérisaient les sociétés pré-industrielles. L'échange avec le lointain était très rare, ce qui expliquait l'existence de langues et de cultures distinctes.

Toutefois, l'évolution technique a modifié cet état des choses. À partir de la moitié du XIX^e^ siècle, la télécommunication, ou la transmission d'information à distance, a connu un bond prodigieux. Ceci s'est fait d'abord grâce à l'apparition du télégraphe électrique, qui permettait d'envoyer et de recevoir des messages écrits (ou télégrammes) d'une manière rapide et fiable. Puis elle s'est renforcée avec l'arrivée du téléphone, qui donnait la possibilité de transférer des paroles à distance. En outre, la radiocommunication, basée sur l'usage des ondes radioélectriques pour partager de l'information, a rendu ces techniques beaucoup plus pratiques. Il est ainsi devenu possible de communiquer rapidement d'un continent à l'autre, chose qui a notamment profité aux États, qui pouvaient désormais gérer leurs territoires éloignés d'une manière plus fluide et centralisée.

Cette évolution de la télécommunication a considérablement accru le be-

soin de sécuriser l'information transmise, afin d'éviter qu'elle soit interceptée par l'ennemi lors d'une guerre par exemple. C'est pourquoi la cryptographie, qui existait depuis l'Antiquité, a connu un essor sans précédent au cours du XX^e siècle.

La cryptographie est la discipline mathématique qui a pour but la sécurisation de la communication en présence de tiers malveillants. À l'origine, il s'agit de dissimuler de l'information par une méthode de chiffrement, ce qui explique le mot, qui vient du grec ancien κρυπτός, kruptós (« caché ») et de γράφειν, gráphein (« écrire »). Par la suite, la cryptographie s'est étendue à l'authentification de messages avec la signature numérique et à la vérification de données par l'intermédiaire des fonctions de hachage. En résumé, cette discipline permet d'assurer la confidentialité (chiffrement), l'authenticité (signature) et l'intégrité (hachage) de l'information transmise.

La cryptographie porte en elle la notion d'adversaire ou d'antagoniste (de l'anglais *adversary*) qui est une entité malveillante dont le but est d'empêcher les utilisateurs d'un cryptosystème de réaliser leurs objectifs. Il n'y a en effet pas besoin de cacher, d'authentifier ou de vérifier quoi que ce soit en l'absence d'une menace externe. C'est pour cette raison que le chiffrement et son pendant, la cryptanalyse, ont été développés en premier lieu par et pour les États.

Le chiffrement est un procédé permettant de rendre impossible la compréhension d'un message pour les personnes qui ne disposent pas d'une information spécifique, appelée la clé de déchiffrement. La cryptanalyse est la technique visant à déduire un texte en clair à partir d'un message chiffré sans disposer de la clé.

À l'origine, le chiffrement se fait uniquement de manière symétrique, c'est-à-dire que la clé de chiffrement et de déchiffrement sont les mêmes et que les deux parties doivent avoir connaissance de cette clé secrète pour communiquer. L'exemple typique de chiffrement symétrique est le code de César, ou chiffrement par décalage, qui est l'une des méthodes les plus simples et les plus connues pour chiffrer un texte. Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet. La clé est alors le nombre correspondant au décalage. Par exemple, un décalage de 21 lettres vers la droite transforme le mot « bitcoin » en « wdoxjdi ». Cette méthode tient son nom du fait que Jules César l'utilisait dans ses correspondances secrètes.

Le chiffrement symétrique pose néanmoins un problème logistique. La clé doit en effet être transmise entre les deux parties qui communiquent et

peut donc être interceptée. De plus, le nombre de clés à partager augmente de manière exponentielle en fonction du nombre de personnes impliquées (3 clés pour 2 personnes, 6 pour 3, 10 pour 4, etc.), ce qui multiplie considérablement les risques. C'est ce qui explique pourquoi l'apparition du chiffrement asymétrique, qui permettait de s'affranchir de cette contrainte, a constitué une innovation.

Le développement du chiffrement a motivé la conception de machines de plus en plus perfectionnées. Le chiffrement correct d'un message à la main pouvait prendre des heures, de sorte que l'utilisation d'un automate devenait pertinente. Après la Première Guerre mondiale, durant laquelle la cryptologie avait joué un rôle clé notamment avec l'affaire du télégramme Zimmermann, les premières machines de chiffrement sont ainsi apparues à l'instar de la machine Enigma et des machines de Lorentz utilisées par l'Allemagne.

Au cours de la Seconde Guerre, le besoin de cryptanalyse a poussé les belligérants à construire des machines à calculer programmables spécialisées, pouvant évaluer un grand nombre de possibilités dans un contexte précis. La Bombe de Turing et le Colossus ont ainsi été fabriqués par les services de cryptanalyse britanniques afin de casser les codes allemands. En parallèle, d'autres calculateurs (appelés *computers* en anglais) ont été développés dans le but de calculer les trajectoires balistiques. C'était le cas de la machine Zuse Z3 en Allemagne ou de l'*Atanasoff–Berry Computer* aux États-Unis. Le premier ordinateur au sens moderne du terme (Turing-complet, entièrement électronique, à mémoire enregistrée) a été l'ENIAC, qui a été conçu en 1945 par des ingénieurs de la *Moore School of Electrical Engineering* et dont l'architecture a été reprise en 1948 par le mathématicien américain John von Neumann.

Après la Seconde Guerre mondiale, les ordinateurs sont devenus progressivement plus efficaces grâce à l'invention du transistor (1947), du circuit intégré (1958) et du microprocesseur (1971). Ceci a débouché, au cours des années 1970, sur l'apparition de l'ordinateur personnel (*personal computer*), un ordinateur destiné à l'usage d'une personne et dont les dimensions sont assez réduites pour tenir sur un bureau. L'exemple le plus célèbre est sans doute l'Apple II, conçu par Steve Wozniak et sorti en 1977 qui est le premier ordinateur personnel fabriqué à grande échelle.

La développement des ordinateurs a naturellement coïncidé avec l'élaboration des premiers langages de programmation, compilés et interprétés : le FORTRAN est apparu en 1957, le LISP en 1958, le COBOL en 1959, le BASIC en 1964, et le C en 1972. Le langage C++, dans lequel Satoshi Nakamoto

a écrit la première version du logiciel de Bitcoin, a fait son apparition plus tard, en 1985. Cette évolution a entraîné la démocratisation de la programmation informatique. Elle a aussi marqué le début de la sous-culture des *hackers*, axée sur la compréhension approfondie des systèmes informatiques et sur le détournement de leur rôle prédéfini.

Les systèmes d'exploitation standards ont été conçus à partir des années 1970. Unix a été présenté par AT&T au public pour la première fois en 1973. DOS, l'ancêtre de Windows, a été créé en 1981. Le Système 1 d'Apple, adapté à ses ordinateurs Macintosh, a été lancé en 1984. Le système libre GNU/Linux a quant à lui été créé en 1991.

L'apparition de la cryptographie moderne

La deuxième avancée majeure dans l'histoire technique qui a mené à Bitcoin est l'apparition de la cryptographie moderne regroupant le chiffrement asymétrique, la signature numérique et le hachage de données. L'utilisation de plus en plus répandue des ordinateurs, notamment au sein des universités américaines, a poussé les cryptographes à imaginer des méthodes plus gourmandes en puissance de calcul, mais bien plus efficaces pour le chiffrement. La percée a été réalisée en 1976 lorsque les chercheurs Whitfield Diffie et Martin Hellman ont publié un article scientifique, intitulé *New Directions in Cryptography*, dans lequel ils décrivaient un algorithme d'échange de clés (destiné à la transmission des clés secrètes pour le chiffrement symétrique) ainsi qu'un procédé de signature électronique. L'introduction commençait comme suit :

> « Nous sommes aujourd'hui à la veille d'une révolution dans le domaine de la cryptographie. Le développement de matériel numérique bon marché a permis de s'affranchir des limites de conception de l'informatique mécanique et de ramener le coût des dispositifs cryptographiques de haute qualité à un niveau tel qu'ils peuvent être utilisés dans des applications commerciales telles que les distributeurs de billets distants et les terminaux d'ordinateurs. À leur tour, ces applications créent un besoin pour de nouveaux types de systèmes cryptographiques qui minimisent la nécessité de sécuriser les canaux de distribution des clés et fournissent l'équivalent d'une signature écrite. Dans le même temps, les développements théoriques de la théorie de l'information et de l'informatique promettent de fournir des cryptosystèmes dont la sécurité est prouvée, transformant ainsi cet art ancien en science [1]. »

S'ils ont été les premiers à publier ces méthodes, ils n'ont pas été les seuls à faire ces découvertes au cours de la période. Clifford Cocks, James

Ellis et Malcolm Williamson avaient déjà mis au point un tel cryptosystème quelques années plus tôt (qu'ils appelaient le « chiffrement non secret ») pour le compte du GCHQ britannique, mais leurs recherches sont restées classifiées. Le cryptographe Ralph Merkle avait également décrit l'échange de clés de Diffie et Hellman dans un article écrit en 1974 et publié en 1978 par l'intermédiaire de ce qu'on appelle les puzzles de Merkle.

L'avancée de Diffie et Hellman a marqué le début de la cryptographie asymétrique, ou cryptographie à clé publique, une discipline qui regroupe le chiffrement asymétrique et la signature numérique. Dans un système asymétrique, deux clés se distinguent : une clé privée, censée rester secrète, et une clé publique, dérivée de la clé privée. La clé privée ne peut pas être retrouvée facilement à partir de la clé publique, ce qui fait que cette dernière peut être partagée à tous en toute quiétude.

Le chiffrement asymétrique consiste à utiliser la clé publique comme une clé de chiffrement et la clé privée comme une clé de déchiffrement. Le destinataire génère une paire de clés, garde la clé privée pour lui et partage la clé publique à son interlocuteur pour qu'il lui envoie des messages. Le fonctionnement de ce chiffrement est ainsi analogue à celui d'une boîte aux lettres que le destinataire utilise pour recevoir des lettres et dont lui seul possède la clé.

La signature numérique quant à elle, repose sur le fait d'utiliser la clé privée comme une clé de signature et la clé publique comme clé de vérification. L'expéditeur signe un message à l'aide de la clé privée et l'envoie à son interlocuteur, qui peut vérifier son authenticité en utilisant la clé publique.

Le système cryptographique asymétrique le plus connu a été conçu juste après la publication du papier de Diffie et Hellman : il s'agit de l'algorithme de chiffrement RSA, créé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman et breveté par le MIT en 1983. Celui-ci se base sur des opérations algébriques et sa sécurité provient de la difficulté à décomposer de très grands nombres en facteurs premiers. Il permet de chiffrer un message pour l'envoyer à quelqu'un, mais aussi (grâce à l'interversion des rôles des clés) de signer électroniquement ce message pour le publier. Cet algorithme est encore aujourd'hui utilisé très largement sur Internet, et en particulier dans le commerce électronique.

Du côté du chiffrement, d'autres algorithmes ont été conçus par le suite. C'était le cas de l'algorithme de chiffrement d'ElGamal qui a été présenté par Taher ElGamal en 1984, et dont la fiabilité reposait sur le problème du logarithme discret, c'est-à-dire la difficulté mathématique à retrouver l'exposant

d'un élément dans un groupe cyclique fini [2].

Du côté de la signature, des algorithmes destinés à servir uniquement à cet usage ont été également développés. C'était le cas du modèle d'ElGamal, qu'il a présenté en même temps que son système de chiffrement en 1984, du schéma de signature de Schnorr, conceptualisé par Claus-Peter Schnorr en 1991, et du *Digital Signature Algorithm* (DSA), conçu la même année par le NIST. Tous les trois se basaient aussi sur le problème du logarithme discret.

La cryptographie sur courbes elliptiques est apparue en 1985 grâce aux contributions indépendantes de Neal Koblitz et de Victor Miller. Elle a amené un bon nombre d'innovations, dont le procédé d'échange de clés ECDH et l'algorithme de chiffrement hybride ECIES. Le schéma de signature ECDSA, qui est l'algorithme principal utilisé dans Bitcoin pour autoriser les transferts, a été créé en 1992.

La cryptographie asymétrique ouvrait également la voie aux fonctions à sens unique, des fonctions dont le calcul d'une image est facile mais dont l'obtention d'un antécédent est difficile. En effet, les systèmes de chiffrement à clé publique pouvaient former eux-mêmes des fonctions de ce type. De ce fait, la recherche dans la découverte de telles fonctions s'est développée à partir de cette base.

On a assisté en particulier au développement des premières fonctions de hachage cryptographiques, dont les premiers modèles datent de la fin des années 1970. Ces fonctions avaient pour particularité de transformer un message de taille variable en une empreinte de taille fixe. Entre 1989 et 1991, plusieurs algorithmes de hachage (MD2, MD4, MD5) ont été conçus par Ronald Rivest pour le MIT. Puis, l'algorithme SHA-0 a été créé en 1993 et SHA-1 en 1995. La suite d'algorithmes SHA-2, qui incluait le fameux SHA-256 largement utilisé dans Bitcoin, a été publiée en 2001.

En parallèle, les idées pour l'utilisation de ces fonctions de hachage ont fleuri. Ces dernières permettaient de garantir l'intégrité de l'information de façon à ce que tout changement soit détecté en sortie. En 1979, Ralph Merkle a mis au point les arbres de hachage qui permettaient d'authentifier un ensemble volumineux de données, auxquels il a donné son nom. Ces arbres ont également été inclus dans la conception originelle de Bitcoin [3].

L'usage civil de la cryptographie

Ces découvertes de la cryptographie moderne ont inspiré les esprits libres, qui ont tout de suite imaginé les applications qui pouvaient en découler. En

quelques années, un vaste domaine d'études venait d'être ouvert dans le monde civil, et beaucoup d'individus allaient s'y engouffrer.

C'était le cas de David Chaum, informaticien et cryptographe américain, né en 1955 dans une famille juive à Los Angeles et étudiant à l'université de Californie à Berkeley, qui s'est vite pris de passion pour la protection de la vie privée. À partir de 1979, ce dernier a contribué de manière primordiale au monde de la cryptographie par la publication d'articles fondateurs. En 1981, il publiait l'article *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* [4], où il décrivait les bases de la communication anonyme au travers de réseaux de mélange (*mix networks*), qui serait notamment utilisée par les services de relai de courriel (Mixmaster) et par les réseaux anonymes Tor, I2P et Freenet. En 1982, il décrivait le procédé de signature aveugle, qui permettait notamment de mettre en place une monnaie électronique anonyme [5], que Chaum mettrait en œuvre quelques années plus tard via sa société DigiCash, ainsi que l'émission de certificats automatiques, utilisée par exemple dans ZeroLink aujourd'hui. Durant la même année, il a également publié sa thèse de doctorat écrite en 1979, qui présentait un système de coffres cryptographiques ayant pour but d'arriver à un consensus au sein d'un ensemble d'acteurs ne se faisant pas confiance. En 1985, il a publié un protocole permettant de résoudre le problème du dîner des cryptographes en garantissant l'anonymat de l'auteur d'un message partagé au sein d'un groupe [6].

David Chaum était obsédé par la protection de la vie privée, qu'il estimait être en danger. Même si cette obsession n'atteignait pas la radicalité des cypherpunks (dont il en était un précurseur), il n'en restait pas moins qu'il était très inquiet pour l'avenir de la liberté et de la confidentialité dans la société informatisée. En juillet 1995, il déclarait ainsi devant la Chambre des représentants des États-Unis :

> « Les "techniques de protection de la vie privée" permettent aux individus de protéger leurs propres informations et leurs intérêts, tout en assurant un niveau de sécurité très élevé aux organisations. Il s'agit essentiellement de faire la différence entre, d'une part, un système centralisé dans lequel les participants sont privés de leurs droits (comme des animaux marqués électroniquement dans des fermes d'engraissement) et, d'autre part, un système dans lequel chaque participant est en mesure de protéger ses propres intérêts (comme les acheteurs et les vendeurs sur une place de marché) [7]. »

Un autre exemple était Philip Zimmermann, informaticien et cryptographe américain originaire de Philadelphie et ayant fait ses études en Floride. Activiste politique opposé aux armes nucléaires, il avait travaillé pour la *Nuclear*

Weapons Freeze Campaign à Boulder dans le Colorado. Passionné par les énigmes et les secrets, il a découvert l'existence de la cryptographie asymétrique par le biais d'un article de Martin Gardner [8]. Il a publié un article dans la revue *IEEE Computer* en 1986 sur RSA avant de concevoir PGP.

PGP (de l'anglais *Pretty Good Privacy*) était un logiciel de chiffrement hybride, qui se basait sur RSA pour l'échange de clés et sur un algorithme de chiffrement symétrique pour la communication. Il permettait aussi de générer des signatures. Il était spécialisé dans l'échange de courriels [9].

Le 5 juin 1991, Phil Zimmermann en a publié la version 1.0 sous licence libre. Dans le manuel d'utilisation il expliquait sa démarche :

> « Si la confidentialité est interdite, seuls les hors-la-loi en bénéficieront. Les agences de renseignement ont accès à des techniques cryptographiques performantes. Il en va de même pour les grands trafiquants d'armes et de drogue, ainsi que pour les entreprises de défense, les compagnies pétrolières et les autres géants de l'industrie. En revanche, les citoyens ordinaires et les associations politiques locales n'ont généralement pas accès à des techniques de cryptographie à clé publique "de qualité militaire" à un prix abordable. PGP permet aux gens de prendre en main leur vie privée. La société en a de plus en plus besoin. C'est pourquoi je l'ai conçu [10]. »

Il a diffusé la première version de PGP depuis les États-Unis par l'intermédiaire d'Internet ce qui fait que, en raison de la nature internationale du réseau, le logiciel de chiffrement est rapidement devenu disponible dans le monde entier. En faisant cela, Zimmermann était conscient qu'il risquait d'attiser une réponse du pouvoir : la Réglementation américaine sur le trafic d'armes au niveau international (*International Traffic in Arms Regulations* ou ITAR) considérait en effet les produits cryptographiques comme des « munitions » et en interdisait l'exportation sans licence. En février 1993, alors que PGP commençait à se populariser, une enquête contre Zimmermann a par conséquent été ouverte par l'État fédéral. Heureusement cette enquête a été abandonnée quelques années plus tard, notamment suite à la réaction des cypherpunks, dont Zimmermann est toutefois resté à l'écart (à l'instar de Chaum).

Enfin, les scientifiques Stuart Haber et Scott Stornetta ont aussi été inspirés par ces découvertes. Stuart Haber était cryptographe et informaticien, Scott Stornetta était physicien et chercheur. Les deux hommes se sont rencontrés dans les locaux de Bell Communications Research (« Bellcore »), un consortium de recherche et développement dans la télécommunication pour lequel ils travaillaient.

Ils ont conceptualisé le premier système d'horodatage de documents dans l'article *How to time-stamp a digital document* publié en 1991, et qui a plus tard été cité au sein du livre blanc de Bitcoin [11]. Il s'agissait d'appliquer une fonction de hachage (par exemple MD4) à un document numérique et de publier l'empreinte résultante dans un registre public, de sorte à prouver l'existence du document à une date donnée. Ils ont mis leur idée en application par la publication d'empreintes dans les petites annonces du New York Times à partir de 1992. Ils ont ensuite créé leur propre société en 1994, Surety Technologies, dans le but de se consacrer pleinement à cette activité. Ils sont ainsi connus pour avoir créé la première chaîne temporelle d'horodatages, préfigurant la chaîne de blocs de Bitcoin, en incluant l'empreinte précédente dans le calcul de la nouvelle empreinte à publier dans le journal [12].

De manière générale, tous ces individus ont, par leur compréhension de la cryptographie asymétrique, largement préfiguré les cypherpunks. Ces derniers ont été cependant bien plus loin en radicalisant les idées politiques qu'esquissaient ces techniques mathématiques.

L'émergence d'Internet et le partage de données

Avec l'émergence des ordinateurs est venue la volonté de les connecter en réseau. C'est ainsi que les premiers réseaux informatiques se sont formés dans les années 50. Mais ces réseaux n'étaient pas interconnectés. Pour cela, il a fallu attendre un effort public et ouvert, qui a été fait à partir des années 70, par l'intermédiaire du développement du réseau des réseaux international : Internet.

L'idée derrière Internet était de transmettre des paquets de données (et plus spécifiquement des datagrammes) par le biais d'une technique nommée la commutation de paquets, initialement décrite en 1964 par l'informaticien polono-américain Paul Baran [13]. Cette technique consistait à indiquer la destination dans l'en-tête des paquets de sorte à ce qu'il puissent être relayés sur le réseau, notamment au moyen de routeurs. Elle s'opposait à la commutation de circuits, qui reposait sur une liaison déterminée entre l'expéditeur et le destinataire pour transmettre les données. À l'époque, les communications transitaient au travers des lignes téléphoniques au moyen d'un modem.

Le premier réseau d'Internet tire son origine dans la recherche militaire. Il s'agissait du réseau ARPANET, conçu par l'ARPA, une agence de recherche technique rattachée au département de la Défense [14]. Le but était de développer un réseau de communication qui puisse résister aux attaques nucléaires dans le cadre de la Guerre froide. Par la suite, d'autres réseaux se sont développés

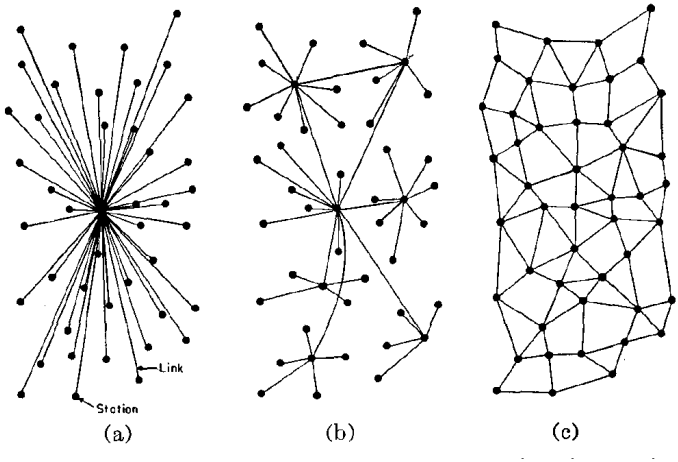

FIGURE 5.1 – Réseaux : (a) centralisé ; (b) décentralisé ; (c) distribué. (Paul Baran, « *On Distributed Communications Networks* », 1964)

de manière similaire dans le monde militaro-universitaire comme le réseau du NPL au Royaume-Uni, le Merit Network aux États-Unis ou le réseau Cyclades en France.

Le concept proprement dit d'Internet est apparu en 1974, avec l'émergence d'une suite de protocoles facilitant l'interconnexion des réseaux : la suite TCP/IP [15]. Ces protocoles permettaient de standardiser la communication des paquets. La standardisation a été finalisée avec la publication de la version 4 de IP et de la version 4 de TCP en 1981, et avec leur intégration dans ARPANET (le réseau fédérateur d'Internet) en 1983. En 1985, a été créé le NSFNET, qui a rapidement pris de l'ampleur, à tel point qu'il a remplacé ARPANET en tant que réseau fédérateur. Le projet ARPANET a été officiellement mis hors service en 1990. Mais on pouvait considérer qu'Internet était alors lancé.

Internet a provoqué un choc sans précédent sur la possibilité de diffusion des informations. Toutefois, son développement et son adoption ont été progressifs, à mesure que les gens estimaient son potentiel et son utilité. Cette croissance est passée par l'apparition de cas d'utilisation diverses qui ont amené de plus en plus de gens à utiliser le réseau des réseaux.

Le courrier électronique a été la première application d'Internet. Au début, il s'agissait d'envoyer des textes par l'intermédiaire du protocole FTP, puis des protocoles spécifiques ont été développés dans les années 80. Le premier courriel a été envoyé en 1971. Les listes de diffusion sont également apparues

rapidement avec le développement de logiciels permettant d'envoyer le même message à un ensemble de personnes. Le logiciel LISTSERV est ainsi sorti en 1986, Majordomo en 1992, GNU Mailman en 1999.

Un autre cas d'utilisation est l'émergence de forums de discussions, qui permettaient aux gens de discuter publiquement de sujets spécifiques. Usenet, un réseau de forums de discussion, a ainsi été lancé en 1980 et est devenu entièrement compatible avec Internet en 1986. L'utilisateur y accédait par un logiciel appelé un lecteur de nouvelles. Usenet a été très populaire à la fin des années 80 et au cours des années 90, notamment grâce aux universités. C'est de Usenet que provient le concept de « septembre éternel », qui fait référence au mois de septembre 1993, durant lequel de nombreux nouveaux utilisateurs étaient arrivés, faisant drastiquement baisser la qualité du discours, tant au niveau du fond que de la forme [16]. Usenet a été la cause du développement des premiers fournisseurs d'accès à Internet (FAI), qui permettaient à leurs clients d'y accéder sans restrictions, sans matériel nécessaire, contre le paiement d'un abonnement. Notons enfin que Usenet a été cité par Satoshi Nakamoto dans le livre blanc de Bitcoin et dans plusieurs de ses messages, ce qui témoigne de son influence dans la cyberculture.

C'est également à cette époque qu'est apparu le protocole de communication textuelle IRC (pour *Internet Relay Chat*), qui permettait à des individus d'échanger des messages en temps réel.

Mais l'évènement vraiment déterminant dans le développement d'Internet a été l'arrivée du Web, qui a réellement encouragé l'afflux du grand public. Celui-ci a été conçu en 1989 par le chercheur Tim Berners-Lee pour le compte du CERN, qui a été aidé par l'ingénieur Robert Cailliau pour en définir les spécificités. Le modèle a été finalement rendu public en août 1991.

Le World Wide Web, abrégé communément en Web, et parfois appelé « la Toile » en français, est un système hypertexte public fonctionnant sur Internet, c'est-à-dire un système permettant de passer d'une page à l'autre (via des hyperliens) sans devoir revenir à la racine. Même si l'idée n'était pas nouvelle (le concept d'hypertexte avait été inventé par Ted Nelson en 1965, dans le cadre de son projet Xanadu), le Web innovait par trois caractéristiques : les adresses sous forme d'URL, le protocole de communication HTTP, et le langage informatique HTML.

L'accès à la Toile se faisait par le biais d'un navigateur Web développé par Berners-Lee, baptisé WorldWideWeb, qui ne constituait guère plus qu'une preuve de concept. Ainsi, le Web n'a vraiment décollé que grâce aux navigateurs Mosaic, créé en 1993, et surtout Netscape, conçu en 1994. Le Web a

engendré un engouement sans précédent, notamment grâce à l'idée du commerce électronique. Cela a finalement abouti à une bulle financière appelée la bulle Internet (que les anglophones nomment la *dot-com bubble*), qui a éclaté en mars 2000.

Les années 2000 ont aussi été marquées par le développement du partage de fichiers en pair-à-pair. En 1999, Napster permettait de partager de la musique avec d'autres utilisateurs. Néanmoins, il reposait sur un serveur central pour référencer les fichiers, ce qui l'a contraint à fermer en 2001 sous la pression de la RIAA, l'association représentant l'industrie du disque aux États-Unis.

Afin de résoudre ce problème, des protocoles purement pair à pair sont apparus. Il s'agissait de créer un réseau où tous les ordinateurs (appelés nœuds) possédaient le même niveau de privilège, par opposition au modèle client-serveur, de sorte qu'il n'y ait plus de point de défaillance unique à attaquer pour faire cesser le partage. C'était le cas de Gnutella et de eDonkey, tous deux créés en 2000. Mais surtout c'était le cas de BitTorrent, dont la première version a été publiée en 2001 [17]. Ces protocoles formaient une alternative beaucoup plus fiable puisqu'il fallait poursuivre chaque utilisateur individuellement, ce qui représentait une charge considérable pour l'État.

Une dernière innovation a été le routage en ognon qui venait ajouter de la confidentialité dans la transmission de données. Le routage en ognon a été inventé en 1996 par Paul Syverson, aux côtés de David Goldschlag et Michael Reed, pour le compte du *Naval Research Laboratory*, un laboratoire de recherche rattaché à la Navy [18]. Les trois hommes avaient pour mission de construire un réseau de mélange pour protéger les communications des agences étasuniennes. La mise en œuvre de cette technique a été réalisée quelques années plus tard, par le biais du réseau Tor, dont le nom est l'acronyme de *The Onion Router* et qui a été lancé en 2002 grâce à une subvention de la DARPA. Il a été rendu public en 2003, afin d'agrandir l'ensemble d'anonymat dans lequel pouvaient se fondre les communications fédérales. Cela avait l'avantage de créer un réseau anonyme dans lequel pouvaient œuvrer les hors-la-loi.

Internet, et plus particulièrement le partage de pair à pair et le routage en ognon, semblaient donner la possibilité aux gens de continuer leurs activités malgré la réticence des autorités en charge, de sorte qu'elles ont inspiré la conception originelle de Bitcoin. Par son architecture distribuée, le réseau permettait de répartir les risques pour ne pas subir une attaque qui puisse mettre le système à genoux. Satoshi écrivait ainsi dans son courriel du 6 novembre 2008 :

« Les États sont bons pour couper les têtes des réseaux contrôlés de manière cen-

> tralisée comme Napster, mais les réseaux purement pair à pair comme Gnutella et Tor semblent tenir le coup [19]. »

La philosophie du logiciel libre

La possibilité de diffusion des informations apportée par l'émergence d'Internet a remis au goût du jour la critique à l'encontre de la « propriété intellectuelle », c'est-à-dire du monopole intellectuel exercé par certaines personnes sur certaines idées. En effet, il devenait facile d'accéder à l'information et de la propager ce qui rendait l'application de cette propriété beaucoup plus complexe. De ce fait, pour un certain nombre de personnes, les restrictions liées à ce monopole paraissaient totalement absurdes.

Le « propriété intellectuelle » est un privilège accordé à un acteur économique sur une production de l'esprit, qui peut être une invention industrielle (auquel cas on parle de brevet) ou une création littéraire ou artistique (auquel cas on parle de droit d'auteur). Il ne s'agit pas simplement d'autoriser l'auteur d'une invention ou d'une œuvre à l'utiliser ou à la diffuser ; il s'agit d'interdire à tous les autres de l'utiliser ou de la diffuser sans son autorisation.

Le monopole intellectuel est par essence contraire au droit naturel en raison de l'absence de rareté liée à l'information [20]. Pour le dire autrement, copier n'est pas voler. Thomas Jefferson, qui a pourtant participé à l'établissement du bureau américain des brevets, écrivait ainsi en 1813 :

> « Celui qui reçoit une idée de moi reçoit un savoir sans diminuer le mien ; tout comme celui qui allume sa bougie à la mienne reçoit la lumière sans me plonger dans la pénombre [21]. »

Le monopole intellectuel permet à des personnes de toucher des redevances sans avoir signé un quelconque contrat avec celui qui les paie. Il encourage la consolidation de l'activité économique au sein de grandes entreprises. Dans le domaine informatique, il a permis à des sociétés de devenir de grands empires reposant sur le paiement de licences de leurs logiciels « propriétaires ». L'exemple le plus parlant est celui de Bill Gates et de son entreprise Microsoft. Il permet de contrôler l'utilisation d'une œuvre, et par conséquent d'influencer la culture d'une société.

La manière légale de s'opposer à cet ensemble de privilèges dans l'informatique a été l'émergence des licences libres. Celles-ci permettaient de prendre l'adversaire à son propre jeu en publiant un contenu sous une licence interdisant à quiconque de se l'approprier ou de l'inclure dans un contenu non libre. Ces licences ont émergé dans le cadre du développement logiciel, qui

était soumis au droit d'auteur aux États-Unis.

Le mouvement a été initié dans les années 80 par Richard Stallman, un physicien ayant grandi à New York et ayant étudié à Harvard. Ce dernier avait travaillé pour le département de recherche en intelligence artificielle au MIT où il avait été introduit à la culture des *hackers* et fait l'expérience des problématiques posées par les licences dans le cadre du développement du langage LISP.

Il a fondé le projet GNU en 1983 dans le but de concevoir une alternative entièrement libre au système d'exploitation UNIX. Le projet a été lancé par un courriel diffusé sur le forum Usenet net.unix-wizards. En 1985, il écrivait le manifeste GNU [22] et fondait la *Free Software Foundation*, ce qui marquait la naissance du mouvement du logiciel libre, et de la mouvance libriste en général.

Richard Stallman a formellement décrit la notion de logiciel libre pour la première fois en 1986, au sein du premier bulletin d'informations de GNU, qu'il réduisait à deux libertés de base :

> « Premièrement, la liberté de copier un programme et de le redistribuer à vos voisins, qu'ils puissent ainsi l'utiliser aussi bien que vous. Deuxièmement, la liberté de modifier un programme, que vous puissiez le contrôler plutôt qu'il vous contrôle ; pour cela, le code doit vous être accessible [23]. »

Il a par la suite raffiné cette définition pour qu'elle inclue quatre libertés fondamentales : la liberté d'utiliser le code dans n'importe quel but, la liberté de l'étudier et de le modifier, la liberté de le distribuer sans restriction et la liberté d'en distribuer des versions modifiées.

Deux types de licences libres se sont distingués : le type permissif, et le type contaminant dit *copyleft*. Le premier type de licence exigeait que le code soit librement utilisable, copiable, distribuable et modifiable tout en permettant la réutilisation dans un programme non libre. Le second type était encore plus restrictif et imposait à tout programme utilisant le code d'être publié sous la même licence.

La première licence libre a été la licence MIT, qui a été développée par le *Massachusetts Institute of Technology* à partir de 1985. Licence permissive, elle était initialement présente au sein du protocole de fenêtrage *X Window System* développé conjointement avec la DEC et IBM. Une version standarde a été publiée en 1987 (X11), puis sa version finale a été publiée en 1998 pour être utilisée pour la bibliothèque Expat.

Une autre licence permissive à apparaître rapidement a été la licence BSD, dont la première version a été publiée en 1988 pour distribuer, comme son

nom l'indique, le code du système d'exploitation BSD. Plusieurs variantes de cette licence ont été publiées au cours des années : la licence BSD proprement dite, à 4 clauses, en 1990 ; la licence BSD modifiée, à 3 clauses, en 1999 ; la licence FreeBSD, à 2 clauses, en 1999 également ; et la licence BSD à zéro clause en 2013.

La première licence contaminante (*copyleft*) a été la *GNU General Public License*, plus connue sous l'abréviation de GPL, qui a été créée par Richard Stallman en février 1989. Une version 2 a été partagée en 1991 et une version 3 en 2007.

La notion d'*open source* ou de code source ouvert n'est venue qu'après, avec l'invention du terme par Christine Peterson en 1998 et l'implication d'Eric Steven Raymond. Le terme se rapportait à l'origine seulement au logiciel libre, dans le but de lever l'ambiguïté de l'appellation « *free software* » en anglais (*free* signifie à la fois libre et gratuit). Mais il a fini par désigner tous les logiciels dont le code source était disponible publiquement, qu'ils soient publiés sous licence libre ou non.

Le code du prototype de Bitcoin (v0.1) a été publié en 2009 sous licence MIT. Pour un tel système ouvert, il était en effet nécessaire que le code soit ouvert. De plus, dans le but de réduire au maximum le contrôle sur le protocole, il fallait que le logiciel soit libre, comme nous l'expliquerons dans les chapitres 10 et 11.

La tendance extropienne

L'évolution technique prodigieuse qui s'est produite durant le XX^e^ siècle, et qui ne s'est pas cantonnée à l'informatique et à la cryptographie, a fait évoluer la vision du monde des gens et la façon dont ils envisageaient l'avenir. Le développement de procédés de plus en plus avancés faisait entrevoir des possibilités inédites pour l'homme, comme l'amélioration de ses capacités, la conception de machines perfectionnées, la production de substances psychotropes, le voyage spatial et la création de mondes virtuels. C'est ce qui a mené à la fondation du mouvement des extropiens au sein de la Silicon Valley à la fin des années 80.

L'extropianisme était une philosophie transhumaniste libérale optimiste, qui préconisait l'utilisation proactive de la technique en vue d'accroître les capacités humaines individuelles et civilisationnelles. Cette tendance se fondait sur l'extropie, un terme créé pour l'occasion pour désigner le principe d'organisation qui s'oppose à l'entropie et qui forme la base de la vie matérielle [24].

Le cœur de l'extropianisme était ainsi la survie et la prospérité dans un univers matériel souvent hostile, résolument entropique et finalement mortel.

Les extropiens ont été précédés par des individus qui ont par la suite été présentés comme des « *high-tech hayekians* [25] », dont l'économiste et futuriste Phil Salin, le pionnier des nanotechnologies Eric Drexler et l'informaticien et programmeur Mark S. Miller. Ceux-ci adhéraient au principe de l'ordre spontané – selon lequel le laissez-faire aboutit à un ordre supérieur à celui décrété par une autorité constructiviste – qui avait été développé par les économistes de l'école autrichienne et qui avait été spécialement mis en valeur par le prix Nobel d'économie Friedrich Hayek. Ayant assisté à l'accélération de la propagation de l'information apportée par le développement d'Internet, ils anticipaient l'ordre nouveau qui allait en résulter. Ils ont cherché à construire des systèmes qui s'inscrivaient dans cette évolution, comme l'*American Information Exchange* (AMIX), une place de marché automatisée dédiée à l'information, et le projet Agorics, un modèle d'échange de calcul informatique.

Le mouvement extropien a, lui, été fondé en janvier 1988 par Max T. O'Connor (futur Max More) et Tom W. Bell (aussi connu sous le nom de Tom Morrow), deux étudiants en philosophie de l'Université de Californie du Sud qui partageaient la même passion pour l'anticipation futuriste de l'évolution du monde. Au cours de l'automne 88, ils ont lancé un magazine appelé *Extropy*, dans lequel ils présentaient leur doctrine de manière détaillée et autour duquel le mouvement s'est ensuite construit. Une liste de diffusion a été mise en place durant l'été 1991 par Perry Metzger, par l'intermédiaire de laquelle les extropiens pouvaient échanger par courriel sur des sujets divers. Les extropiens présents dans la région de la baie de San Francisco ne manquaient pas non plus de se rencontrer dans la vraie vie, au moyen de ce qu'ils appelaient des Extropaganzas. Un institut, appelé l'*Extropy Institute*, a aussi été fondé en mai 1992 dans le but de faire la promotion des principes extropiens. La première conférence organisée par l'institut, nommée « Extro 1 », a eu lieu en avril 1994 à Sunnyvale dans la Silicon Valley. Elle faisait notamment intervenir, outre Max More et Tom Bell, le spécialiste en robotique Hans Moravec et le cryptographe Ralph Merkle. Cette conférence a été relatée au cours de l'automne par le magazine Wired, jetant un peu de lumière sur le mouvement [26].

Rationaliste, cette doctrine reposait sur quatre principes, définis en 1990 : l'expansion illimitée, l'auto-transformation, l'optimisme dynamique et la technologie intelligente [27]. L'extropianisme représentait ainsi un transhumanisme,

une volonté de transcender la nature humaine, déjà envisagée auparavant par des personnes comme Julian Huxley, Robert Ettinger et FM-2030.

La philosophie extropienne n'était pas seulement descriptive, mais prescriptive. Conformément au principe de l'optimisme dynamique (ou pragmatique), les extropiens souhaitaient intervenir pour accélérer l'avènement de l'avenir qu'ils anticipaient. Ils promouvaient ainsi la recherche et l'expérimentation dans les domaines scientifiques qui avaient pour but d'améliorer la condition matérielle de l'homme.

D'abord, dans leur lutte contre la mort, les extropiens étaient en particulier enthousiastes à propos de la cryogénisation, c'est-à-dire de la conservation à très basse température de corps de défunts dans l'espoir de les ressusciter grâce à un futur progrès technique. L'*Alcor Life Extension Foundation*, fondée en 1972 par Fred Chamberlain III et sa femme, basée en Arizona, était la principale organisation qui prenait en charge ce type de service.

Les extropiens étaient également ouvertement hostiles à l'autorité. Ils promouvaient le principe de l'ordre spontané, décentralisé par nature, par opposition au technocratisme centralisé, qu'ils considéraient comme ralentissant le progrès technique [28]. Certains extropiens s'inspiraient notamment de l'ouvrage de David Friedman *The Machinery of Freedom*, qui décrivait comment pouvait s'organiser une société sans État et dont la seconde édition a été publiée en 1989.

Ensuite, c'est tout naturellement que la cryptographie forte constituait un des centres d'intérêt des extropiens. Nécessaire pour préserver leur liberté, elle constituait une des briques de base pour parvenir à leurs fins. C'est pourquoi le mouvement extropien était en réalité étroitement lié au mouvement cypherpunk, lui aussi inspiré par le développement technique, de nombreuses personnes s'investissant dans les deux, comme Tim May, Hal Finney (qui a été cryogénisé par la Fondation Alcor en 2014) ou Nick Szabo.

Les extropiens s'intéressaient enfin à la monnaie. Une monnaie solide était en effet nécessaire pour imaginer pouvoir conserver de la valeur à très long terme, par exemple dans le cas d'une cryogénisation. Le sujet était ainsi abordé dans le magazine Extropy. En 1993, Hal Finney a présenté le fonctionnement du système d'argent liquide électronique eCash [29]. En 1995, le numéro 15 de la revue a été ouvertement dédié à la monnaie électronique et à la concurrence des monnaies, comme l'attestait sa couverture illustrée par un billet de banque privée à l'effigie de Hayek [30].

La monnaie numérique constituait donc l'un des enjeux mis en avant par les extropiens. Mais ces derniers ne le faisaient pas autant que les cypherpunks

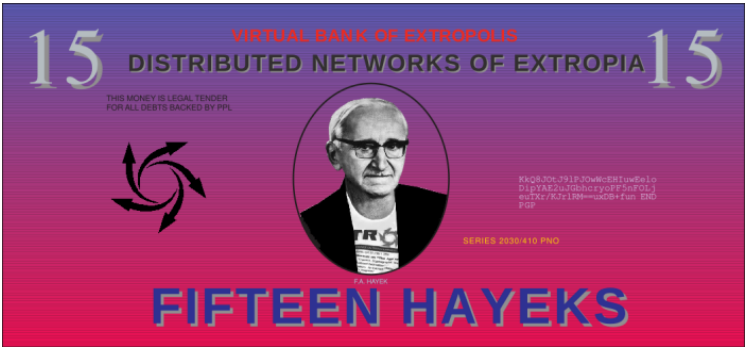

FIGURE 5.2 – Le billet fictif de 15 hayeks en couverture du magazine Extropy.

qui, des années plus tard, tenteraient de mettre en pratique leur connaissance de la cryptographie pour en créer une.

Le mouvement des cypherpunks

Le mouvement cypherpunk est apparu en 1992 dans la Silicon Valley. Les cypherpunks étaient des gens qui prônaient l'utilisation proactive de la cryptographie en vue d'assurer la confidentialité et la liberté des individus sur Internet. Ils s'opposaient à la surveillance, à la censure et à l'exploitation des données personnelles, et préconisaient la programmation et la publication ouverte de logiciels, préférablement sous licence libre, dans le but de combattre ces menaces. Leur nom, calqué sur cyberpunk, était un mot-valise composé des mots anglais *cypher*, signifiant « chiffre » (dans le sens de code secret), et *punk*, désignant originellement un voyou. Les cypherpunks étaient donc formellement des rebelles amateurs de cryptographie.

Les cypherpunks s'inspiraient partiellement du cyberpunk, un mouvement culturel construit autour de la littérature de science-fiction, qui prenait sa source à la fois dans la sous-culture des punks et dans la mouvance des hackers. Même si l'esthétique de ce dernier datait de la fin des années 70, le genre littéraire a largement été inauguré par l'écrivain William Gibson via la publication de ses premières nouvelles à partir de 1981 et surtout de son roman *Neuromancien*. Le mot, qui faisait référence à la cybernétique, c'est-à-dire la science des systèmes complexes et des réseaux, a quant à lui été inventé en 1983 par Bruce Bethke, et a été popularisé par Gardner Dozois en décembre 1984 dans un éditorial pour le Washington Post.

La caractéristique principale du genre cyberpunk était de décrire un futur

dystopique où la technique de pointe était omniprésente (implants informatiques, réalité augmentée, réalité virtuelle, intelligence artificielle, robots) et où la société était sujette à la consommation à outrance (drogue, sexe, etc.), au crime généralisé et à l'avarice des corporations. Le cyberpunk décrivait ainsi un monde combinant haute technologie et bassesse humaine, pour reprendre l'expression de Bruce Sterling, dont le héros tentait de s'extraire tant bien que mal.

De ce genre cyberpunk est né tout un mouvement d'individus qui partageaient la même vision du monde, formant notamment une contreculture cyberdélique, née de la fusion de la cyberculture et du psychédélisme. Cette sous-culture en vogue dans la Silicon Valley était incarnée par la revue *High Frontiers*, fondée en 1984 par R. U. Sirius, qui est plus tard devenue *Reality Hackers* puis *Mondo 2000*.

Les cypherpunks tiraient leur inspiration de ce mouvement. Toutefois, ils n'étaient pas pour autant des cyberpunks : s'ils avaient bien conscience des scénarios dystopiques qui pouvaient dériver de l'évolution technique (notamment en ce qui concerne la surveillance), ils ne partageaient pas la vision pessimiste relayée par le cyberpunk. De ce fait, le mouvement cypherpunk constituait en quelque sorte une réaction au cyberpunk, dans le sens où il postulait, à l'instar des extropiens, que l'évolution technique pouvait amener les êtres humains à s'émanciper plutôt qu'à tomber dans l'esclavage mutuel.

Les cypherpunks basaient en particulier leurs réflexions sur une longue nouvelle publiée en 1980 par l'auteur de science-fiction Vernor Vinge, intitulée *True Names*. Cette nouvelle, qui abordait des thèmes propres au genre cyberpunk sans strictement en faire partie, contait l'histoire de Roger Pollack, un individu agissant au sein d'un groupe de pirates dans un monde virtuel appelé « *The Other Plane* », utilisant le pseudonyme de Mr. Slippery et faisant attention à ne surtout pas révéler son « Vrai Nom » (à savoir son nom civil) au risque de subir une « Vraie Mort » (par exécution étatique). Cet enjeu correspondait par conséquent à l'enjeu principal de la cryptographie : la préservation de l'anonymat dans le but de conserver sa liberté et, *in fine*, sa vie.

Les cypherpunks avaient ainsi le regard tourné vers l'avenir. Mais leur préoccupation centrale concernait surtout l'avenir proche : c'était la confidentialité dans le cyberespace naissant [31]. C'est pourquoi leur mouvement pouvait rassembler des optimistes et des pessimistes, des extropiens et des cyberpunks, qui trouvaient du sens dans cette lutte contre la surveillance de masse.

À l'origine, le mouvement cypherpunk a été le fruit de la pensée et de

l'action de Timothy C. May, dit Tim May. Ce dernier était un scientifique, ingénieur et informaticien né en 1951 en périphérie de Washington D.C. Passionné de science-fiction et de physique, il avait travaillé pour Intel de 1974 à 1986, où il avait contribué à résoudre le problème des particules alpha dans les circuits intégrés. Il avait accumulé une certaine fortune au cours de ces années, si bien qu'il avait décidé de prendre sa retraite (à l'âge de 35 ans) pour se consacrer à ses passions politiques.

Tim May a rencontré Phil Salin en 1987, avec qui il a pu discuter des implications de la cryptographie. Ses discussions avec Salin, ainsi qu'avec d'autres personnes comme Marc Stiegler, l'ont poussé à écrire le *Manifeste crypto anarchiste* en août 1988. Dans ce manifeste, il posait les bases de ce qui allait devenir la doctrine des cypherpunks et décrivait le potentiel d'émancipation individuelle apporté par la cryptographie et par l'anonymat. Le manifeste, pastiche ironique du *Manifeste du parti communiste*, décrivait comment l'avènement des méthodes cryptographiques modernes allait, d'après lui, déstabiliser l'État en permettant aux individus d'échanger librement de l'information et de la richesse. En particulier, il écrivait :

> « Tout comme la technique de l'imprimerie a altéré et réduit le pouvoir des corporations médiévales et la structure sociale de pouvoir, les méthodes cryptologiques altèrent fondamentalement la nature de l'interférence de l'État et des grandes entreprises dans les transactions économiques [32]. »

Tim May n'était pas seul à penser de cette manière et communiquait avec d'autres personnes qui partageaient ses idées. C'était le cas de son ami Eric Hughes, un jeune mathématicien et programmeur ayant grandi dans une famille mormone en Virginie près de Washington et à Salt Lake City. Ce dernier avait travaillé brièvement pour DigiCash à Amsterdam avant de revenir sur la côte Ouest. En mai 1992, alors qu'il cherchait à emménager dans la Silicon Valley, lui et Tim May ont longuement discuté de cryptographie, à tel point qu'ils ont décidé de reproduire ce type d'échange avec un plus grand nombre de personnes en organisant des réunions physiques.

La première réunion du mouvement cypherpunk a ainsi eu lieu au cours de la journée du 19 septembre 1992, dans la maison d'Eric Hughes à Oakland. L'accès à cette réunion se faisait uniquement sur invitation afin de préserver la discrétion du groupe. Libertariens pour la plupart, extropiens pour certains, les invités étaient des connaissances de May et Hughes issues de la communauté des hackers et des entreprises informatiques de la région. Durant la réunion, Tim May y a lu le *Manifeste crypto anarchiste*. En guise d'animation, les personnes conviées ont également participé à un « jeu de la crypto anarchie »,

qui consistait à simuler un réseau de mélange par l'échange et l'ouverture d'enveloppes de papier [33].

Parmi les invités se trouvait John Gilmore, un informaticien américain connu pour avoir été l'un des premiers employés de Sun Microsystems. Il avait aussi cocréé la hiérarchie ouverte alt.* sur Usenet et était un contributeur majeur du projet GNU. Alors en retraite anticipée depuis 1986, tout comme May, il s'était engagé dans l'activisme dans le but de protéger les libertés civiles sur Internet. En 1989, il avait cofondé Cygnus Support, une entreprise spécialisée dans le support professionnel de composants fondés sur GNU. Il avait également participé à la création de l'*Electronic Frontier Foundation* (EFF), une ONG internationale de protection des libertés sur Internet, aux côtés de Mitch Kapor et de John Perry Barlow en 1990. Lui aussi voyait la cryptographie comme un moyen de libération individuelle [34].

Une autre personne présente durant cette réunion fondatrice était l'activiste Judith Milhon, une femme née en 1939 qui avait participé au mouvement des droits civiques pour l'abolition des discriminations raciales dans les années 60 et avait été emprisonnée pour désobéissance civile. Programmeuse, hackeuse, elle était alors la coéditrice de la revue cyberpunk *Mondo 2000*, à laquelle elle participait sous le nom de plume de St. Jude. Elle était également la compagne d'Eric Hughes, malgré leur grande différence d'âge.

C'est elle qui a donné leur nom aux cypherpunks lors de cette réunion, sur le ton de la plaisanterie. « Je pense que vous êtes des cryptoanarchistes – ce que j'appellerais des cypherpunks ! », a-t-elle écrit par la suite [35]. Le terme capturait bien l'esprit de la cryptoanarchie, tout en donnant au mouvement un côté moins formel et dogmatique. En effet, les gens préoccupés par ces enjeux n'étaient pas tous anarchistes : ils pouvaient s'opposer fermement à l'autoritarisme et à la surveillance, sans pour autant vouloir remettre en cause les fondements même de l'État [36]. C'est ce côté informel qui a fait que le terme a été adopté immédiatement.

Après la réunion, Eric Hughes, avec l'aide de Hugh Daniel, a créé une liste de diffusion de courrier électronique nommée « Cypherpunks ». Le courriel de bienvenue a été envoyé dans la soirée du 21 septembre (PDT). La liste était relayée par le serveur associé au nom de domaine `toad.com` appartenant à John Gilmore. Ce dernier a aussi offert la disponibilité des locaux de Cygnus pour les réunions ultérieures.

La liste a accueilli de nombreuses discussions relatives à la cryptographie et à son utilisation concrète, dont notamment l'argent liquide électronique. Beaucoup de gens sont intervenus dès les premiers mois, comme par exemple

l'ancien pirate téléphonique John Draper. En un an à peine, la liste recensait ainsi plus de 500 participants.

L'un de ces participants était Harold T. Finney II, dit Hal Finney, informaticien et cryptographe américain, diplômé de Caltech et programmeur de jeux vidéos pour les consoles Intellivision et Atari VCS. Extropien et enthousiasmé par la popularisation d'Internet, il était obsédé par la cryptographie, à tel point qu'il était rentré en contact avec Phil Zimmermann pour travailler avec lui sur la version 2.0 de PGP, sortie le 2 septembre 1992. Hal Finney était aussi fasciné par les idées de David Chaum. En novembre 1992, il écrivait à la liste de diffusion :

> « Nous voici confrontés aux problèmes de la perte de confidentialité, de l'informatique envahissante, des bases de données massives, de l'augmentation de la centralisation – et Chaum propose une direction à suivre complètement différente, une direction qui met le pouvoir entre les mains des individus plutôt qu'entre celles des États et des grandes entreprises. L'ordinateur peut être utilisé comme un outil pour libérer et protéger les personnes, plutôt que pour les contrôler[37]. »

La vision des cypherpunks était claire : mettre en pratique ce qui avait été jusque-là de vagues spéculations. Il était en effet stérile de théoriser des choses si cela ne se traduisait pas par des actions concrètes. Cet esprit pratique a été parfaitement résumé par Eric Hughes dans son *Manifeste d'un Cypherpunk* envoyé à la liste de diffusion en mars 1993, où il écrivait alors :

> « Nous devons défendre notre propre vie privée si nous voulons en avoir une. Nous devons nous rassembler et créer des systèmes qui rendent possibles les transactions anonymes. Depuis des siècles, les gens défendent leur vie privée par des chuchotements, par l'obscurité, par des enveloppes, des portes fermées, des poignées de main secrètes et des messagers. Les techniques du passé ne permettaient pas une forte confidentialité ; les techniques électroniques, elles, le permettent.
>
> Nous, les Cypherpunks, nous consacrons à construire des systèmes anonymes. Nous défendons notre vie privée avec la cryptographie, avec les systèmes anonymes de transfert de courriels, avec les signatures numériques, et avec la monnaie électronique.
>
> Les Cypherpunks écrivent du code. Nous savons que quelqu'un doit concevoir des logiciels pour défendre la vie privée en général, et puisque nous ne pouvons pas avoir de vie privée si tout le monde n'en a pas, nous allons nous en charger. Nous publions notre code pour que nos collègues Cypherpunks puissent le mettre en pratique et expérimenter avec. Notre code est libre d'utilisation pour tous, dans le monde entier. Nous ne nous soucions guère que vous n'approuviez

> pas les logiciels que nous concevons. Nous savons que les logiciels ne peuvent pas être détruits et qu'un système largement dispersé ne peut pas être arrêté [38]. »

Deux mois plus tard, en mai 93, le mouvement était définitivement lancé : les cypherpunks faisaient la une du magazine Wired, récemment fondé dans le but de parler de l'incidence culturelle, économique et politique des techniques émergentes. Tim May, Eric Hughes et John Gilmore apparaissaient masqués sur la couverture, et un long article détaillait leurs idées et leurs revendications [39]. C'était la préfiguration du rôle qu'ont joué par la suite les cypherpunks dans la sauvegarde de la liberté sur Internet.

L'action des cypherpunks pour la liberté

Le mouvement cypherpunk est né juste après le triomphe des États-Unis dans la guerre froide les opposant à l'URSS et au début de l'adoption d'Internet par le grand public, amorcée notamment par la popularisation de Usenet et par l'apparition du World Wide Web. Il est apparu en quelque sorte « au bon moment » pour accompagner cette mutation majeure qui a marqué le monde entier.

Le premier accomplissement des cypherpunks a été leur intervention dans la guerre contre la cryptographie orchestrée par l'État fédéral étasunien. Cette guerre a été inaugurée en février 1993 par la bataille contre PGP, lorsque Phil Zimmermann a été poursuivi en justice pour en avoir publié les deux premières versions en ligne, l'exportation de produits cryptographiques sans licence étant prohibée par la réglementation américaine (ITAR).

Cette décision a naturellement suscité une forte réaction de la part des cypherpunks qui, en réponse à la tentative d'application de cette réglementation absurde, se sont mis à partager le code de chiffrement dans une démarche de désobéissance civile. Le jeune britannique Adam Back l'a ainsi fait imprimer sur des t-shirts qu'il distribuait aux autres et certains ont été jusqu'à se le tatouer sur leur corps. En 1995, Phil Zimmermann a publié la version 2.6.2 de PGP dans un livre, dans le but de réduire au maximum la distinction entre le code et l'expression, cette dernière étant protégée par le premier amendement de la Constitution des États-Unis.

Les charges contre Zimmermann ont finalement été abandonnées en 1996, notamment grâce au soutien de membres du MIT. Cela lui a permis de créer son entreprise pour travailler sur PGP et engager des employés, comme Hal Finney. En novembre de la même année, Bill Clinton signait l'Ordre exécutif 13026 qui assouplissait considérablement les restrictions sur l'exportation des produits cryptographiques.

Cependant, la guerre contre la cryptographie ne s'arrêtait pas là. En effet, elle ne concernait pas que l'interdiction d'utiliser la cryptographie forte, mais également l'obligation pour les constructeurs de matériel informatique d'intégrer des portes dérobées dans leurs produits. Le projet de loi sénatoriale 266, proposé par Joe Biden en 1991, devait ainsi faire en sorte que tous les appareils de communication puissent être surveillés par l'État fédéral :

> « Le Congrès estime que les fournisseurs de services de communications électroniques et les fabricants d'équipements de services de communications électroniques doivent veiller à ce que les systèmes de communications permettent au gouvernement d'obtenir le contenu en texte clair des communications vocales, informatiques et autres lorsque la loi l'autorise de manière appropriée [40]. »

Ce projet s'est matérialisé le 16 avril 1993 par l'annonce de la puce Clipper par la Maison-Blanche, un cryptoprocesseur servant à chiffrer les messages vocaux et les données, qui implémentait (au moyen de son algorithme Skipjack) un dispositif d'autorité de séquestre permettant aux agences étasuniennes de déchiffrer les communications au besoin. Cette puce était développée et produite par la NSA et était destinée à équiper les appareils électroniques vendus au grand public. La Maison-Blanche se justifiait en prétendant que la puce pourrait « à la fois fournir aux citoyens respectueux de la loi un accès au chiffrement dont ils ont besoin et empêcher les criminels de l'utiliser pour cacher leurs activités illégales [41] ».

Cette annonce a provoqué une levée de boucliers chez les cypherpunks qui y voyaient un projet orwellien et s'y sont opposés en bloc. Cependant, la lutte n'a pas été longue : en juin 1994, le cypherpunk Matt Blaze a découvert une vulnérabilité au sein du dispositif d'autorité de séquestre, qui rendait le dispositif inefficace et permettait à la puce d'être utilisée pour chiffrer les données normalement. À partir de là, le projet a perdu progressivement en ampleur pour être définitivement abandonné en 1996. La liberté avait gagné, au moins temporairement [42].

Comme on l'a observé, l'optique des cypherpunks était d'être dans l'action, d'écrire du code et de partager des programmes qui puissent être utilisés. Ils se sont donc focalisés sur la construction de systèmes axés sur trois aspects majeurs : la protection de la vie privée, la diffusion de l'information et le commerce en ligne.

Le premier domaine d'innovation a été celui des serveurs de courriel anonyme, qui permettaient de retransmettre les courriers électroniques de façon à masquer l'identité de leur expéditeur. Le premier serveur de ce type a été mis en place par Eric Hughes et Hal Finney pour la liste des cypherpunks

dès octobre 1992, et il utilisait PGP pour le chiffrement. En 1994, Lance Cottrell a amélioré la chose en proposant le modèle Mixmaster, qui permettait d'envoyer des courriels par paquets de taille fixe et de les réordonner, pour empêcher le traçage des courriels par la surveillance de l'activité du serveur.

Outre le courriel, l'objectif des cypherpunks était de rendre la navigation sur Internet plus anonyme, le fonctionnement du Web étant trop transparent. C'était l'idée des frères Austin et Hamnett Hill qui ont lancé le réseau Freedom en 1999 par l'intermédiaire de leur entreprise Zero-Knowledge Systems, qui employait notamment les cypherpunks Ian Goldberg et Adam Back. Mais cette expérience s'est arrêtée en 2001, faute d'utilisation suffisante.

Un projet du même type dans lequel les cypherpunks se sont impliqués était le réseau Tor, lancé publiquement en 2003, qui se basait, comme on l'a déjà expliqué, sur le routage en ognon. En effet, si Tor était le résultat d'une recherche militaire provenant de la Navy, les individus ayant travaillé sur son implémentation n'en avaient pas moins des convictions allant dans le sens des cypherpunks. Roger Dingledine et Nick Mathewson, les deux informaticiens qui ont aidé Paul Syverson dans cette conception, en faisaient partie : le premier était derrière le projet Free Haven, qui avait pour but de développer un système décentralisé de stockage de données ; le second est crédité pour avoir créé le programme de serveur de courriel anonyme Mixminion. On peut également citer le jeune Jacob Appelbaum, qui s'est fortement impliqué dans le projet Tor entre 2004 et 2016.

Un troisième secteur auquel les cypherpunks ont contribué a été la fluidification des flux informationnels, notamment face à la censure. En 1993, Tim May a repris le modèle de l'AMIX de Phil Salin pour introduire un concept de place de marché de l'information appelé BlackNet. Cette plateforme devait servir à échanger des secrets commerciaux, des recettes de fabrication, des techniques relatives aux nanotechnologies, des informations sur les décisions d'entreprises, au moyen de « CryptoCredits », la monnaie interne du système. Il s'agissait donc de libérer l'information des contraintes étatiques : « BlackNet n'est officiellement affilié à aucune idéologie, mais considère les États-nations, les lois d'exportation, les lois sur les brevets, les considérations de sécurité nationale, etc. comme des reliques de l'ère pré-cyberspatiale », écrivait Tim May [43].

Le concept de BlackNet était une simple expérience de pensée et n'a jamais été mis en œuvre. Toutefois, il a préfiguré d'autres modèles qui ont ouvert la voie au partage d'informations sensibles sur Internet. C'était par exemple le cas de Cryptome, un site web lancé en 1996 par le cypherpunk John Young

pour héberger des documents sensibles et censurés par les États.

Mais c'était surtout le cas de WikiLeaks, une plateforme facilitant la publication de documents classifiés fondée en 2006 par l'informaticien australien Julian Assange. Julian Assange était un cypherpunk assumé : il envoyait des courriels sur la liste depuis au moins 1995 et a par la suite coécrit un livre à ce sujet intitulé *Cypherpunks: Freedom and the Future of the Internet*. WikiLeaks a permis le développement de l'activité des lanceurs d'alertes (*whistleblowers*) révélant les agissements illégaux ou injustes de leurs employeurs, et en particulier des États, largement inaugurée par la publication des Pentagon Papers en 1971 par Daniel Ellsberg. Grâce à l'utilisation du chiffrement et de Tor, WikiLeaks permettait aux personnes à l'origine des fuites de conserver leur anonymat.

Enfin, les cypherpunks se sont aussi investis dans le développement du pair-à-pair. En 2000, le développeur Jim McCoy, cypherpunk de la première heure, a ainsi lancé Mojo Nation, un projet de plateforme d'échange de fichiers en pair-à-pair intégrant une devise interne [44]. En 2001, un contributeur au projet, appelé Bram Cohen, s'en est séparé et a lancé son propre protocole, BitTorrent, qui est rapidement devenu une référence pour le partage de fichiers. Mojo Nation, alors rebaptisé Mnet, a été repris par Zooko Wilcox. Ce dernier a lancé son propre système, Tahoe-LAFS, en 2006.

Mais ce qu'il manquait à tous ces systèmes, c'était une monnaie numérique robuste qui soit adaptée au cyberespace, chose à laquelle les cypherpunks aspiraient depuis le début. Leurs modèles possédaient parfois des unités de compte internes, mais elles étaient très instables. Malheureusement, une telle monnaie ne serait conçue que des années plus tard, en 2008, sous la forme de Bitcoin.

Satoshi Nakamoto était-il un cypherpunk ? À notre connaissance, il n'a pas participé au mouvement originel des années 90, ni ne s'est jamais réclamé explicitement de celui-ci. Toutefois, il a très clairement été influencé par l'héritage des cypherpunks comme le suggèrent plusieurs éléments. D'abord, il semblait bien connaître ce qui s'était passé et de ce qui avait été fait précédemment dans le domaine de la monnaie numérique, malgré quelques lacunes (voir le chapitre 6). Puis, il a publié le livre blanc sur la liste de diffusion dédiée à la cryptographie gérée par Perry Metzger, qui était la digne héritière de la liste des cypherpunks, dont l'usage avait malheureusement périclité vers 1997. Ensuite, il a utilisé un pseudonyme et, par de bonnes pratiques comme l'utilisation de PGP, Tor et Namecheap, il est parvenu à préserver son anonymat malgré une activité en ligne s'étalant sur presque trois années. Enfin, il a « écrit

du code » en programmant un outil émancipateur, conformément à l'appel à la pratique d'Eric Hughes. Il est donc tout à fait raisonnable d'associer Satoshi aux cypherpunks, tout en l'en dissociant partiellement, ne serait-ce parce qu'il est toujours resté très mesuré dans ses quelques jugements politiques.

Une guerre perpétuelle

Bitcoin s'inscrit pleinement dans la guerre technologique opposant l'autorité à la liberté. Son code n'est pas neutre : il n'est pas une vague technique qu'on puisse utiliser dans un sens ou dans l'autre, mais il a pour objectif clair d'amener plus d'autonomie individuelle. Bitcoin n'est pas un assemblage aléatoire de procédés, mais un objet ancré dans son époque, qui prend racine dans les mouvements techno-idéologiques qui l'ont précédé.

Bitcoin est ainsi issu de mouvements qui appellent à la pratique. Les libristes promouvaient la publication sous licence libre dans le but de mettre en commun l'ensemble des connaissances de l'humanité. Les extropiens préconisaient la recherche et l'expérimentation pour améliorer drastiquement les conditions de vie matérielles de l'être humain. Les cypherpunks prônaient le fait d'écrire du code afin de préserver la confidentialité des individus dans le cyberespace. Il est donc naturel que la communauté de Bitcoin s'inscrive dans la même démarche en encourageant la pratique monétaire en vue de résister au contrôle de plus en plus grand de l'État et des banques sur le transfert d'argent.

Cependant, pour arriver à ce résultat, il a fallu concevoir un système qui permette de répartir les risques entre les participants sans nécessiter l'intervention d'un tiers de confiance. Une quête que nous raconterons dans le prochain chapitre.

6

La cybermonnaie avant Nakamoto

La cybermonnaie est une monnaie dont le fonctionnement repose entièrement sur un réseau informatique appartenant à Internet. Elle est définie au sein de ce réseau et est transférée par son intermédiaire. Il s'agit d'une monnaie native du cyberespace, le nouvel espace créé par l'émergence d'Internet, conçu comme une juridiction séparée du monde physique.

Une forme plus spécifique de cybermonnaie est l'argent liquide numérique, ou *digital cash* en anglais, qui transcrit les propriétés des espèces sonnantes et trébuchantes dans le cyberespace. Toutefois, bien que cette conception remonte à l'émergence même d'Internet, elle n'a pas tout de suite pu voir le jour en raison de limitations techniques et conceptuelles. L'argent liquide numérique a fait l'objet d'une véritable quête, à laquelle ont participé de nombreux individus désireux d'utiliser Internet pour créer un nouveau paradigme économique, dont les cypherpunks.

Bitcoin est le résultat de cette quête. Il n'est pas sorti de nulle part : il est le fruit de réflexions, de recherches et d'expérimentations en tous genres. La découverte de Satoshi Nakamoto constitue ainsi une percée dans un domaine qui existait antérieurement.

L'échange monétaire sur Internet

Internet a généralisé le partage informationnel et, ce faisant, a créé un nouvel espace d'interactions humaines : le cyberespace. L'apparition de cet espace a naturellement mené à l'émergence d'une demande pour l'échange monétaire, demande qui s'est manifestée par le développement du commerce électronique dans les années 90. Comme le résumait très bien Robert Hettinga en 1998, la problématique était la suivante :

> « Depuis l'invention du télégraphe, le règlement des transactions financières se heurte à un problème : comment faire des affaires à distance alors que le moyen le plus simple d'exécuter, de compenser et de régler une transaction est l'échange de certificats au porteur [1] ? »

La première solution était d'utiliser du crédit bancaire. L'usage de celui-ci comme intermédiaire d'échange s'était progressivement généralisé en Occident avec la bancarisation de la société. Au cours du temps, une solution technique avait prévalu : la carte de paiement, aussi appelée carte de débit ou carte de crédit selon son fonctionnement. Cette solution n'avait pas constitué quelque chose de novateur [2], mais s'était considérablement popularisée à partir des années 60, par le biais de l'adoption bancaire et de la formation de sociétés spécialisées dans le transfert électronique de fonds comme NBI / Visa et Interbank / MasterCard [3].

Mais le paiement par carte bancaire n'était pas forcément adapté au cyberespace, car difficile à mettre en place, coûteux et peu sécurisé à l'époque. C'est pourquoi on a vu émerger différentes solutions techniques permettant de faire des paiements sur Internet au milieu des années 90, comme CyberCash, First Virtual ou Open Market. Des systèmes de micropaiements ont également fait leur apparition à l'instar de CyberCoin (géré par CyberCash), NetBill et MilliCent.

Ces systèmes ont fini par échouer, mais c'est dans cette niche que s'est développé le service PayPal à partir de 1999. Celui-ci était conçu pour être simple d'accès (PayPal signifie littéralement « payer copain ») : il permettait des paiements faciles et sans frais, entre adresses de courrier électronique. Son modèle économique se fondait sur la perception des intérêts liés à la conservation des fonds des clients en banque, afin de payer les coûts de fonctionnement et de rémunérer les actionnaires. C'était donc un service de troisième couche, bâti au-dessus du système bancaire, lui-même basé sur le système de monnaie centrale [4].

En dépit des bonnes intentions de leurs créateurs, ces systèmes étaient

complètement à la merci du régulateur. Ceux qui ont survécu se sont par conséquent engagés dans la surveillance et la censure, à un niveau jamais vu auparavant.

La deuxième solution pour échanger de la valeur sur Internet était d'émettre une nouvelle monnaie numérique, de manière centralisée, si besoin en l'adossant à une monnaie existante. Cette solution consistait à ne pas demander l'autorisation, en jouant sur le flou juridique qui pouvait exister dans un domaine relativement nouveau.

Les jeux vidéos en ligne massivement multijoueurs, dont les fameux MMORPG, ont contribué à installer l'idée de monnaie numérique indépendante dans les esprits. On peut penser au Token, la monnaie native de Habitat, l'un des premiers MMORPG graphiques, développé en 1985 par Lucasfilm Games et jouable sur Commodore 64. On peut aussi citer les cas des pièces de métaux précieux dans Everquest en 1999, du dollar Linden de Second Life en 2003 ou encore de l'or de World of Warcraft en 2004. Tous ces exemples prouvaient qu'une économie réelle pouvait émerger d'une monnaie virtuelle.

Un exemple anecdotique de ce type de système de monnaie numérique était le Hawthorne Exchange, lancé le 24 mars 1993 sur la liste de diffusion extropienne par un individu du nom de Brian Holt Hawthorne. Il s'agissait d'un marché de réputation pour les membres de la liste, dont l'unité de compte servant à l'échange était le Thorne. Le système était peu accessible et peu robuste, mais les extropiens l'ont utilisé et ont donné de la valeur au Thorne, par anticipation du futur. Quelques échanges monétaires contre du dollar et des services ont été réalisés entre les membres de la liste. Toutefois, le Hawthorne Exchange était simplement une expérimentation, le Thorne n'ayant aucune prétention à être une réelle monnaie, que son auteur a décidé d'arrêter en 94.

Un système bien plus sérieux est apparu en 1996 : e-gold. Comme décrit dans le chapitre 4, il s'agissait d'un modèle de monnaie en or numérique dont l'unité de compte était théoriquement adossée à de l'or. Le système reposait sur l'entreprise *Gold & Silver Reserve Inc.* fondée par Douglas Jackson, qui conservait l'or physique dans ses coffres. Il a connu un grand succès dans les années 2000 avant d'être fermé en 2007 par le Secret Service.

Toutefois, le problème avec ce type de monnaie était qu'il dépendait toujours d'une entité qui constituait un point de défaillance unique. Ainsi, même si les personnes qui le géraient n'étaient pas malintentionnées, ce type de système n'était pas robuste et ne pouvait pas perdurer à long terme.

La troisième solution de cybermonnaie était la conception d'un argent liquide électronique, confidentiel, non contrôlé et décentralisé. L'idée était de

diminuer le rôle du tiers de confiance le plus possible pour que la monnaie en question se rapproche au mieux de l'argent liquide physique, de minimiser la confiance impliquée. Idéalement l'objectif était d'obtenir un « or numérique » qui soit à la fois « infalsifiable, sans inflation, et intraçable [5] ».

Les cypherpunks considéraient que ce type de monnaie numérique était quelque chose d'essentiel dans leur combat pour la liberté et la confidentialité. Ils prévoyaient en effet d'utiliser ce type d'unité de compte dans leurs projets, comme en témoignent les Cryptocredits de BlackNet ou le mojo de Mojo Nation. C'est donc tout naturellement qu'ils ont cherché à développer une telle monnaie.

Cependant, la conception d'un argent liquide numérique, d'une authentique cybermonnaie, n'était pas une tâche facile. La quête pour sa réalisation a mis de longues années avant d'aboutir. Et la première étape dans cette quête a été l'apparition de eCash, qui a eu le mérite de poser sur la table une proposition cohérente, répondant aux exigences des cypherpunks.

eCash : l'argent liquide chaumien

eCash est un concept de monnaie numérique confidentielle qui a été conçu par le cryptographe David Chaum dans les années 80 et qui a été mis en application au cours des années 90. Il a été décrit initialement par Chaum en 1982 avant d'être mis en avant en 1985 dans son article intitulé *Security without Identification* qui promettait de « rendre Big Brother obsolète [6] ». Le modèle repose sur le mécanisme de signature aveugle, qui garantit la propriété de la monnaie et l'anonymat des échanges.

Le modèle eCash gère des billets numériques de différentes coupures qui peuvent être conservés par les utilisateurs. Les billets sont émis et remplacés par des serveurs appelés des banques (*banks*) ou des monnaieries (*mints*). Lorsqu'un billet est transféré, le destinataire l'envoie à sa banque qui se charge de le vérifier et de lui en redonner un autre. Les banques du système entretiennent chacune un registre des billets dépensés pour empêcher la double dépense. Le système est chapeauté par une autorité centrale qui délivre les habilitations.

L'émission d'un billet numérique utilise comme on l'a dit le mécanisme de signature aveugle. Pour l'utilisateur, il s'agit essentiellement de choisir un grand nombre et de le faire signer par sa banque, de manière à ce que ce nombre reste uniquement connu de lui. Le fonctionnement de ce procédé mathématique est analogue à la signature d'un billet physique en papier carbone représentant

une quantité précise d'unités monétaires (coupure). Voici comment se passe la création d'un billet par Alice :

1. Alice crée un billet en papier carbone (en générant aléatoirement un très grand nombre x) ;
2. Alice place le billet dans une enveloppe fermée (en utilisant une fonction de commutation c qu'elle seule connaît) ;
3. Alice envoie l'enveloppe contenant son billet à la banque et lui communique la coupure souhaitée ;
4. La banque signe l'enveloppe en indiquant la quantité d'unités que le billet représente (la banque dispose d'une clé privée pour chaque coupure), ce qui a pour effet de signer le billet en papier carbone à l'intérieur ;
5. La banque renvoie l'enveloppe à Alice ;
6. Alice ouvre l'enveloppe pour récupérer son billet signé (en utilisant la fonction d'inversion c') ;
7. Alice vérifie que la signature de la banque est authentique (en vérifiant qu'elle correspond à la clé publique de la banque liée à la coupure demandée).

Le transfert du billet signé se fait en le donnant à quelqu'un d'autre. Ainsi, le paiement de Bob par Alice pour un service rendu se compose des étapes suivantes : d'abord, Alice transmet le billet à Bob ; puis, Bob vérifie qu'il a bien été signé par la banque d'Alice ; ensuite, il envoie immédiatement le billet réceptionné à sa banque ; enfin, la banque de Bob vérifie que le billet n'a pas déjà été utilisé et, le cas échéant, signe un nouveau billet de la même coupure pour le donner à Bob.

Les billets numériques peuvent être émis pour eux-mêmes, auquel cas ils forment une monnaie de base. Mais ils peuvent également être adossés à une autre monnaie comme le dollar. Dans ce dernier cas, l'utilisateur peut à tout moment rendre ses billets à sa banque pour récupérer la somme correspondante.

La principale conséquence du procédé est qu'aucune banque du système ne peut relier le paiement à l'identité d'Alice. La banque d'Alice sait qu'un billet signé par elle a été dépensé, mais elle ne peut pas savoir de manière absolue qu'il s'agit d'un billet ayant appartenu à Alice. La banque de Bob sait que Bob a reçu le paiement et qu'il provient de la banque d'Alice, mais rien de plus. C'est pour cette raison qu'eCash peut être considéré comme un modèle respectueux de la vie privée.

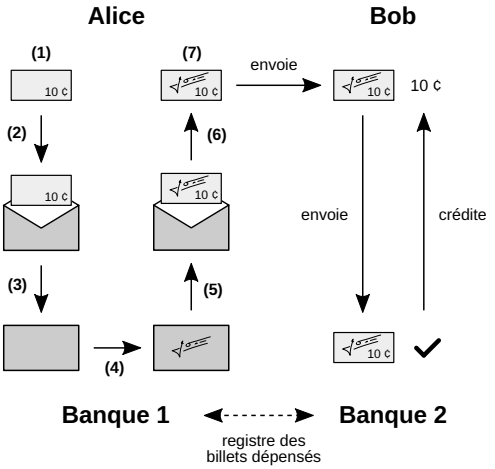

FIGURE 6.1 – Création et remplacement d'un billet chaumien.

Toutefois, cette confidentialité du système repose sur une supposition forte : la bienveillance des banques du système. En effet, si une banque voulait obtenir des informations liées à un billet particulier (par exemple sous la pression étatique), elle pourrait les demander à son propriétaire en échange de l'autorisation du transfert. On peut ainsi imaginer un système eCash qui respecte pleinement les normes de surveillance, comme le suggère l'implémentation de Chaum pour une MNBC conceptualisée en 2021 [7].

Magic Money, les CyberBucks et les banques

Le concept d'eCash a été mis en application au cours des années 90. À l'époque, le Web venait tout juste d'apparaître, le commerce électronique était inexistant et cette idée constituait une formidable opportunité. Cette mise en œuvre a été réalisée d'abord par les cypherpunks par l'intermédiaire du protocole Magic Money, puis par la société de David Chaum, DigiCash, au moyen de jetons d'essai appelés les CyberBucks et d'un déploiement dans le système bancaire classique.

Le protocole Magic Money a été présenté sur la liste de diffusion des cypherpunks le 4 février 1994 par un développeur anonyme se faisant appeler Pr0duct Cypher et utilisant PGP pour s'identifier. Magic Money permettait de créer sa monnaie en faisant fonctionner un serveur de courrier électronique qui servait de monnaierie eCash [8]. Magic Money utilisait l'algorithme RSA

et la signature aveugle, deux techniques qui étaient brevetées à l'époque, de sorte que son déploiement était *de facto* illégal et devait se confiner à l'expérimentation. Cette annonce a toutefois été accueillie favorablement sur la liste, notamment par Hal Finney.

Le premier système basé sur Magic Money a été mis en ligne par Mike Duvos quelques semaines plus tard avec les Tacky Tokens, dont les pièces étaient émises en valeurs de 1, 2, 5, 10, 20, 50 et 100 unités. Malgré des propositions, aucune transaction réelle n'a été réalisée, ce qui a poussé Tim May à se demander « pourquoi l'argent liquide numérique [n'était] pas utilisé [9] ». D'autres implémentations fantaisistes de Magic Money ont vu le jour par la suite, comme les GhostMarks, les DigiFrancs ou les NexusBucks, mais n'ont pas connu un plus grand succès. L'activité a très rapidement reculé au cours des semaines.

Le concept d'eCash a ensuite été mis en pratique par la société DigiCash B.V., fondée par David Chaum en 1990 et basée à Amsterdam aux Pays-Bas, qui avait pour mission de mettre en application les idées du cryptographe. Plusieurs cypherpunks ont travaillé pour cette entreprise comme Eric Hughes, Bryce Wilcox (le futur Zooko Wilcox-O'Hearn) et Nick Szabo. Après quelques années de développement, un prototype a été présenté en mai 1994 lors de la première conférence internationale sur le World Wide Web au CERN à Genève.

DigiCash a ensuite réalisé un essai qui a débuté le 19 octobre de cette année, avec l'émission de CyberBucks. Bien que leur nom fasse référence à la monnaie étasunienne (« *a buck* »), ceux-ci n'étaient pas adossés au dollar et possédaient donc un prix flottant par rapport à ce dernier. Une distribution initiale de 100 CyberBucks par nouvel utilisateur a été effectuée afin d'aider l'amorçage du système. Les cypherpunks se sont appropriés la chose en effectuant des échanges réels : la récompense pour la résolution d'un problème, la vente de t-shirts, la vente de logiciels, et bien sûr le change avec le dollar [10]. Divers commerçants acceptaient les CyberBucks dans le cadre de cette expérience.

Mais les CyberBucks ne constituaient qu'une monnaie d'essai, qui a périclité en octobre 1995 lorsque la Mark Twain Bank, une petite banque du Missouri, a lancé sa propre version du protocole en partenariat avec DigiCash. Contrairement à l'essai précédant, l'unité échangée était adossée au dollar étasunien. Bien que l'expérience des CyberBucks ne se soit pas techniquement arrêtée là, leur valeur s'est effondrée à cause de cette nouvelle [11].

Par la suite, DigiCash a conclu des partenariats avec différentes banques

pour s'inscrire dans le milieu financier traditionnel. Entre 1996 et 1998, six banques situées aux quatres coins du monde ont suivi la Mark Twain Bank : la Merita Bank en Finlande, la Deutsche Bank en Allemagne, l'Advance Bank en Australie, la Bank Austria en Autriche, la Den norske Bank en Norvège et le Crédit Suisse en Suisse. On lui promettait alors un avenir radieux [12].

C'était toutefois sans compter sur le caractère de David Chaum, qui était têtu, suspicieux et souhaitait garder le contrôle sur son entreprise [13]. Ainsi, ce dernier a refusé des partenariats avec de grands acteurs comme ING et ABN AMRO (deux des trois plus grandes banques néerlandaises à l'époque), Visa, Netscape et Microsoft. Finalement, il a dû, sous pression des actionnaires et des employés, quitter son poste de PDG pour devenir directeur technique et céder sa place à Michael Nash, ancien employé de Visa, en 1997. Le siège social de DigiCash a été déménagé en Californie et l'entreprise est par conséquent devenue une société étasunienne.

Le 17 septembre 1998, la Mark Twain Bank (rachetée par la Mercantile Bancorporation en 1996) a annoncé abandonner eCash, ce qui a provoqué la fin de DigiCash. Le 3 novembre, l'entreprise est entrée en faillite et a été placée sous la protection du chapitre 11 aux États-Unis, de sorte que ses possessions ont été progressivement revendues au fil des années, dont ses brevets en 2002. Avec DigiCash, c'était le concept même d'eCash qui disparaissait de la circulation.

En 1999, Chaum a expliqué les raisons de l'échec de sa société, à savoir le manque d'adoption dû à la difficulté d'utilisation. Cette disparition a progressivement laissé les cartes de paiement et PayPal triompher.

La fin de DigiCash a ainsi laissé un vide sur le marché de l'argent liquide numérique. Mais la demande n'a jamais disparu, de sorte qu'on pouvait pressentir qu'il réapparaîtrait d'une façon ou d'une autre. Tel que le prédisait Milton Friedman, prix Nobel d'économie et fondateur de l'École de Chicago, en 1999, au micro de la National Taxpayers Union Foundation :

> « Je pense qu'Internet va devenir l'une des forces majeures qui va réduire le rôle de l'État. La seule chose qui manque, mais qui sera bientôt développée, c'est un argent liquide électronique fiable, une méthode qui permette de transférer des fonds de A à B sur Internet sans que A connaisse B ou que B connaisse A [14]. »

libtech-l : révolutionner la monnaie

Après l'échec d'eCash en octobre 1998, l'idée d'un argent liquide numérique réel a progressivement été délaissée par les cypherpunks, qui se sont

contentés pour la plupart des expériences de monnaie privée et des systèmes de paiement existants. Mais ce n'était pas le cas de tous les membres du mouvement. Un petit nombre d'entre eux s'est ainsi regroupé sur une liste de diffusion privée appelée libtech-l où ils ont pu parler de comment la monnaie évoluerait.

La liste libtech-l, créée en 1994 par Nick Szabo [15], avait pour but, comme son nom l'indique, d'héberger des discussions sur les techniques libératoires, à même de protéger la liberté individuelle face à l'autorité, dans l'esprit des mouvements extropien et cypherpunk dont les membres étaient par ailleurs des participants. On pouvait y retrouver notamment les interventions des cypherpunks Wei Dai et Hal Finney, ainsi que celles des économistes Larry White et George Selgin. Ces cinq individus formaient le noyau dur de cette liste privée, dont émergeraient plusieurs idées de monnaie numérique.

Nicholas J. Szabo, dit Nick Szabo, était un informaticien américain d'origine hongroise. Extropien, puis cypherpunk, il s'était notamment illustré par son implication dans le combat contre la puce Clipper. En 1994, il avait formalisé la notion de *smart contract*, qu'il avait définie comme « un protocole de transaction informatisé qui exécute les termes d'un contrat [16] », et l'avait approfondie dans les années qui ont suivi.

Nick Szabo avait une personnalité curieuse et éclectique, de sorte qu'il s'intéressait à une multitude de domaines, tels que l'informatique, l'économie, la politique et la biologie, et écrivait de manière prolifique à leur sujet [17]. Il avait un intérêt particulier pour le droit, dont il possédait une conception libérale et jusnaturaliste, un intérêt qui le pousserait par la suite à retourner étudier et à obtenir un diplôme dans la discipline en 2006.

Il avait travaillé pendant six mois comme consultant pour DigiCash à Amsterdam vers 1995. Il y avait appris le rôle néfaste (et, finalement, fatal) des tiers de confiance. C'est de cette expérience que provenait son obsession pour la minimisation de la confiance, qu'il s'efforçait à mettre en valeur au sein de ses travaux [18].

Hal Finney, comme déjà indiqué dans le chapitre précédent, était un informaticien et cryptographe qui vivait dans la région de Los Angeles. Extropien et cypherpunk de la première heure, il travaillait alors pour Phil Zimmermann sur le développement de PGP, officieusement depuis 1992, puis officiellement à partir de 1996. Hal Finney s'était aussi passionné pour les idées de David Chaum dont son fameux eCash [19].

Wei Dai était un jeune cryptographe sino-américain vivant à Seattle. Ayant fui la Chine communiste et émigré aux États-Unis avec ses parents à l'âge de

10 ans, il avait réussi à se faire une place dans le monde du travail et avait été rapidement engagé par Microsoft, où il avait participé à l'élaboration de plusieurs brevets. Il avait découvert le mouvement cypherpunk en 1994 et s'y était joint. Le jeune prodige avait contribué au domaine de la cryptographie notamment avec Crypto++, une bibliothèque de fonctions cryptographiques en C++, et Pipenet, un protocole de communication anonyme. Il s'était intéressé aux monnaies numériques et aux contrats autonomes à partir de 1995, et avait conceptualisé un modèle de crédit anonyme en 1997. En 1998, Wei Dai disait être « fasciné par la crypto-anarchie de Tim May », où « l'État [n'était] pas temporairement anéanti mais définitivement oublié et inutile » et où « la violence [était] impossible parce que ses participants ne [pouvaient] pas être reliés à leur vrai nom ou à leur localisation géographique [20] ».

Lawrence H. White, dit Larry White, et George A. Selgin étaient deux économistes ayant été formés dans des universités prestigieuses. Ils étaient tous les deux inspirés par les idées de l'école autrichienne d'économie, sans pour autant y adhérer pleinement. Ils avaient été marqués par les travaux de Friedrich Hayek, et notamment par son ouvrage *The Denationalization of Money* publié en 1976 qui faisait l'apologie de la concurrence absolue dans le domaine monétaire et bancaire. C'est pourquoi, à partir des années 80, ils s'étaient évertués à promouvoir le système de la banque libre dans lequel des monnaies privées pourraient être librement émises par des sociétés financières, menant à un équilibre de marché.

Ces individus, présents sur la liste libtech-l, souhaitaient améliorer la monnaie. Ils avaient vu la chute de DigiCash et l'échec d'eCash, et étaient conscients des problèmes liés aux tiers de confiance. C'est ainsi que Wei Dai, Nick Szabo et Hal Finney ont tous les trois développé leur propre concept de monnaie numérique : Wei Dai a imaginé un concept appelé b-money, Nick Szabo a mis au point un modèle nommé bit gold et Hal Finney a construit le système RPOW.

Leurs projets se fondaient sur la notion de preuve de travail, une notion qui avait été mise en pratique en 1997 par Adam Back avec son algorithme Hashcash, dont le but initial était de fournir un moyen de lutter contre le courrier électronique indésirable [21]. Le cypherpunk britannique avait pensé à en faire la base d'une monnaie numérique, mais il avait conscience que les preuves de travail ainsi obtenues ne pouvaient pas être transférées d'une manière pleinement distribuée (à cause du problème de la double dépense) et qu'il fallait par conséquent passer par un système de monnaieries à la eCash [22].

L'idée d'utiliser ce type de preuve de travail comme base de la devise était

répandue. Par exemple, en 1996, Ronald Rivest et Adi Shamir avaient décrit MicroMint, un système de micropaiement centralisé dont les pièces devaient être impossibles à contrefaire grâce à la production de preuves de travail. Mais elle manquait d'un bon agencement qui puisse lui donner vie de manière robuste et durable.

Le concept b-money

Le premier concept de monnaie numérique à être sorti de la liste libtech-l était b-money, proposé par Wei Dai. Il s'agissait d'un concept de protocole décentralisé gérant une unité de compte du même nom, la b-money, dont la valeur était censée suivre le cours d'un panier de marchandises.

Wei Dai a travaillé sur son idée à partir de 1995. Comme il l'a expliqué par la suite, sa motivation était de « rendre possible l'établissement d'une économie en ligne qui soit purement volontaire, une économie qui ne puisse pas être taxée et réglementée par la menace de violence [23] ».

Le texte descriptif de b-money a été publié le 26 novembre 1998 par Wei Dai sur sa page personnelle. Il en a fortuitement partagé le lien à la liste de diffusion cypherpunk dans un courriel où il décrivait b-money comme « un nouveau protocole d'échange monétaire et d'exécution des contrats pour les pseudonymes [24] ».

Le texte était court (un peu plus de 1 000 mots) mais riche conceptuellement. Deux versions du protocole étaient décrites par Wei Dai. L'une était irréalisable mais simple, l'autre était plus complexe mais partait d'hypothèses plus réalistes.

Dans la première version du protocole, chaque participant faisait partie d'un réseau pair à pair intraçable. Chacun était identifié par un « pseudonyme numérique » (c'est-à-dire une clé publique) et chaque message transactionnel était signé par l'expéditeur et chiffré pour le destinataire. Chacun maintenait une base de données séparée qui recensait combien d'unités de b-money possédait chaque pseudonyme.

La création monétaire était ouverte à tous les participants et se faisait par preuve de travail en diffusant la solution d'un problème informatique connu et précédemment non résolu. Le nombre d'unités créées dépendait alors du coût de cet effort exprimé par rapport à un panier standard de marchandises, pouvant inclure des métaux précieux par exemple : lorsque son cours par rapport au panier de marchandises augmentait, les acteurs économiques déployaient plus de puissance de calcul pour abreuver le marché ; à l'inverse lorsque son cours

baissait, les acteurs économiques étaient incités à utiliser moins de puissance de calcul, ce qui ralentissait la production de b-money. Il s'agissait donc d'un « stablecoin » décentralisé avant l'heure [25].

Le système offrait également la possibilité de créer et d'exécuter des contrats directement sur le réseau, grâce à un procédé rudimentaire de dépôt fiduciaire. Dans un contrat, les parties impliquées étaient contraintes de mettre en jeu une caution et de désigner un arbitre qui avait pour rôle d'intervenir en cas de litige. Sans résolution à l'amiable, c'était le réseau qui devait trancher selon les éléments diffusés, la position de l'arbitre étant en théorie privilégiée.

Dans la seconde version du protocole, le registre de propriété n'était plus conservé par tout le monde, mais uniquement par un sous-ensemble de participants appelés des serveurs. Les participants à une transaction devaient alors vérifier que leur transaction avait bien été traitée en envoyant des requêtes à un échantillon aléatoire de serveurs. Puisqu'il était nécessaire de faire confiance à ceux-ci dans une certaine mesure, un mécanisme économique de preuve d'enjeu était mis en place pour faire en sorte qu'ils restent honnêtes. Chaque serveur devait déposer un montant de b-money sur un compte spécial afin d'être pénalisé en cas de mauvaise conduite, et était en outre contraint de publier régulièrement sa création de monnaie et son registre.

Le concept de b-money présenté par Wei Dai était donc assez ingénieux pour l'époque. Toutefois, il n'était pas fonctionnel et présentait quelques défauts majeurs. D'abord, la première version du protocole était impossible à mettre en place à grande échelle, notamment parce qu'elle ne résistait pas à la multiplication excessive des identités (attaque Sybil), chacun pouvant ajouter facilement de nouveaux ordinateurs sur le réseau. Ensuite, la seconde version semblait plus réaliste, mais avait pour effet de centraliser le système en un petit nombre de serveurs, le rendant ainsi plus vulnérable aux attaques et à la corruption. Enfin, la stabilité par rapport à un panier de marchandises aurait requis ce qu'on appelle aujourd'hui un système décentralisé d'oracles, ce qui est un problème complexe à résoudre [26].

b-money a attiré l'attention des cypherpunks, et en particulier celle d'Adam Back. Néanmoins, Wei Dai n'a jamais implémenté son modèle, non seulement parce qu'il était dysfonctionnel, mais aussi à cause de sa désillusion à l'égard de la cryptoanarchie. Comme il l'a affirmé en 2014 :

> « Je n'ai pris aucune mesure pour coder b-money. Cela a en partie été dû au fait que b-money n'était pas encore un modèle complètement réalisable. Mais si je n'ai pas continué à travailler sur ce modèle, c'est parce que j'étais un peu désenchanté par la cryptoanarchie au moment où j'ai fini d'écrire b-money, et

> que je ne prévoyais pas qu'un système comme celui-ci, une fois mis en œuvre, pourrait attirer autant d'attention et d'utilisation en dehors d'un petit groupe de cypherpunks inconditionnels [27]. »

Le modèle bit gold

Le deuxième modèle qui a émergé de la liste libtech-l était le système bit gold. Celui-ci était censé gérer la création et les échanges d'une ressource virtuelle appelée le bit gold. Contrairement à l'e-gold qui était garanti par de l'or physique, ou la b-money indexée en théorie sur un panier de marchandises, le bit gold ne devait être adossé à aucun autre bien, mais posséder une rareté infalsifiable intrinsèque, et constituer ainsi un or intégralement numérique.

C'est au cours de l'année 1998 que Nick Szabo a développé son idée de bit gold, qu'il a décrite initialement sur libtech-l, avant d'héberger une ébauche de livre blanc en 1999 sur son site personnel [28]. Il a présenté bit gold au grand public en décembre 2005 dans un article publié sur son blog Unenumerated [29]. La logique derrière bit gold était de minimiser la confiance dans le but de reproduire autant que possible la cherté de production des métaux précieux dans le cyberespace.

L'élément central du protocole était que la création monétaire se faisait par preuve de travail : les morceaux de bit gold étaient créés grâce à la puissance de calcul des ordinateurs [30]. Chaque solution était calculée à partir d'une autre, ce qui conduisait à former une chaîne de preuves de travail. Les acteurs responsables de cette production étaient appelés des « mineurs » par Szabo.

La date et l'heure de production de ces preuves de travail étaient certifiées au moyen de serveurs d'horodatage multiples. Cette diversité, bien que peu satisfaisante, permettait de limiter le risque lié à un service particulier.

La garantie de la possession et des échanges se faisait par le biais d'un registre public de titres de propriété. Les utilisateurs étaient identifiés par leur clé publique et signaient les transactions grâce à leur clé privée. Le registre était vérifié et maintenu par un réseau de serveurs appelé « club de propriété », serveurs qui se mettaient d'accord par un algorithme de consensus : le *Byzantine Quorum System* de Malkhi et Reiter. Ainsi, n'importe qui pouvait se référer à ce registre pour connaître le propriétaire d'un morceau de bit gold.

Il est intéressant de noter que les trois éléments constitutifs de bit gold – les preuves de travail, leurs horodatages et le registre de propriété – étaient séparés. En particulier, ils étaient pris en charge par des acteurs différents : les mineurs, les serveurs d'horodatage et les membres du club de propriété. Plus tard, dans Bitcoin, ces trois éléments seraient combinés en un seul et même

concept : la chaîne de blocs.

Malgré sa volonté de minimiser la confiance, le système imaginé par Szabo possédait quelques problèmes conceptuels. Tout d'abord, la façon dont étaient produits les morceaux de bit gold faisaient qu'ils n'étaient pas fongibles, c'est-à-dire qu'ils ne pouvaient pas être mélangés entre eux, et devaient donc être évalués sur un marché, de sorte à pouvoir être utilisés pour servir de base à une réelle unité de compte homogène. Ensuite, bit gold faisait usage de serveurs d'horodatage centralisés, qui formaient des points de défaillance uniques non négligeables. Enfin, le système reposait sur un algorithme de consensus dit « classique » qui requérait que les membres du club de propriété soient choisis à l'avance, qu'ils soient connus de tous, et que 66 % d'entre eux se comportent correctement.

À l'époque, bit gold était pensé comme un système de règlement permettant de gérer une monnaie de réserve rare, et au-dessus duquel serait construite une économie bancaire libre, si possible utilisant le modèle chaumien. Nick Szabo a longtemps réfléchi à comment mettre en application son idée, redemandant même de l'aide en avril 2008 dans un commentaire sur son blog [31]. Szabo n'a jamais pu mettre en œuvre son concept, contrairement à Hal Finney qui a essayé au moyen de son système RPOW.

Le système RPOW

Hal Finney a repris le concept de Nick Szabo et l'a simplifié pour l'implémenter dans un système inédit : celui des preuves de travail réutilisables ou *Reusable Proofs of Work*, abrégées en RPOW, qu'il a décrit le 15 août 2004. Ce système se basait sur un serveur transparent qui permettait de rendre transférables les preuves de travail produites par Hashcash. Ainsi, le modèle de sécurité ne venait pas d'un réseau distribué comme dans les cas de b-money et de bit gold [32].

Dans ce système, les jetons de preuve de travail réutilisable étaient gérés par un serveur qui se chargeait de les signer à l'aide du chiffrement RSA. Ils étaient fabriqués par la production d'une preuve de travail via Hashcash, ou bien à partir d'un jeton de RPOW précédent. Chaque jeton de RPOW se composait d'une valeur (définie comme une puissance de 2) et des données relatives à la signature du serveur. Un utilisateur pouvait par conséquent vérifier lui-même l'intégrité du jeton.

Le système RPOW reposait sur l'utilisation d'un serveur central qui s'occupait de détruire et de recréer les preuves de travail impliquées dans chaque

opération, notamment en vérifiant qu'elles ne faisaient pas l'objet d'une double dépense. Afin d'assurer la divisibilité de l'unité de compte, le système permettait de séparer une RPOW en plusieurs RPOW de valeur moindre et de combiner plusieurs RPOW pour en obtenir une seule.

Lors d'un paiement, l'expéditeur donnait ses jetons de RPOW au destinataire, qui s'empressait de communiquer avec le serveur pour recevoir un ou plusieurs nouveaux jetons, dont la valeur globale était égale à la valeur en entrée. Le fonctionnement des RPOW était ainsi similaire à celui des billets numériques dans eCash : les jetons de RPOW reposaient sur les informations qu'ils contenaient et pouvaient être transférés de manière confidentielle, mais chaque transaction demandait d'interagir avec le serveur pour garantir l'absence de double dépense.

Le modèle de sécurité reposait sur le type de serveur mis en place : il s'agissait d'un « serveur transparent [33] » utilisant le cryptoprocesseur IBM 4758 Secure Cryptographic Coprocessor, un cryptoprocesseur de haute sécurité résistant aux falsifications, qui permettait, par un procédé d'authentification conçu par IBM, de vérifier quels programmes étaient exécutés sur la machine. De cette manière, un utilisateur externe pouvait s'assurer à tout instant que le serveur RPOW faisait fonctionner le bon programme, dont le code était par ailleurs disponible publiquement.

Avec son système RPOW, Hal Finney tentait ainsi de réduire la confiance requise à un minimum. Le système était confidentiel dans le sens où l'utilisateur n'avait jamais à s'identifier auprès du serveur et pouvait communiquer avec lui de manière chiffrée. La transparence du serveur permettait, autant que faire se peut, de s'assurer que le système n'était pas corrompu. En particulier, on pouvait rigoureusement supposer que la quantité de jetons de RPOW dépendait d'une production réelle de preuves de travail, propriété qui permettait d'assimiler les jetons de RPOW à de l'or. Il s'agissait, en somme, d'une mise en œuvre partielle du bit gold de Nick Szabo.

Le système a été lancé en production le même jour que sa description, le 15 août 2004. Hal Finney l'a annoncé sur la liste des cypherpunks et l'annonce a été retransmise sur la liste de Metzdowd.com par Robert Hettinga. Le système a été mis à jour plusieurs fois pour améliorer son fonctionnement et est resté opérationnel pendant des mois.

Hal Finney a présenté son système à la CodeCon 2005 organisée à San Francisco. Il y a fait part des usages qu'il envisageait pour RPOW à savoir le transfert de la valeur, la régulation du courrier indésirable (dans la droite lignée de Hashcash), le commerce dans les jeux vidéos, le jeu d'argent en

ligne comme le poker, et l'anti-parasitisme sur les protocoles de partage de fichiers comme BitTorrent [34]. Fidèle à son optimisme, Hal Finney envisageait un avenir prometteur pour RPOW et comptait notamment multiplier le nombre de serveurs autour du monde, une fois que son déploiement initial serait réalisé.

Toutefois, RPOW présentait des défauts intrinsèques qui peuvent expliquer pourquoi il n'a pas rencontré le succès escompté. L'inconvénient majeur était son modèle de sécurité qui démontrait une certaine faiblesse : le ou les serveurs devaient être connus et pouvaient être arrêtés facilement, de sorte qu'ils constituaient des points de défaillance unique. De plus, un autre inconvénient venait de sa politique monétaire qui, bien que théoriquement viable, n'était pas spécialement attractive en raison de la hausse exponentielle des performances informatiques.

De ce fait, l'utilisation réelle de RPOW a été anecdotique. Le système était loin d'être parfait et ne pouvait pas, de toute évidence, devenir un système monétaire solide. Toutefois, il a eu le mérite de constituer une preuve de concept expérimentale, quatre ans avant Bitcoin.

Le projet Ripple

Les cypherpunks n'étaient pas les seuls à essayer de construire des systèmes distribués qui puissent servir à l'échange monétaire. C'était le cas du développeur canadien Ryan Fugger, qui en 2004 a conçu un protocole de crédit distribué du nom de Ripple. Ce protocole s'inspirait du concept du système d'échange local (SEL) imaginé par Michael Linton dans les années 1980. Fugger lui-même avait participé à un tel système à Vancouver avant de concevoir Ripple. Son invention était ainsi un pur produit du localisme monétaire.

Ryan Fugger a publié le livre blanc de Ripple en 2004 [35]. Le concept se fondait sur l'idée que la monnaie était essentiellement constituée de reconnaissances de dette (*IOUs*), c'est-à-dire de crédit.

Le système Ripple s'établissait sur un réseau pair à pair dont les liens étaient des relations de crédit entre des personnes. Chaque relation était composée de deux paramètres : la dette existante, qui indiquait combien une partie devait à l'autre, et la dette potentielle, qui prenait en compte la propension à prêter et à emprunter des deux parties. Ripple constituait ainsi un système où tous les participants étaient des banquiers. Concernant la monnaie de base, le protocole pouvait gérer de multiples unités de compte (du dollar, de l'euro ou même des heures de travail), mais celles-ci devaient être converties pour être transférées dans une autre devise.

Dans Ripple, les paiements se faisaient par le routage d'une série d'emprunts. En supposant des relations de confiance entre Alice et Bob, Bob et Carole, et Carole et David, Alice réalisait un paiement de 10 $ vers David en prêtant 10 $ à Bob, et en demandant à Bob de faire de même auprès de Carole, puis à Carole de faire de même auprès de David. Le compte de David était alors crédité de 10 $ issus de la création monétaire d'Alice. Ce fonctionnement par propagation du crédit au sein d'un réseau de confiance explique le nom du projet, le mot *ripple* signifiant ondulation en anglais.

La compensation se faisait par la découverte de cycles de crédit dans le réseau. Si Bob devait 5 $ à Alice, Carole 5 $ à Bob et Alice 5 $ à Carole, alors leurs dettes mutuelles disparaissaient, ce qui permettait à tous les acteurs d'avoir une capacité d'emprunt plus grande pour recevoir de futurs paiements. Une dette pouvait également être éteinte par son règlement entre les deux parties dans l'unité de compte indiquée.

En 2006, dans l'idée de faire progresser son projet, Ryan Fugger a mis en ligne une preuve de concept appelée Ripplepay. Celle-ci était basée sur un serveur central (`ripplepay.com`) et permettait aux utilisateurs de se connecter avec une simple adresse de courrier électronique. Ryan Fugger a également créé un Google Group en janvier 2007.

Malgré l'enthousiasme de sa communauté et quelques milliers d'utilisateurs, Ripple possédait des défauts inhérents à son fonctionnement distribué. En particulier, il souffrait du « problème de l'engagement décentralisé [36] » : durant un paiement, les participants ne pouvaient pas s'engager d'une façon sûre pour assurer la chaîne de prêts [37].

Voyant que son implémentation n'allait nulle part, Ryan Fugger a laissé les rênes de son projet entre les mains des dirigeants de l'entreprise OpenCoin Inc., Chris Larsen et Jed McCaleb, en novembre 2012, qui l'avaient approché quelques mois plus tôt. Ces derniers voulaient combiner son idée avec un nouvel algorithme de consensus, développé par Jed, David Schwartz et Arthur Britto. Le résultat a été sensiblement différent du concept initial, faisant intervenir une unité de compte native, le XRP, et étant bien plus centralisé et contrôlé que ce qu'on attendrait d'un protocole de crédit universel. La société OpenCoin a été rebaptisée Ripple Labs en 2013. Ryan Fugger a finalement modifié le nom de sa preuve de concept en Rumplepay en 2020 pour éviter la confusion.

Vers Bitcoin

Tous ces concepts de monnaie numérique ont, directement ou indirectement, mené à Bitcoin, soit parce que Satoshi Nakamoto avait connaissance de ces projets, soit parce qu'il partageait les mêmes références que leurs inventeurs. Bitcoin constituait en effet l'aboutissement de ces tentatives de construire une forme de monnaie numérique native du cyberespace.

Tout d'abord, Satoshi Nakamoto était pleinement familier de l'eCash de David Chaum et avait de toute évidence lu les échanges des cypherpunks à son sujet. Dans le livre blanc de Bitcoin, il y faisait clairement référence au moment d'aborder le problème de la double dépense tout en utilisant le terme *mint* (traduit ici par monnaierie), qui était un vocable courant parmi les cypherpunks pour désigner les banques chaumiennes :

> « Une solution courante consiste à introduire une autorité centrale de confiance, ou monnaierie, qui vérifie chaque transaction pour s'assurer qu'il n'y a pas de double dépense [38]. »

De plus, Satoshi Nakamoto a explicitement reconnu la faiblesse de eCash dans ses interventions publiques et privées. Ainsi, dans un courriel adressé à la liste de diffusion p2p-research en février 2009, il réagissait à la comparaison entre Bitcoin et eCash par Martien van Steenbergen en disant :

> « Bien sûr, la plus grande différence est l'absence de serveur central. C'était le talon d'Achille des systèmes chaumiens : lorsque l'entreprise centrale fermait ses portes, la monnaie disparaissait [39]. »

En privé, il écrivait aussi à Dustin Trammell en 2009 :

> « Je pense qu'il y avait beaucoup plus de gens qui étaient intéressés [par la monnaie électronique] dans les années 90, mais après plus d'une décennie d'échecs de systèmes basés sur des tiers de confiance (Digicash, etc.), ils considèrent qu'il s'agit d'une cause perdue. J'espère qu'ils sauront distinguer que c'est la première fois, à ma connaissance, que nous essayons un système qui n'est pas fondé sur la confiance [40]. »

La dernière référence au modèle de Chaum était la première version du livre blanc datant du mois d'août 2008 qui s'intitulait de façon limpide « *Electronic Cash Without a Trusted Third Party* » (« Un argent liquide électronique sans tiers de confiance » en français) et dont le nom du fichier était `ecash.pdf` [41].

Satoshi Nakamoto s'était donc clairement intéressé à eCash avant de concevoir Bitcoin. Toutefois, ce n'était pas le cas des concepts de b-money, bit

gold et RPOW, dont il n'avait vraisemblablement pas connaissance en 2007. Ces systèmes ont cependant joué un rôle indirect dans l'histoire de Bitcoin.

Comme raconté dans le chapitre 1, dans sa préparation à la publication de son concept en août 2008, Satoshi est rentré en contact avec Adam Back, qui l'a renvoyé vers Wei Dai, car le britannique avait remarqué les similitudes de Bitcoin avec b-money. C'est à ce moment-là que Satoshi a ajouté la référence à b-money au livre blanc.

Satoshi a appris l'existence du modèle bit gold imaginé par Szabo plus tard, probablement grâce à la première intervention de Hal Finney sur la liste de diffusion le 7 novembre 2008. Ce dernier a instantanément noté la similarité entre Bitcoin et le système de Szabo :

> « Je crois aussi qu'il y a une valeur potentielle dans une forme de jeton infalsifiable dont le taux de production est prévisible et ne peut pas être influencé par des acteurs corrompus. Un tel jeton serait plus comparable à l'or qu'aux monnaies fiat. Nick Szabo a décrit il y a plusieurs années un concept qu'il appelait "bit gold", et il pourrait s'agir d'une mise en œuvre de cette idée [42]. »

La référence à bit gold a fini par être ajoutée sur la page web de Bitcoin.org au début de l'année 2009, aux côtés du lien vers le texte descriptif de b-money.

Satoshi Nakamoto a reconnu *a posteriori* la ressemblance de ces deux concepts avec son propre modèle. Le 20 juillet 2010, au sein d'une discussion sur le forum parlant de la possible suppression de l'article concernant Bitcoin par Wikipédia, il écrivait pour montrer le sérieux du projet :

> « Bitcoin est une implémentation de la b-money proposée par Wei Dai sur la liste de diffusion des Cypherpunks en 1998 et du Bitgold proposé par Nick Szabo [43]. »

Cette phrase, censée démontrer l'inscription de Bitcoin dans l'histoire de la monnaie numérique, est restée gravée dans les esprits, à tel point que la b-money et le bit gold sont régulièrement cités comme des précurseurs de la cryptomonnaie.

En revanche, Satoshi Nakamoto n'a jamais indiqué à une seule occasion qu'il connaissait le système RPOW de Hal Finney [44]. Celui-ci n'était après tout qu'un modèle eCash basé sur la preuve de travail, dont le serveur central avait la particularité d'être transparent aux yeux des utilisateurs. Néanmoins, Hal Finney a joué un rôle majeur dans les débuts de Bitcoin et a évoqué son système en 2013 sur Bitcointalk [45], de sorte que RPOW est aujourd'hui lui aussi considéré comme un prédécesseur de la découverte de Satoshi.

La proximité des idées de ces trois hommes avec Bitcoin est étonnante de

prime abord, si bien que beaucoup ont spéculé que Satoshi Nakamoto était l'un ou plusieurs d'entre eux. Ces hommes, qui ont avoué avoir découvert l'existence de Bitcoin assez rapidement (Wei Dai lorsque Satoshi l'a contacté en août 2008, Hal Finney lors de la publication du livre blanc, Nick Szabo courant 2009), avaient le profil pour avoir imaginé le concept, malgré quelques éléments contradictoires. Cependant, ils ont tous les trois démenti la chose.

Le dernier projet de monnaie numérique qui a marqué l'histoire de Bitcoin est le projet Ripple de Ryan Fugger. Même si celui-ci ne ressemblait pas vraiment à Bitcoin, il a néanmoins eu son influence sur le développement de ce dernier. Satoshi Nakamoto connaissait en effet Ripple. En février 2009, sur la liste de diffusion de la Fondation P2P, il répondait à Martien van Steenbergen qui y faisait référence :

> « En ce qui concerne les systèmes de confiance, Ripple est unique en ce qu'il répartit la confiance plutôt que de la concentrer[46]. »

Le deuxième lien entre Ripple et Bitcoin est l'implication du développeur Mike Hearn. Ce dernier s'était intéressé au Ripple de Ryan Fugger dès ses débuts et, en 2007, il avait été l'une des premières personnes à intervenir sur le Google Group nouvellement créé. En découvrant Bitcoin en avril 2009, Hearn n'a ainsi pas pu s'empêcher de demander à Satoshi Nakamoto ce qu'il pensait de ce modèle alternatif, et ce dernier lui a alors répondu que Ripple était « intéressant » dans la mesure où c'était « le seul autre système qui [faisait] quelque chose de la confiance en dehors de la concentrer au sein d'un serveur central[47] ».

Mais Ripple différait sensiblement de Bitcoin, en particulier par le fait qu'il constituait, à proprement parler, un système de crédit distribué et non pas une monnaie de base décentralisée. C'est ce qui a éloigné Ryan Fugger, qui ne voyait pas « pourquoi un bitcoin aurait une quelconque valeur, puisqu'il n'y avait apparemment rien pour le garantir », mais qui s'est finalement rendu à l'évidence que le modèle de Satoshi Nakamoto était « une excellente idée[48] ».

Bitcoin ajoutait donc la dernière pierre à l'édifice de l'argent liquide électronique. Il apportait enfin une technique permettant de construire une monnaie numérique réellement solide et durable. Le 26 janvier 2009, Zooko Wilcox-O'Hearn témoignait de cette volonté dans un article de blog, qui serait relayé quelques semaines plus tard sur Bitcoin.org. En voici le texte intégral :

> « Depuis quelque temps, je réfléchis à la manière dont des services de jeux comme *World of Warcraft* et *Second Life* (qui prétend ne pas être un jeu) ont réussi là où nous, à DigiCash, avons échoué : développer un argent liquide

> numérique programmable, pratique et largement utilisé. Le problème est que toute nouvelle monnaie de ce type est contrôlée de manière centralisée par une seule entité, ce qui limite le champ d'action des gens qui dépendent d'elle et la valeur qu'ils sont prêts à risquer dessus. Certaines pistes sont évoquées pour faciliter le change entre les monnaies, mais cette approche ne résoudra pas le problème. *Une pléthore de services centralisés concurrents n'est pas la même chose qu'un service décentralisé.* Même s'il était bon marché et commode d'échanger des LindenBucks contre de l'or de WoW, on ne ferait que revenir à l'équivalent des monnaies des États-nations modernes : des monnaies essentiellement centralisées (en raison de *l'effet de réseau*), lourdement taxées / réglementées / manipulées, et sujettes à des effondrements désastreux. Ce que je veux, c'est une monnaie que tout le monde puisse utiliser de manière pratique et peu coûteuse, mais que *personne* n'ait le pouvoir de manipuler. Je veux que personne n'ait le pouvoir de gonfler ou de dégonfler la masse monétaire ; que personne n'ait le pouvoir de surveiller, de taxer ou d'empêcher les transactions. Un véritable équivalent numérique de l'or, dans les périodes et les lieux où l'or était la monnaie universelle. Voyez l'idée de BitGold de Nick Szabo et l'idée de b-money de Wei Dai, ainsi que la récente tentative de mettre en œuvre un système de ce genre : le BitCoin de Satoshi Nakamoto [49]. »

L'aboutissement d'une quête

La conception de Bitcoin a ainsi constitué la conclusion logique de la quête de l'argent liquide numérique. D'une part, il exploitait des techniques envisagées précédemment, comme la signature numérique, l'horodatage et la preuve de travail. D'autre part, il s'inscrivait dans une lignée de systèmes ingénieux qui n'avaient pas rencontré le succès escompté à cause de leurs défauts intrinsèques, à l'instar de eCash, de b-money, de bit gold, du système RPOW et du projet Ripple.

La particularité de Bitcoin était qu'il résolvait le problème de la double dépense sans reposer sur un tiers de confiance, d'une manière jamais vue auparavant. Sa robustesse et sa simplicité permettaient d'enfin disposer d'une cybermonnaie solide et durable, qui puisse résister aux aléas de la réalité. Bitcoin représentait le Saint Graal de la monnaie numérique, trouvé par Satoshi Nakamoto en 2007 et offert au monde le 31 octobre 2008.

7

La valeur de l'information

Bitcoin est un concept de monnaie numérique libre. En tant que tel, il doit garantir la propriété des unités de compte sans nécessiter d'identification auprès d'un tiers de confiance. Il repose pour cela sur un algorithme de signature numérique qui permet d'autoriser une transaction grâce à la connaissance d'une information, la clé privée.

Pour la première fois dans l'histoire de l'humanité, Bitcoin rend ainsi possible la possession souveraine d'un bien numérique rival, c'est-à-dire de quelque chose qui ne puisse pas simplement être copiée. Puisque cette possession est exercée par la connaissance exclusive des clés privées, l'information possède plus que jamais de la valeur. Il en découle un certain nombre de conséquences qui diffèrent du modèle traditionnel de la propriété.

Dans ce chapitre technique, nous verrons comment les données sont représentées au sein de Bitcoin, comment la cryptographie et la signature numérique interviennent, ce qu'est le hachage. Puis, nous décrirons comment est réalisée la génération des clés et des adresses, ce que sont les portefeuilles et comment ils se structurent. Nous examinerons enfin les conséquences de ce modèle, à commencer par la responsabilité conférée au gardien des clés.

La représentation des données

En informatique, une information est un ensemble de données stockées sur un support matériel. Elle est communément représentée sous forme de chiffres binaires (appelés bits par contraction de l'anglais *binary digits*), pour refléter le fonctionnement de l'électronique numérique utilisée dans les ordinateurs. Les deux valeurs possibles (0 et 1) correspondent en effet à deux états électriques distincts, comme par exemple la présence ou l'absence de courant.

Dans ce contexte, l'information est essentiellement un nombre. Même si elle prend l'allure d'un contenu multimédia, une information doit être encodée pour être traitée et interprétée par les ordinateurs. Typiquement, l'encodage [1] d'un texte pourra se faire en ASCII ou en UTF-8, celui d'une image en JPEG ou en PNG, celui d'une musique en MP3 ou en FLAC et celui d'une vidéo en MPEG ou en H.264. De cette façon, tout se ramène aux nombres.

Dans notre monde moderne occidental, nous avons pour habitude de représenter les nombres au moyen d'un système de numération à 10 chiffres, fondé sur la base 10. Il s'agit d'une convention, liée au fait que nous avons longtemps compté avec nos 10 doigts. Mais ce système décimal n'est pas le seul qui existe, et l'informatique fait usage de plusieurs autres bases.

Tout d'abord, comme on l'a dit, les ordinateurs sont basés sur un système binaire, composé de deux chiffres (le 0 et le 1). Ces deux chiffres sont donc utilisés pour écrire les nombres : 0, 1, 10, 11, 100, etc. Dans ce système, le nombre 21 (base 10) s'exprime comme suit :

$$21 = 16 + 4 + 1 = \mathbf{1} \times 2^4 + \mathbf{0} \times 2^3 + \mathbf{1} \times 2^2 + \mathbf{0} \times 2^1 + \mathbf{1} \times 2^0 = \texttt{0b10101}$$

Le préfixe `0b` est usuellement placé avant le nombre pour indiquer que ce dernier est exprimé en binaire.

Un autre système de numération communément utilisé en informatique est le système hexadécimal, qui est composé de 16 chiffres, symbolisés par les 10 chiffres arabes et les 6 premières lettres de l'alphabet latin :

```
0123456789abcdef
```

Dans cette base, le « a » représente le nombre 10, le « b » 11, etc. jusqu'au « f » qui représente le 15.

Le système hexadécimal permet de condenser la représentation des données. En particulier, il est très adapté pour écrire les octets (appelés *bytes* en anglais), qui sont des ensembles de 8 bits, et qui peuvent être symbolisés par 2 caractères hexadécimaux. De cette manière, le nombre 2008 (base 10) s'écrit :

$$2008 = 1792 + 208 + 8 = 7 \times 16^2 + 13 \times 16^1 + 8 \times 16^0 = \texttt{0x7d8}$$

On place usuellement le préfixe `0x` avant le nombre pour indiquer qu'on utilise le système hexadécimal.

Dans Bitcoin, deux bases de numération supplémentaires interviennent, notamment pour représenter certaines informations capitales, comme les clés privées et les adresses. La première est la base 58. Dans ce système à 58 chiffres, les nombres sont écrits en utilisant tous les caractères alphanumériques (chiffres arabes, lettres latines minuscules, lettres latines majuscules) à l'exception des caractères `0` (zéro), `O` (o majuscule), `l` (L minuscule) et `I` (i majuscule), qui peuvent être confondus entre eux et constituer une source d'erreur. Les chiffres de cette base sont donc, dans l'ordre :

```
123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz
```

Le seconde est la base 32, moins compacte mais plus adaptée pour les codes QR. Les symboles utilisés dans cette base sont les chiffres arabes et les lettres latines minuscules, auxquels on retranche le `1`, le `b`, le `i` et le `o` pour éviter les confusions, à savoir les caractères suivants :

```
qpzry9x8gf2tvdw0s3jn54khce6mua7l
```

Ces systèmes d'encodage permettent de représenter l'information de manière brute. Cependant, elle peut également être encodée dans un format particulier incluant une somme de contrôle. Une somme de contrôle (*checksum*) est une courte séquence de données numériques calculée à partir d'un ensemble de données plus important permettant de vérifier, avec une très haute probabilité, que l'intégrité de cet ensemble a été préservée lors d'une opération de copie, de stockage ou de transmission. Celle-ci est généralement placée après l'information pour que le tout soit ensuite représenté dans la base adéquate.

Dans le cas de Bitcoin, la somme de contrôle est essentielle pour transmettre les informations sensibles, comme les clés privées et les adresses, afin qu'une faute de frappe soit détectée immédiatement. Les trois encodages qui mettent en œuvre ce type de somme de contrôle dans BTC sont les formats Base58Check, Bech32 et Bech32m. Le premier a été mis en place par Satoshi dès les débuts de la cryptomonnaie et consiste à calculer une somme de contrôle grâce à l'empreinte cryptographique tronquée de l'information. Il concerne les clés privées et les adresses dites « traditionnelles », comme par exemple l'adresse `1FjBKPQ7MTiPSDkJ2ZwPgAXUKQ8yoGbVJX`.

Les deux autres ont vu le jour en 2017 et en 2021 (respectivement). Ils font intervenir des sommes de contrôle par code BCH (Bose–Chaudhuri–Hocquenghem), qui permettent non seulement de détecter la présence d'erreurs de frappe mais aussi de les localiser. Ces formats servent à encoder (respectivement) les adresses natives de SegWit, comme par exemple `bc1q5x9a0aqmgtrucm4l5n0y8e4kxfy9xm4udhygr2`, et les clés publiques utilisées dans Taproot, telle que `bc1pqlqqhzrg60v5h87r8lugusrddgz0j306shcupthy0tdqaqurwn8qr8qsej`. Le format Bech32 est également utilisé pour encoder les demandes de paiement sur le réseau Lightning.

La cryptographie et Bitcoin

La cryptographie est la discipline mathématique qui a pour but la sécurisation de la communication en présence de tiers malveillants. Elle avait pour rôle initial de dissimuler de l'information grâce au chiffrement, mais s'est par la suite étendue à l'authentification de l'auteur d'un message (grâce à la cryptographie asymétrique) et à la vérification de données (grâce aux fonctions à sens unique). Aujourd'hui, la cryptographie permet donc d'assurer la confidentialité (chiffrement), l'authenticité (signature) et l'intégrité (hachage) de l'information transmise.

Bitcoin est un produit cryptographique. D'un point de vue technique, il repose sur des méthodes développées dans les dernières décennies du XX^e^ siècle, comme les arbres de Merkle ou la preuve de travail. D'un point de vue idéologique, il est issu du mouvement cypherpunk, qui préconisait une utilisation proactive de la cryptographie pour sauvegarder la confidentialité et la liberté des individus sur Internet. C'est dans ce double sens qu'on le désigne comme une cryptomonnaie.

Dans le contexte de Bitcoin, le chiffrement peut être utile pour protéger les clés privées ou pour envoyer des messages à d'autres utilisateurs. Dans de nombreux portefeuilles, il est courant que les clés privées soient chiffrées à l'aide d'un mot de passe (clé secrète) pour éviter qu'une personne malveillante ayant accès à l'appareil puisse dépenser les fonds. Dans Electrum par exemple, les clés privées sont chiffrées par le biais de l'algorithme symétrique AES-256-CBC.

Néanmoins, contrairement à ce qu'on imagine parfois, aucun chiffrement n'est impliqué directement dans le protocole de Bitcoin : toutes les données sont publiques en raison du fonctionnement ouvert et sans autorisation du système. Bitcoin n'est pas un produit cryptographique parce que les transactions

seraient chiffrées (elles ne le sont pas), mais parce qu'il repose sur les deux autres fonctions de la cryptographie : l'authentification grâce à la signature numérique et la vérification des données avec le hachage. La signature numérique permet d'authentifier la personne à l'origine d'une transaction pour assurer au réseau qu'il s'agit du propriétaire des bitcoins dépensés. Le hachage intervient lui dans la dérivation des clés et des adresses, dans la construction des blocs et dans le fonctionnement du minage.

La signature numérique

Bitcoin étant conçu pour l'échange de valeur, il repose de manière centrale sur les transactions. Celles-ci sont dans la plupart des cas des transferts d'unités entre deux propriétaires, même si elles peuvent prendre des formes beaucoup plus complexes comme nous le verrons dans le chapitre 12. L'unité transférée est usuellement le satoshi, qui forme la plus petite unité (indivisible) gérée par le protocole et qui correspond à un cent-millionième de bitcoin : 1 satoshi = 0,00000001 bitcoin. Elle a été nommée comme telle en hommage au créateur de Bitcoin, Satoshi Nakamoto [2].

Dans le protocole, la signature numérique est utilisée pour autoriser ces mouvements de fonds. Comme nous l'avons décrit dans le chapitre 5, ce procédé se base sur une paire de clés : une clé privée, secrète, qui *signe* le message, et une clé publique, connue de tous, qui permet de *vérifier* la signature produite. Dans le cas d'un transfert simple, le message à signer est la transaction et le signataire du message est le propriétaire des satoshis à envoyer.

L'algorithme de signature produit une signature différente pour chaque transaction. Il ne s'agit pas de se contenter de révéler un secret pour effectuer une dépense, auquel cas tout le monde sur le réseau pourrait tenter de dépenser les fonds, mais bien de produire une donnée qui puisse ensuite être vérifiée par le réseau conformément à ce qui est attendu.

Ce fonctionnement confère un rôle fondamental à la clé privée. Tout individu la connaissant peut accéder aux fonds qu'elle protège et s'en emparer. C'est pourquoi elle doit rester absolument secrète : car celui qui la connaît devient le propriétaire *de facto* des bitcoins concernés.

L'algorithme principal utilisé dans Bitcoin est ECDSA (*Elliptic Curve Digital Signature Algorithm*), une variante de DSA utilisant la cryptographie sur courbes elliptiques. L'algorithme fait appel à des notions d'algèbre complexes, mais on peut tenter d'en expliquer brièvement le fonctionnement.

La variante d'ECDSA utilisée dans Bitcoin se base sur la courbe elliptique secp256k1 [3], qui sert à dériver la clé publique de la clé privée, à signer les transactions grâce à la clé privée et à vérifier les signatures à l'aide de la clé publique. L'équation mathématique de cette courbe est $y^2 = x^3 + 7$ dont les coordonnées x et y évoluent dans le corps fini des nombres entiers modulo p, où p est un nombre premier spécifique [4] inférieur à 2^{256}.

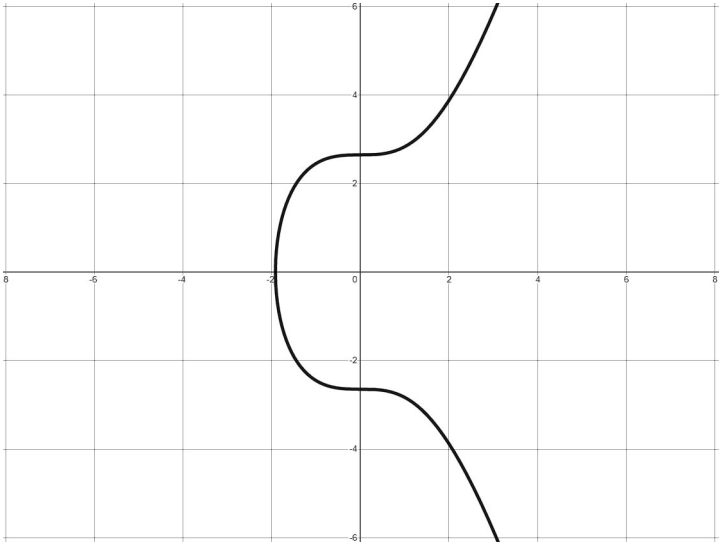

FIGURE 7.1 – Représentation graphique de la courbe secp256k1 sur les nombres réels (source : Loïc Morel, *Bitcoin démocratisé*, 2022).

Une addition est définie sur cette courbe pour faire en sorte que la somme de deux points soit également un point de la courbe [5]. La multiplication par un scalaire est définie comme étant le fait d'additionner le même point à plusieurs reprises : $m\ P = P + \ldots + P$ (m fois). En fixant un point sur la courbe, appelé point de base et noté G [6], on peut définir une opération transformant un entier d en un point de la courbe : $Q = d\ G$.

Ces opérations peuvent être représentées géométriquement sur la courbe. Par exemple, l'équivalent géométrique du doublement du point G (addition avec lui-même) consiste à tracer la tangente du point, à considérer l'intersection de cette tangente avec la courbe et à en prendre l'opposé, comme représenté sur la figure 7.2. Toutes ces opérations sont non réversibles.

En choisissant une clé privée k, on peut ainsi calculer la clé publique K qui est $K = k\ G$. Puisque la multiplication par un scalaire est non réversible,

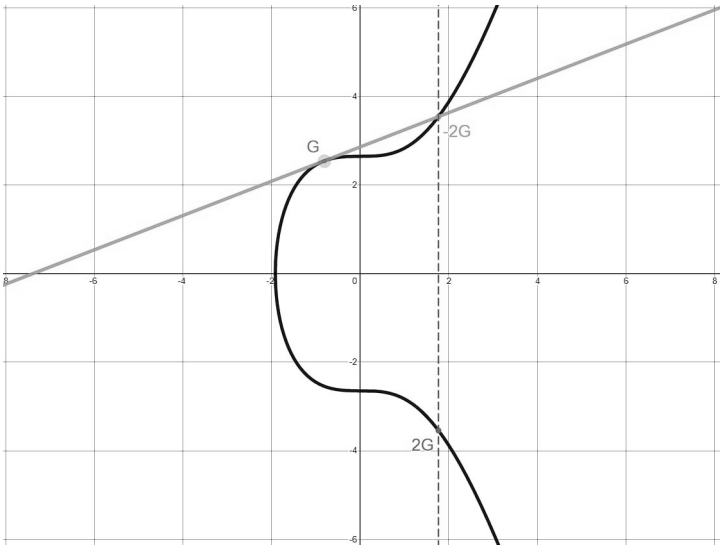

FIGURE 7.2 – Représentation géométrique du doublement du point G sur secp256k1 (source : Loïc Morel, *Bitcoin démocratisé*, 2022).

le passage de la clé privée à la clé publique constitue une fonction à sens unique. En d'autres termes, il est en pratique impossible de retrouver la clé publique à partir de la clé privée sans essayer chaque possibilité une à une.

Regardons ce que cela donne en pratique. La clé privée est un nombre choisi aléatoirement. Elle doit être comprise entre 1 et $n-1$ où n est l'ordre du point G (qui approche 2^{256}) :

$$n = \texttt{0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141}$$

Par exemple, le nombre hexadécimal suivant est tout à fait valide pour servir de clé privée :

$$k = \texttt{0x999bb87eea489b2fc6219226e7b95d9083a3b627246ea852e85567ac4d72444f}$$

La clé publique est un point de la courbe défini par $K = k\ G$. Si l'on calcule ce point à partir de la clé privée précédente, on obtient :

$$K = (\ \texttt{0xf6a6c7c39c88b767bfac4ac687c3ff32372e76c9fb633e2278e54472e300b3bd},$$
$$\texttt{0x5822f24e0fdb4e568f97a7fff246c07ba486c1756f82971765cc9cf8e45ff5e6}\ )$$

Dans Bitcoin, cette clé publique est représentée de manière sérialisée. Elle peut l'être sous forme non compressée, auquel cas elle est précédée par le préfixe `0x04`. Dans notre cas, son expression sérialisée est :

```
04 f6a6c7c39c88b767bfac4ac687c3ff32372e76c9fb633e2278e54472e300b3bd
5822f24e0fdb4e568f97a7fff246c07ba486c1756f82971765cc9cf8e45ff5e6
```

Il existe également une représentation compressée de la clé publique. Celle-ci est rendue possible par la symétrie de la courbe par rapport à l'axe des abscisses : car en effet, le fait que le point (x, y) appartienne à la courbe implique que le point $(x, -y)$ y soit aussi. Pour compresser l'information, il suffit ainsi de donner l'abscisse x et un préfixe qui vaut `0x02` si y est pair ou `0x03` si y est impair [7]. On peut ensuite retrouver grâce à l'équation de la courbe. Dans notre cas, la clé publique compressée est :

```
02 f6a6c7c39c88b767bfac4ac687c3ff32372e76c9fb633e2278e54472e300b3bd
```

Ce format permet de réduire la taille des transactions (et donc les frais) : c'est pour cela qu'il est utilisé dans la plupart des portefeuilles récents, et qu'il est imposé dans le cas de SegWit. Le format non compressé tend ainsi à disparaître, même s'il reste toujours valide dans les transactions classiques.

Dans Bitcoin, la clé publique servait initialement à recevoir les fonds directement (« *Pay to Public Key* »), de sorte qu'on la confond encore aujourd'hui avec la notion d'adresse. Toutefois, c'est son empreinte obtenue par hachage (« *Pay to Public Key Hash* »), qui sert généralement d'adresse de réception, comme nous le décrirons plus bas.

L'algorithme de signature ECDSA s'applique à un message m qui est précédemment haché et produit une signature (r, s). Il est ensuite possible de faire correspondre la signature avec la clé publique K grâce à un algorithme de vérification qui ne nécessite pas de connaître la clé k [8].

Dans Bitcoin, le message est la transaction. L'algorithme de vérification montre ainsi que la personne qui a produit la signature connaît k tel que $K = k\,G$, c'est-à-dire qu'elle est propriétaire des bitcoins. C'est ce qui permet aux nœuds du réseau de s'assurer de la validité des signatures, et par conséquent de celle de la transaction. Un exemple de signature correspondant à notre clé publique et à une transaction réalisée sur le réseau principal est [9] :

$(r, s) =$ (`0x19b83a5e354ef62e98413e6ef3f37ad0c69f75cea7daa6a352cf66f4668a9a0b`,
`0x4c13f9b6f2c8ea7af224b3f6a3d9cfdfe5085bbafa150fb1aa72a20ce7cac6b0`)

Notez que l'algorithme ECDSA présenté ici n'est pas le seul qui existe. En novembre 2021, BTC a intégré un autre algorithme, le schéma de signature

numérique de Schnorr, qui est basé sur la même courbe elliptique mais qui apporte des bénéfices majeurs. Certaines autres variantes de Bitcoin comme Monero utilisent EdDSA, un algorithme de signature basé sur une courbe d'Edwards tordue.

Le hachage

Bitcoin fait également usage du hachage. Le hachage est un procédé cryptographique permettant de garantir l'intégrité d'une information numérique. Le nom de ce procédé est issu d'une analogie avec la cuisine, où des aliments peuvent être coupés en petits morceaux et regroupés dans un hachis. Il est mis en œuvre par une fonction de hachage qui transforme un *message* de taille variable en une *empreinte* de taille fixe. Cette empreinte est aussi appelée condensat ou *hash*.

Les fonctions de hachage sont des fonctions déterministes, facilement exécutables, qui possèdent en théorie trois caractéristiques [10] :

— Elles sont irréversibles : ce sont des fonctions à sens unique construites de telle sorte qu'il est difficile de retrouver le message à partir d'une empreinte donnée (résistance à la préimage) ;
— Elles sont imprédictibles : toute modification du message initial résulte en une empreinte profondément différente, si bien qu'il est difficile de trouver une empreinte similaire ;
— Elles sont résistantes aux collisions : il est difficile de trouver deux messages dont l'empreinte résultante soit la même.

L'une des fonctions les plus connues est SHA-256, dont le nom vient de l'abréviation de *Secure Hash Algorithm* et de la taille des empreintes qu'elle produit (256 bits, soit 32 octets). Par exemple, si on considère le message « Bitcoin », le fait de l'orthographier en minuscules ou d'ajouter un point change complètement son empreinte, comme montré dans le tableau 7.1. Cette particularité permet notamment de détecter si le message comporte une erreur.

Message	**Empreinte (SHA-256)**
Bitcoin	`b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4`
bitcoin	`6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b`
Bitcoin.	`a9adf3c04d168153b296083f05015f587d7df6e0b85305b6c7beb2a69e3f4e75`

TABLEAU 7.1 – Empreintes par SHA-256 de messages légèrement différents.

Le hachage intervient à de multiples endroits dans Bitcoin : dans l'algorithme de signature (hachage du message), dans le calcul des adresses, dans la dérivation des clés, pour le calcul des sommes de contrôle, pour le calcul des identifiants des transactions et des blocs, dans la construction des arbres de Merkle dans les blocs, et enfin au cœur du minage.

Trois fonctions de hachage sont utilisées : SHA-256, qui produit des empreintes de 256 bits (32 octets) ; RIPEMD-160, dont le nom est le sigle de l'anglais *RACE Integrity Primitives Evaluation Message Digest*) et qui résulte en des condensats de 160 bits ; et SHA-512, qui hache les données en des empreintes de 512 bits.

La fonction la plus présente est le double SHA-256 (noté SHA-256d ou HASH-256), qui intervient presque partout. Il est supposé que ce doublement mis en place par Satoshi avait pour rôle la protection contre les attaques par extension de longueur. La composée de SHA-256 par RIPEMD-160 est utilisée pour le calcul des adresses. C'est le seul endroit où RIPEMD-160 intervient de manière substantielle [11]. Enfin, SHA-512 intervient dans l'algorithme de dérivation des clés mis en place dans les portefeuilles.

Les clés privées

Par essence, la clé privée est une information numérique, c'est-à-dire un nombre. Plus précisément, il s'agit d'un très grand nombre compris entre 1 et $n-1$, où n est l'ordre du point G et approche 2^{256} soit $1,1579 \times 10^{77}$. L'intervalle est considérablement grand, si bien qu'il est statistiquement impossible de tomber sur une même clé privée en la choisissant au hasard. À titre de comparaison, le nombre d'atomes dans l'univers observable est proche de 10^{80}.

La clé privée est créée au hasard, la plupart du temps grâce à des algorithmes générateurs de nombres pseudo-aléatoires permettant de reproduire le hasard de la manière la plus fidèle possible en informatique. Cette génération repose sur l'entropie informatique issue de l'appareil, c'est-à-dire la quantité d'aléatoire qu'il collecte par le biais de sources matérielles (variance du bruit du ventilateur ou du disque dur) ou de sources extérieures (mouvement de la souris, signaux du clavier, etc.). Les outils utilisés pour générer des clés privées sont le plus souvent considérés comme cryptographiquement fiables (CSPRNG).

La caractère aléatoire du procédé est fondamental, constituant la base de la sécurité du modèle. Par exemple, une personne qui choisirait le nombre 1

comme clé privée ne pourrait jamais utiliser l'adresse correspondante, car la sécurité liée à cette clé est nulle. Tous les bitcoins qui seraient déposés sur cette adresse seraient instantanément débités par un programme spécialisé [12].

Il en est de même des *brain wallets*, portefeuilles « cérébraux » reposant sur la mémorisation d'une information, qui sont souvent créés de manière non sécurisée. Les gens partent le plus souvent d'une phrase cohérente (comme une citation tirée d'un livre ou d'une chanson) de sorte à pouvoir la retenir facilement, puis la hachent et utilisent l'empreinte résultante en tant que clé privée. Cette manière de faire est hautement risquée en raison de la forte prévisibilité du langage humain, et les adresses créées comme cela ont de bonnes chances d'être vidées, comme l'a montré une enquête de BitMEX Research [13].

Cette importance du hasard se retrouve également dans l'algorithme ECDSA qui repose sur la génération d'une clé éphémère pour produire la signature. Dans le cas où cette valeur ne serait pas correctement générée, un attaquant pourrait déduire les clés privées à partir des signatures. C'est notamment ce qui s'est passé en août 2013, lorsqu'une vulnérabilité (CVE-2013-7372) a été découverte au sein de la fonction SecureRandom de Java et a affecté la sécurité de plusieurs portefeuilles logiciels sur Android [14]. L'exploitation de cette faille a mené à la perte d'au moins 55,82 bitcoins, soit 5 200 $ à l'époque.

Après avoir été générées, les clés privées doivent ensuite être encodées dans le but de faciliter leur transmission, pour l'import dans un portefeuille ou pour l'export. Dans Bitcoin, elles sont ainsi représentées grâce à l'encodage Base58Check. C'est pourquoi on parle parfois de *Wallet Import Format* (WIF).

L'encodage d'une clé suit une série d'étapes simples. Tout d'abord, la clé est préfixée par l'octet de version `0x80` qui indique qu'il s'agit d'une clé privée. Puis, un suffixe `0x01` est ajouté (ou non) pour indiquer si l'on souhaite en dériver une clé publique compressée (ou non compressée). Dans le cas de notre clé-exemple, on obtient les octets suivants :

```
80 999bb87eea489b2fc6219226e7b95d9083a3b627246ea852e85567ac4d72444f 01
```

Ensuite, la somme de contrôle est calculée en prenant les 4 premiers octets de l'empreinte par le double SHA-256 et ajoutée après l'ensemble :

```
80 999bb87eea489b2fc6219226e7b95d9083a3b627246ea852e85567ac4d72444f 01
1dd28791
```

Enfin, le tout est encodé en base 58. Dans le cas « compressé », la clé commence toujours par un K ou un L. Ici, notre clé privée s'écrit :

```
L2NJfKog9SEdoAkAkm8ZNYDcpWQop95orPepbhsTE2t5Bf1yFmYk
```

Dans le cas « non compressé » (de moins en moins utilisé), la clé commence toujours par un 5. Ici, notre clé privée devient :

```
5JywJHwyuD4YSsErniGJkrDNi87kggSZNADCEkhRyRScqfMMTEt
```

Les adresses

Dans Bitcoin, une adresse constitue en quelque sorte un numéro de compte servant à recevoir des fonds. Cette donnée est disponible publiquement sur la chaîne de bloc et n'importe qui peut en vérifier le solde. Néanmoins, un utilisateur peut générer autant d'adresses qu'il le désire afin de ne pas dévoiler l'entièreté de son activité.

De manière générale, une adresse est l'empreinte d'une clé publique (PKH), la clé publique elle-même (PK), ou bien l'empreinte d'un script (SH). Ici nous parlerons des adresses simples, dérivées de clés publiques par hachage, qui sont les plus utilisées sur le réseau BTC.

Une adresse simple est obtenue par les hachages successifs de la clé publique sérialisée par les fonctions SHA-256 et RIPEMD-160. La composée de ces deux fonctions est communément appelée HASH-160. La fonction RIPEMD-160 a été choisie par Satoshi dans le but de diminuer la longueur des adresses, car elle produisait des empreintes de 20 octets au lieu des 64 octets d'une clé publique ou des 32 octets produits par SHA-256. En notant A l'adresse, on a ainsi :

$$A = \mathrm{HASH160}(\, K \,) = \mathrm{RIPEMD160}(\, \mathrm{SHA256}(K) \,)$$

Puisque cette composée est elle-même une fonction de hachage, elle a pour particularité d'être de même une fonction à sens unique. Il est de ce fait virtuellement impossible de retrouver la clé publique à partir de l'adresse.

Le risque de collision est lui aussi statistiquement nul, même s'il y a moins d'adresses que de clés privées. La fonction de hachage RIPEMD-160 produit en effet des empreintes de 160 bits, et il existe par conséquent 2^{160} (environ $1,4615 \times 10^{48}$) adresses possibles, soit approximativement 8×10^{28} fois moins d'adresses que de clés privées. Néanmoins ce nombre est suffisamment élevé pour que le risque de tomber par hasard sur la même adresse soit complètement négligeable [15].

Comme une clé publique admet deux représentations sérialisées (compressée et non compressée), il est possible de calculer deux empreintes. Nous

nous focalisons ici sur la représentation compressée. L'empreinte de notre clé publique compressée est :

```
a18bd7f41b42c7cc6ebfa4de43e6b63248536ebc
```

On peut en dériver trois adresses de type différent : une adresse traditionnelle, une adresse SegWit native et une adresse SegWit imbriquée. Dans les trois cas, le principe est le même, bien que l'usage spécifique de l'empreinte dans le protocole diffère.

L'adresse traditionnelle est obtenue grâce à un encodage de l'empreinte en Base58Check avec l'octet de version `0x00`. À cause de cet octet de version, les adresses traditionnelles simples commencent toujours par un 1 (purement symbolique car il vaut 0 en base 58). Notre adresse est :

```
1FjBKPQ7MTiPSDkJ2ZwPgAXUKQ8yoGbVJX
```

Ce type d'adresse est appelé P2PKH (*Pay to Public Key Hash*) et a été le premier type d'adresse dans Bitcoin.

L'adresse SegWit native est encodée grâce au format Bech32. Celui-ci inclut un préfixe indiquant le réseau (`bc` pour BTC) et un séparateur (1). De manière similaire à l'encodage des adresses traditionnelles, il s'agit de prendre l'information brute (la « charge utile »), de la préfixer avec l'octet de version (`0x00` pour la première version de SegWit), de calculer une somme de contrôle et d'exprimer le tout dans la base appropriée, à savoir la base 32. Ce procédé fait que l'adresse résultante commencera toujours par `bc1q`. Dans le cas de notre empreinte de clé publique, on obtient :

```
bc1q5x9a0aqmgtrucm4l5n0y8e4kxfy9xm4udhygr2
```

Ce type d'adresse est appelé P2WPKH (*Pay to Witness Public Key Hash*).

Enfin, on peut également inclure cette donnée sous la forme d'un script dans une adresse P2SH, créant une adresse SegWit dite « imbriquée ». Le script, composé de l'octet de version de SegWit (`0x00`) et de l'empreinte, est haché pour constituer la nouvelle adresse. Comme dans le cas de toutes les adresses P2SH, l'empreinte résultante est encodée en Base58Check avec l'octet de version `0x05`. Cet octet de version a pour conséquence de faire commencer l'adresse par un 3. Notre empreinte devient ici :

```
3JqPHkGuvW7nsUJDgm5CPSNUb47WczCC5e
```

Ce type d'adresse est appelé P2SH-P2WPKH (*P2SH-nested Pay to Witness Public Key Hash*). Nous aborderons plus en détail les différents schémas de script qui sous-tendent ces types d'adresse dans le chapitre 12.

Une fois qu'elles ont été encodées, les adresses peuvent être partagées facilement d'une personne à une autre. Grâce à la somme de contrôle, faire une faute de frappe ne crée théoriquement pas de risque, car le logiciel la détectera et refusera de procéder au paiement. Les adresses sont aussi souvent représentées par des codes QR (voir figure 7.3), plus adaptés pour l'interaction avec un téléphone multifonction.

1FjBKPQ7MTiPSDkJ...

bc1q5x9a0aqmgtruc...

3JqPHkGuvW7nsUJD...

FIGURE 7.3 – Codes QR des adresses.

En résumé : lorsqu'un utilisateur veut recevoir un paiement, il génère une clé privée, en dérive une clé publique et crée à partir de celle-ci une adresse ; il communique son adresse à un autre utilisateur qui lui envoie des fonds ; il peut ensuite dépenser les fonds reçus en signant une transaction à l'aide de sa clé privée. Le réseau pair à pair de Bitcoin vérifie alors que la signature est conforme à la clé publique.

La clé publique n'est révélée au réseau que lors de la transaction. Cela implique que les fonds sont protégés face à l'éventualité d'une mauvaise implémentation de l'algorithme de signature (comme dans le cas de l'exploitation de la faille au sein de SecureRandom en 2013) ou de la compromission généralisée d'ECDSA (par un ordinateur quantique par exemple). Il s'agit d'un bénéfice secondaire issu de l'utilisation de nouvelles adresses à chaque paiement.

Au-delà de BTC, les autres cryptomonnaies ont leur encodage propre pour les adresses, qui n'est souvent qu'une variante du standard modifiant la version ou le préfixe. Ainsi, dans Litecoin, les adresses traditionnelles commencent par un `L` (comme par exemple `LZx8abhwS7xSh2STChvgxBbEXcWG1AZ2iR`) et les adresses SegWit par un `ltc1q` (comme par exemple `ltc1q5x9a0aqmg trucm4l5n0y8e4kxfy9xm4uft7vm6`).

Bitcoin Cash possède également son propre format d'adresse, appelé CashAddr, qui s'inspire fortement du format Bech32. Ce format a été introduit pour différencier les adresses BTC des adresses BCH. Une adresse BCH est simplement une représentation alternative du type P2PKH : dans ce format, l'adresse `1FjBKPQ7MTiPSDkJ2ZwPgAXUKQ8yoGbVJX` devient `bitcoincash:qzsch4l5rdpv0nrwh7jduslxkceys5mwhs03g7e6dq`.

Les portefeuilles

Un portefeuille, de l'anglais *wallet*, parfois aussi qualifié de portemonnaie, est un procédé de stockage des clés privées donnant accès aux pièces de cryptomonnaie de l'utilisateur. Ce procédé est souvent combiné avec la gestion de la cryptomonnaie : sa réception avec la lecture de la chaîne de blocs et son envoi avec la production des signatures. Le moyen utilisé peut être une simple feuille de papier ou un fichier informatique, mais il s'agit généralement d'un logiciel sur mobile ou ordinateur, ou bien d'un appareil spécialisé.

Un portefeuille est donc par essence un *porte-clés*. Son rôle principal est de conserver les clés privées dans le temps pour garantir la propriété des bitcoins. La plupart du temps, les clés sont générées par ces portefeuilles de manière déterministe à partir d'une phrase de récupération de 12 à 24 mots. L'utilisateur doit donc conserver précieusement cette phrase sur un autre support, dans l'éventualité de retrouver ses fonds si son appareil est perdu, cassé ou volé.

En revanche, un compte auprès d'un dépositaire comme une plateforme de change centralisée n'est pas un portefeuille à proprement parler, car ces services conservent les clés privées de leurs utilisateurs à des fins de sécurité et de facilité d'usage. Ainsi, des applications qui ressemblent à s'y méprendre à des portefeuilles, comme le *Wallet of Satoshi* ou l'application Coinbase, n'en sont pas.

On peut classifier les portefeuilles existants en deux grandes catégories : les portefeuilles « à chaud » (*hot wallets*) qui sont connectés à Internet lors de leur utilisation, et les portefeuilles « à froid » (*cold wallets*) qui ne le sont jamais de manière directe. De plus, on retrouve au sein de ces deux catégories différents types de portefeuilles, qui possèdent chacun leurs qualités et leurs défauts.

Le stockage à chaud des clés privées, qui utilise des appareils directement connectés à Internet, concerne notamment les portefeuilles logiciels (*software wallet*) que l'on peut installer sur un mobile, une tablette ou un ordinateur généraliste. Ces logiciels mettent généralement leur code source à disposition

du public pour des raisons évidentes de sécurité. Les clés sont conservées sur l'ordinateur et sont généralement chiffrées. Cette catégorie inclut les logiciels de nœud complet, les portefeuilles légers, les extensions de navigateur et les portefeuilles web.

L'implémentation de nœud complet (*full node implementation*), aussi appelée client complet, est le premier type de portefeuille qui est apparu et le seul qui existait du temps de Satoshi. Comme son nom l'indique, un tel logiciel réalise toutes les opérations nécessaires au maintien d'un nœud sur le réseau pair à pair : il télécharge l'intégralité de la chaîne de blocs et il vérifie et relaie les transactions non confirmées et les blocs. Bitcoin Core est le logiciel de nœud complet le plus connu. Cependant, en raison de la difficulté d'utilisation, ce type de portefeuille n'est généralement plus utilisé directement, les néophytes préférant utiliser des applications plus légères et les utilisateurs confirmés privilégiant des solutions plus sécurisées, qu'ils peuvent ensuite connecter à leur nœud personnel s'ils le souhaitent.

Le portefeuille léger (*lightweight wallet*), aussi appelé portefeuille SPV (pour *Simplified Payment Verification*), est un logiciel qui ne télécharge pas la chaîne de blocs mais qui procède à une vérification simplifiée des transactions à partir de la chaîne des entêtes qui ne nécessite que peu de ressources informatiques. Ce type de portefeuille est particulièrement adapté aux petits appareils comme les téléphones. Le logiciel peut interagir avec l'ensemble des nœuds complets du réseau pair-à-pair, comme le fait BRD (anciennement appelé *breadwallet*), mais il passe de manière générale par l'intermédiaire d'une infrastructure de serveurs dédiés qui rendent l'utilisation plus agréable, comme c'est le cas d'Electrum ou de Sparrow. Ce type de portefeuille garantit la sûreté des fonds, mais peut avoir un effet dommageable à d'autres niveaux, notamment en ce qui concerne la confidentialité. L'utilisateur peut également choisir de connecter son portefeuille à son propre nœud complet.

Un portefeuille peut aussi prendre la forme d'une extension de navigateur web, que ce soit sur Chrome, Firefox ou Brave. Contrairement aux clients légers, ces portefeuilles ne procèdent pas toujours à la vérification des transactions et font confiance au serveur auquel elles sont connectées.

Enfin, le dernier type de stockage à chaud est le portefeuille web. Ces derniers sont des interfaces en ligne permettant de gérer des fonds. Contrairement aux plateformes de change, l'utilisateur garde le contrôle de ses clés privées lorsqu'il passe par ce genre de service : celles-ci sont gérées par le navigateur et ne sont jamais révélées à autrui. Le portefeuille de ce type le plus connu est celui de Blockchain.com.

Mais ces solutions à chaud ne sont pas les seules, et il existe des méthodes de conservation à froid des clés privées, qui sont coupées de tout accès direct à Internet. Cette conservation a le mérite de réduire la surface d'attaque et donc le risque de vol par piratage informatique. Il s'agit de la solution recommandée pour mettre en sécurité des grosses sommes de cryptomonnaie.

Dans l'absolu, il faut disposer d'un appareil qui reste constamment hors-ligne pour générer les clés et les adresses. Cet appareil peut être un vieil ordinateur non connecté à Internet ou bien un appareil spécialisé. Les deux méthodes principales pour réaliser du stockage à froid sont le portefeuille papier et le portefeuille matériel.

Le portefeuille papier (*paper wallet*) est le type de portefeuille le plus simple qu'on puisse imaginer : les clés privées générées hors-ligne (et les adresses qui leur correspondent) sont écrites sur une feuille de papier. L'information écrite peut également être une phrase mnémotechnique. Le portefeuille papier présente néanmoins un inconvénient majeur : l'impossibilité de signer des transactions sans l'importer dans une interface connectée à Internet. Cette méthode n'est pas du tout pratique, car l'utilisateur ne peut pas signer de transaction sans compromettre la sécurité de son portefeuille et doit se contenter de recevoir des paiements. Pour résoudre ce problème, il existe ce qu'on appelle les portefeuilles matériels.

Le portefeuille matériel (*hardware wallet*) est un appareil dont la spécificité est de générer et de conserver les clés privées de manière isolée et de permettre de signer des transactions hors-ligne. Il s'agit aujourd'hui de la solution la plus sûre de détenir du bitcoin. Ces portefeuilles sont construits de telle manière que quelqu'un qui s'en emparerait ne pourrait pas dépenser les fonds sans le mot de passe de l'utilisateur.

Il existe une diversité de portefeuilles matériels. Les plus connus sont les portefeuilles de Satoshi Labs (le Trezor One et le Trezor model T) et ceux de Ledger (le Nano S et le Nano X), qui sont les modèles les plus anciens et les plus reconnus. Ceux-ci peuvent être connectés à l'ordinateur de manière sûre et les transactions sont toujours signées sur l'appareil. Certains autres perfectionnent la sécurité en étant physiquement isolés de tout ordinateur tiers (grâce à un air gap) comme la Cold Card Mk4. D'autres portefeuilles mettent l'accent sur la facilité d'utilisation comme les cartes Satochip qui se basent sur des smartcards.

Tous les portefeuilles impliquent une certaine confiance : vous devez vous fier au logiciel que vous utilisez pour conserver vos bitcoins, au programme dont vous vous servez pour générer un portefeuille papier, au matériel spé-

cialisé dans le stockage à froid. Bien entendu, les solutions ouvertes peuvent être considérées comme plus sûres dans le sens où d'autres personnes que les concepteurs ont pu vérifier le produit final : c'est notamment le cas de nombreux portefeuilles logiciels et de l'infrastructure matérielle des portefeuilles Trezor. Dans tous les cas, une composante basée sur la réputation subsiste.

De manière générale, chaque type de portefeuille possède une utilité : c'est donc à l'utilisateur de déterminer quel portefeuille conviendra mieux à ses besoins.

La dérivation des clés

Durant les débuts de Bitcoin, les clés privées étaient générées aléatoirement par le logiciel à chaque utilisation. Il s'ensuivait que les clés étaient conservées dans un fichier, appelé `wallet.dat`, stocké sur le disque dur de l'ordinateur. Cela rendait la perte des clés plus probable.

Néanmoins, les portefeuilles modernes ne fonctionnent plus comme cela. Les clés et les adresses sont dérivées de manière déterministe à partir d'une seule information générée aléatoirement, qui se présente sous la forme d'une phrase mnémotechnique allant de 12 à 24 mots. Ces mots peuvent être des mots en anglais, en français ou dans une autre langue.

elder process crowd gentle proof taxi bean patient around warm source boil

De ce fait, c'est la conservation de cette phrase, appelée phrase de récupération, qui garantit la sécurité des bitcoins. Cette phrase vous permet de retrouver vos fonds si votre appareil est volé ou cassé. C'est pourquoi elle doit rester secrète.

Ce type de portefeuille est parfois appelé HD wallet pour *Hierarchical Deterministic Wallet* : portefeuille déterministe hiérarchique. Le concept a été développé pour Bitcoin à partir de 2011. Il a été standardisé en 2012 au sein du BIP-32 écrit par Pieter Wuille, et des propositions BIP-39 et BIP-44 écrites par Marek Palatinus et Pavol Rusnak. Il a été élargi aux autres cryptomonnaies en 2014.

En règle générale, la phrase secrète, ou phrase de récupération, est générée par l'appareil de l'utilisateur, qu'il s'agisse d'un téléphone mobile, d'un ordinateur ou d'un portefeuille matériel. Pour ce faire, une entropie est d'abord créée par l'appareil de manière pseudo-aléatoire. L'information, qui possède un nombre de bits précis, est ensuite enrichie d'une somme de contrôle de quelques bits, permettant de détecter les erreurs de saisie, et l'ensemble est

divisé en segments de 11 bits. Enfin, chacun de ces segments est associé à un mot dans la liste standarde de 2048 mots, ce qui permet de former la phrase. Cette dérivation est représentée dans la figure 7.4.

Le nombre de mots de la phrase dépend de la taille de l'entropie désirée. Ainsi une entropie de 128 bits est dotée d'une somme de contrôle de 4 bits, ce qui donne une phrase de 12 mots de 11 bits. Pour 256 bits, on a une somme de contrôle de 8 bits et donc une phrase de 24 mots.

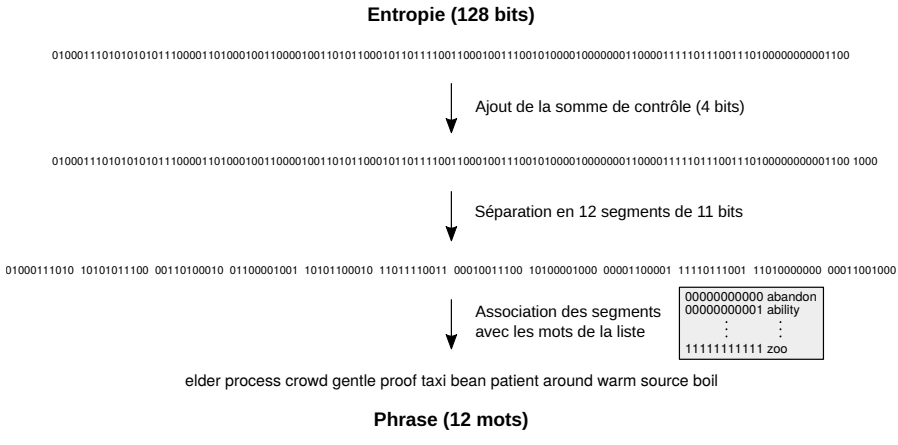

FIGURE 7.4 – De l'entropie à la phrase secrète.

Divers procédés cryptographiques sont utilisés pour dériver les clés et les adresses à partir de cette phrase. Ces procédés de dérivation ont sensiblement les mêmes propriétés que les fonctions de hachage en produisant des résultats irréversibles, imprédictibles et résistants aux collisions.

Le premier est le code d'authentification de message HMAC-SHA512 (HMAC pour *Hash-Based Message Authentication Code*) qui calcule une empreinte en utilisant la fonction de hachage SHA-512 en combinaison avec une clé secrète. Le second est la fonction de dérivation de clé PBKDF2 (*Password-Based Key Derivation Function 2*) qui applique de manière répétée une fonction choisie par l'utilisateur à un message de taille arbitraire avec un sel cryptographique. L'intérêt est de nécessiter une quantité de calcul importante pour éviter un cassage par force brute de l'information supérieure.

Dans Bitcoin, PBKDF2 est utilisée pour dériver une graine à partir de la phrase mnémotechnique, en appliquant la fonction HMAC-SHA512 à 2048 reprises. Le sel cryptographique est le terme `mnemonic` auquel on peut ajouter

une phrase de passe (*passphrase*) pour renforcer la sécurité du procédé. La graine résultante est une information de 512 bits (64 octets), à partir de laquelle la clé maîtresse et les clés suivantes sont dérivées.

La dérivation des clés se fait grâce à la fonction HMAC-SHA512. Tout d'abord, on procède à une première dérivation à partir de la graine. On applique le HMAC à la graine et au sel cryptographique `Bitcoin seed`, ce qui nous donne une clé maîtresse (premiers 256 bits du résultat) et un code de chaîne maître (derniers 256 bits du résultat). Le passage de la phrase secrète à la clé maîtresse et au code de chaîne maître est résumé dans la figure 7.5.

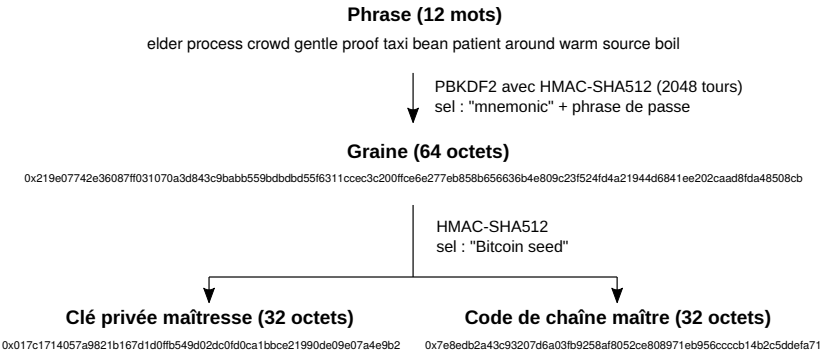

FIGURE 7.5 – De la phrase secrète à la clé maîtresse.

Ces deux informations permettent de réaliser toutes les dérivations suivantes. Le code de chaîne intervient dans la chaîne de dérivation des clés, de sorte qu'il est impossible de procéder à la dérivation sans lui.

Plutôt que de gérer ces deux informations indépendamment, on préfère faire appel aux clés privées étendues (*extended private keys*), qui incluent la clé privée et le code de chaîne, ainsi que d'autres informations comme la profondeur et l'indice de la clé enfant. La clé privée étendue est encodée en Base58Check avec un préfixe spécial qui dépend du type d'adresse dérivé, faisant que le résultat commence par `xprv` (adresses traditionnelles et clés Taproot), par `yprv` (adresses SegWit imbriquées) ou par `zprv` (adresses SegWit natives). Dans notre cas, la clé privée étendue issue de la clé privée maîtresse et du code de chaîne maître est :

```
xprv9s21ZrQH143K3KSN1mSK8myNuDcXNvNoCDcU4KBxMTuj1Wo83zNn
jaj8dKFT81GttcgPftdB4XhAzzQLXJEGDtFp35yssYnxDV3yVDEqv1b
```

De même, la clé publique étendue (*extended private key*) regroupe la clé publique et le code de chaîne correspondant à la clé privée dont elle dérive. En Base58Check, cette clé commence toujours par xpub, ypub ou zpub. La clé publique étendue correspondant à la clé privée maîtresse est :

```
xpub661MyMwAqRbcFoWq7nyKVuv7TFT1nP6eZSY4rhbZuoShtK8GbXh3
HP3cUapsPsqEd52TRk1vhkgkhtAReezgSBi4ELh3YoxjmZgKBk7U98h
```

La dérivation des clés (*child key derivation*) consiste à utiliser l'algorithme HMAC-SHA512 pour dériver des clés étendues « enfant » à partir d'une clé étendue « parent ». Les codes de chaîne sont utilisés comme sel cryptographique. Deux types de dérivation existent : la dérivation normale et la dérivation endurcie.

La dérivation normale fait intervenir la clé publique étendue dans le processus, ce qui rend possibles deux opérations : l'obtention de la clé publique (étendue) enfant à partir de la clé publique (étendue) parent, et l'obtention de la clé privée (étendue) enfant à partir de la clé privée (étendue) parent. Le fonctionnement de ce type de dérivation est schématisé par la figure 7.6.

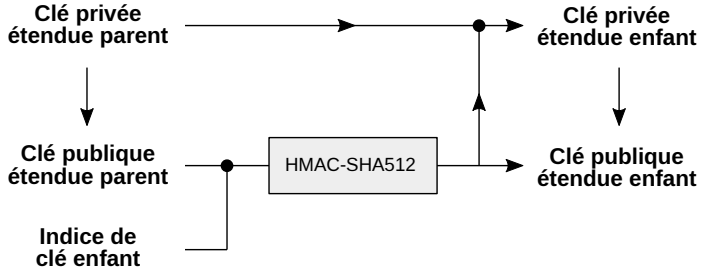

FIGURE 7.6 – Dérivation normale des clés par HMAC-SHA512.

Cette particularité de la dérivation se révèle extrêmement utile pour générer de nouvelles adresses sans compromettre la clé privée racine. Un utilisateur peut ainsi importer la clé publique étendue dans un processeur de paiement afin de vérifier son solde et générer de nouvelles adresses sans avoir à fournir la clé privée. Cela permet aussi aux commerçants d'avoir des employés qui reçoivent des paiements à différentes adresses sans se soucier de la sécurité des fonds.

Cependant, cette particularité comporte un risque potentiel : si une clé privée enfant est divulguée, alors la connaissance de la clé publique étendue parent (et donc du code de chaîne correspondant) permet d'obtenir toutes les clés privées enfant ainsi que la clé privée parent.

C'est pour cela qu'il existe un deuxième type de dérivation, la dérivation endurcie (*hardened derivation*), qui, contrairement à la première, est restreinte au calcul de clés privées (étendues) enfant, ce qui assure une meilleure sécurité. Celle-ci est représentée dans la figure 7.7.

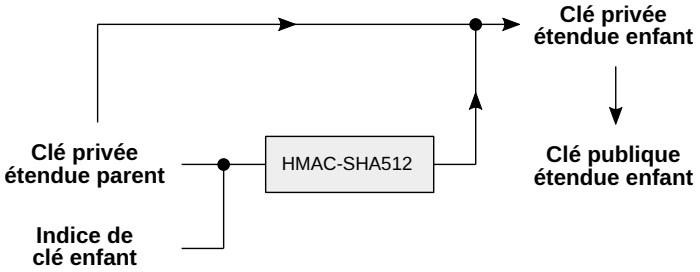

FIGURE 7.7 – Dérivation endurcie des clés par HMAC-SHA512.

Chaque dérivation fait intervenir un indice, encodé sur 32 bits comme un entier signé, dont le bit de signe indique si elle doit être endurcie ou non et dont la valeur indique le numéro de la clé enfant. Ainsi, on peut produire 2 147 483 648 (de 0 à $2^{31} - 1$) clés enfants normales et 2 147 483 648 clés enfants endurcies (de -0 à $-2^{31} + 1$) à partir d'une même clé parent.

L'usage veut qu'on utilise une apostrophe pour désigner ce signe [16]. L'indice `2` indique qu'il s'agit de la troisième clé enfant normale. L'indice `44'` indique qu'il s'agit de la 45e clé enfant endurcie.

Les dérivations successives permettent de créer des arbres de dérivation, dont la position de chaque clé peut être retrouvée grâce à un chemin, le chemin de dérivation. Ce dernier est composé des indices successifs des clés, qui sont séparés par des barres obliques (`/`). On le fait généralement commencer par la lettre `m` pour indiquer qu'on part de la clé privée maîtresse. Un exemple de chemin de dérivation est `m/84'/0'/0'/1/17`.

Chaque portefeuille peut utiliser son propre chemin de dérivation. Néanmoins, un standard a émergé, le BIP-44. Celui-ci simplifie la construction de portefeuilles à usages multiples, supportant plusieurs cryptomonnaies et donnant la possibilité de créer plusieurs comptes pour chacune d'entre elles [17].

Dans ce standard, on procède à trois dérivations endurcies puis à deux dérivations normales pour arriver à une clé privée et à l'adresse correspondante. Chaque dérivation apporte une information :

— La première dérivation (endurcie) sert à définir le but du portefeuille : le 44 (qui fait référence au BIP-44) permet de dériver un compte utilisant des adresses traditionnelles, le 49 (BIP-49) pour les adresses

SegWit imbriquées, le 84 (BIP-84) pour les adresses SegWit natives, le 48 ou le 45 (BIP-45) pour les adresses multisignatures, le 86 (BIP-86) pour dériver les clés publiques liées à Taproot, etc. ;

— La deuxième dérivation (endurcie) indique le protocole cryptoéconomique et *a fortiori* l'unité de compte liée : le chiffre 0 est utilisé pour BTC, le 1 pour le testnet, le 2 pour LTC, le 60 pour ETH, le 128 pour XMR, le 145 pour BCH, etc.

— La troisième dérivation (endurcie) donne l'indice du compte : 0, 1, 2, etc. ;

— La quatrième dérivation (normale) indique le rôle des adresses : le 0 signale qu'il s'agit d'une adresse externe, dont le rôle est de réceptionner des bitcoins, le 1 d'une adresse interne, utilisée pour accueillir la sortie complémentaire lors d'un envoi de bitcoins (phénomène que nous décrirons dans le chapitre 12) ;

— La cinquième dérivation (normale) donne l'indice de la clé et de l'adresse considérée : 0, 1, 2, etc.

De ce fait, le chemin de dérivation ressemble à ceci :

```
m / but' / protocole' / compte' / rôle_adresse / indice_adresse
```

Par exemple, la clé `m/44'/0'/0'/0/0` correspond à la première adresse de réception d'un compte Bitcoin utilisant les adresses traditionnelles. De même, la clé `m/84'/0'/0'/1/17` correspond à la 18e adresse de reste du premier compte Bitcoin utilisant les adresses SegWit natives.

Toutes les adresses d'un portefeuille restent valides même si elles ont été utilisées. Même si l'on peut générer des adresses à l'infini, le portefeuille balaie usuellement 20 adresses à partir de la dernière adresse active.

La propriété dans Bitcoin

La propriété est le contrôle absolu exercé sur un bien par une personne à l'exclusion de toutes les autres. Bien souvent, la propriété s'exerce par l'intermédiaire d'un droit de propriété qui établit *de jure* le rapport de force. Le bien possédé peut être un livre, une voiture ou un terrain.

La propriété est à la base de la monnaie : sans maîtrise réelle sur les unités monétaires, l'échange est impossible. En effet, la cession de pièces de métal précieux ou de billets fiduciaires requiert que le porteur les contrôle entièrement et puisse les abandonner au moment de la transaction. C'est pourquoi on parle aussi d'argent *liquide*.

Sans cette propriété, les caractéristiques de la monnaie s'effritent. Aujourd'hui, l'essentiel des transactions a lieu par l'échange du crédit bancaire, que ce soit par le biais d'un paiement par carte bancaire, d'un virement ou d'un autre moyen numérique. Cette situation fait que les gens s'exposent de plus en plus aux formes de censure issues des contraintes réglementaires et de l'arbitraire bancaire, comme l'interdiction d'envoyer un virement ou le gel de compte sans préavis, outre le risque de solvabilité de la banque.

Bitcoin permet de redevenir pleinement propriétaire de son argent tout en conservant le côté numérique et immatériel de son usage. Cette propriété est de nature différente de celle exercée sur les objets : elle est en effet indissociable de la connaissance exclusive d'une information (les clés privées) et de la protection de cette information.

Ainsi, l'information possède, plus que jamais, de la valeur. On a toujours associé une valeur au savoir en raison du pouvoir que ce dernier apporte (*scientia potentia est*), mais cette valeur était indirecte. Aujourd'hui, une information peut procurer un accès direct à un certain montant de cryptomonnaie : si quelqu'un connaît la clé privée qui correspond à une adresse contenant des bitcoins, il possède *de facto* ces bitcoins.

Un utilisateur peut conserver du bitcoin extrêmement facilement en gardant en mémoire la clé privée ou la phrase de récupération. Il peut par exemple franchir une frontière étatique en ayant en sa possession un papier sur lequel se trouve l'information en question, ou bien tout simplement en la gardant en tête. C'est par exemple le cas d'un criminel allemand qui, après avoir miné frauduleusement 1 700 bitcoins en installant un logiciel sur des ordinateurs à l'insu de leurs propriétaires, a pu conserver sa fortune malgré son emprisonnement de deux ans [18].

Un utilisateur peut recevoir des bitcoins en générant une nouvelle clé privée sur un appareil. Il ne nécessite aucune autorisation du réseau, même s'il doit bien entendu avoir accès à Internet pour vérifier les paiements entrants. En raison de la résistance du système à la censure, il peut faire ce qu'il veut de ses bitcoins : financer des causes sensibles, acheter de la drogue sur le dark web, jouer au casino en ligne, envoyer des fonds à l'étranger, etc. Il n'y a pas de limite de montant, ce qui confère à un individu fortuné un moyen d'avoir un impact autrement plus grand sur le monde.

Le risque de garde

Même si Bitcoin permet l'échange libre au travers du cyberespace, il n'a pas fait disparaître les tiers de confiance pour autant. En effet, beaucoup

de gens sont peu confiants dans leur capacité à conserver eux-mêmes leurs bitcoins, et préfèrent déléguer cette responsabilité à des services dépositaires, comme les services de garde spécialisés, les places de marché en ligne ou les applications de paiement. Il est aussi plus pratique de passer par une banque pour prêter son argent et le faire fructifier, ce qui profite aux plateformes de prêt en ligne.

Bien que ce comportement se comprenne, il faut insister sur le fait que ceux qui épargnent des bitcoins par l'intermédiaire d'un dépositaire ne possèdent pas réellement ces bitcoins. La créance qu'ils possèdent sur le tiers de confiance n'est pas la propriété des bitcoins, puisque c'est le tiers en question qui les garde en son pouvoir. La loi étatique peut intervenir, mais cela n'empêche pas ce contrôle réel de s'exprimer dans une multitude de cas. C'est le sens de l'adage « pas vos clés, pas vos bitcoins » (« *not your keys, not your coins* »), popularisé par Andreas Antonopoulos [19], qui rappelle que celui qui ne gère pas lui-même ses clés privées, ne possède pas réellement les bitcoins qu'il estime détenir.

Si la délégation de la propriété apporte certains avantages, elle a aussi ses inconvénients et fait courir des risques à ceux qui y ont recours. Tout d'abord, les dépositaires peuvent faire faillite dans le cas où leurs réserves deviennent trop basses pour les demandes de retrait. En cas de faillite, le client ne retrouve pas l'intégralité de ses fonds, à moins qu'une autre entité rachète les pertes de la plateforme.

Premièrement, cette faillite peut se matérialiser suite à une perte de fonds, comme ce qui est arrivé en juillet 2011 à la plateforme de change polonaise Bitomat qui avait perdu les clés privées liées à 17 000 BTC suite à un incident technique.

Deuxièmement, elle peut provenir d'un vol externe à la plateforme, issu par exemple d'un piratage, dont l'exemple le plus connu est le cas de la plateforme Mt. Gox qui a connu de multiples piratages entre 2011 et 2013 ayant mené à la volatilisation de 650 000 bitcoins, et qui a fait faillite en 2014. La dette (en dollars) des créanciers de la plateforme devrait être remboursée en 2024, dix ans après les faits.

Troisièmement, cette faillite peut résulter d'une escroquerie de sortie ou d'un vol interne, où le gestionnaire de la plateforme « s'enfuit avec la caisse ». Ce type d'incident a été illustré en juillet 2011 par la fermeture du service MyBitcoin après le vol supposé de 78 740 BTC par son fondateur anonyme Tom Williams. Un autre cas est celui de la plateforme canadienne QuadrigaCX, qui a fait faillite en 2019 suite à la mort de son fondateur et PDG, Gerald

Cotten, qui s'avérait avoir dépensé les fonds pour financer son train de vie et son addiction à la spéculation. La faillite de la plateforme d'échange populaire FTX qui est survenue en novembre 2022 suite à l'utilisation frauduleuse des fonds de ses clients constitue un autre exemple explosif de ce type d'évènement.

Quatrièmement, même si aucune perte ou aucun vol de fonds ne survient, un fonctionnement par réserves fractionnaires du dépositaire peut le pousser à faire faillite à cause d'un resserrement du crédit. C'est notamment arrivé aux plateformes de prêt Celsius, Three Arrows Capital, Voyager Digital, BlockFi et Genesis Files en 2022–2023.

Ensuite, outre le risque de faillite, l'utilisation d'un dépositaire comporte le risque d'intervention étatique. La plateforme, pourvu qu'elle agisse sur le marché légal, se soumet aux diverses réglementations de LCB-FT et peut donc être amenée à geler un compte, voire à saisir les fonds qui s'y trouvent. C'est ce qu'a fait la place de marché Coinbase le 7 mars 2022 en bloquant 25 000 adresses dans le contexte des sanctions occidentales contre la Russie [20]. La plateforme peut également être fermée par les pouvoirs publics, comme cela a été le cas de BTC-e en juillet 2017 qui a été saisie par le département de la Justice des États-Unis [21].

Enfin, un autre inconvénient lié à l'utilisation d'un dépositaire est le cas des scissions, qui sont des duplications permanentes de la chaîne de blocs créant deux monnaies distinctes, et des *airdrops* (« largages »), qui sont des distributions gratuites de jetons à des fins publicitaires. Dans les deux cas, l'adresse de l'utilisateur est créditée d'un actif supplémentaire qui devient sa propriété. Cependant, si la personne passe par l'intermédiaire d'un dépositaire, ce dernier peut choisir de ne pas le lui céder, généralement d'une manière non frauduleuse, selon les critères déterminés par les conditions d'utilisation lors de l'inscription. En ce qui concerne les scissions, on peut citer l'exemple de la plateforme Bitstamp qui a refusé de céder les bitcoins SV de ses utilisateurs après la séparation entre BCH et BSV en novembre 2018 et qui continue de les conserver [22]. Pour les airdrops, on peut évoquer le cas de HEX, pyramide de Ponzi ouverte, dont la genèse en 2020 a été déterminée en partie par la possession de bitcoins : chaque détenteur de bitcoin pouvait prétendre à un montant de jetons HEX proportionnel en publiant une signature numérique sur la chaîne d'Ethereum, mais il semble qu'aucune plateforme n'a pris le risque de tirer profit de ce largage.

La non-distribution des fruits des scissions et des *airdrops* représente ainsi un manque à gagner, voire une perte sèche pour le client, surtout s'il s'agit d'une scission entre deux économies de taille équivalente. Toutefois, rien ne

peut forcer en soi un dépositaire à proposer le retrait de ces gains, car la mise en œuvre technique a un coût non négligeable. Dans le cas contraire, les plateformes seraient contraintes de soutenir toutes les créations de ce type, y compris les plus fantaisistes, comme les scissions opportunistes de BTC qui ont eu lieu en 2017–2018 (Bitcoin Gold, Bitcoin Diamond, Bitcoin Private, etc.)

D'une manière générale, le recours aux dépositaires comporte des inconvénients majeurs qui font que l'utilisateur ne bénéficie pas de la résistance à la censure et de la résistance à l'inflation de Bitcoin. Conserver du bitcoin sur des plateformes réglementées lui permet seulement de profiter de l'indulgence temporaire de l'État vis-à-vis des transferts effectués et des plus-values réalisées. En outre, la généralisation de la garde de fonds présente un risque systémique comme nous le verrons. C'est pourquoi le recours aux dépositaires doit être considéré comme l'exception, et non la règle, en ce qui concerne la conservation des bitcoins.

Propriété et responsabilité

Si Bitcoin permet à l'utilisateur de posséder son argent de manière souveraine, cette propriété s'accompagne d'une responsabilité. Cet utilisateur doit comprendre comment le système fonctionne, au moins de manière rudimentaire. Il doit choisir quels logiciels et quel matériel utiliser. Il doit manipuler les fonds, vérifier les adresses, rester vigilant à tout instant. Dans le cas d'une scission sans protection contre la rediffusion des transactions, il doit procéder lui-même à la séparation des pièces d'un côté et de l'autre. Il est seul face à l'incertitude, et surtout, face à lui-même. Cette responsabilité constitue le prix à payer pour la liberté monétaire.

Il est donc compréhensible que certaines personnes manquant de connaissances techniques finissent par déléguer cette gestion, notamment dans le but de spéculer. Cependant, l'intérêt primordial de Bitcoin n'est pas de revenir à un système bancaire : c'est de posséder pleinement ses fonds, sans que ceux-ci puissent être gelés par un tiers de confiance ou dilués par l'inflation monétaire.

Puisque la sécurisation des bitcoins repose sur la connaissance d'une information, la conservation des bitcoins est inextricablement liée au dilemme qui existe entre la perte de données et la fuite de données. Pour conserver ses bitcoins, il faut à la fois garder l'accès à ses clés privées (éviter la perte de données) et en exclure les autres personnes (éviter la fuite de données), ce qui ne peut jamais être réalisé totalement.

Ce dilemme ne peut être résolu que par un compromis entre la sécurité

contre la perte et la sécurité contre le vol, qui est propre à chaque personne. Ainsi, quelqu'un peut simplement mémoriser sa phrase de 12 ou 24 mots pour conserver ses bitcoins, au risque de l'oublier et de les perdre définitivement. À l'inverse, une autre personne peut conserver des sauvegardes multiples à différents endroits au risque de voir un tiers accéder à l'une d'entre elles et s'emparer de ses fonds.

D'un côté, nous avons le vol de bitcoins. Celui-ci peut se faire par un cambriolage : une personne s'introduit chez autrui et s'empare du support physique sur lequel se trouve la sauvegarde ou le mot de passe. Mais il peut également être réalisé par intimidation : les propriétaires sont attaqués physiquement pour être extorqués. La famille de Hal Finney a ainsi été ciblée par un maître-chanteur, qui lui a fait subir un swatting en réussissant à convaincre les unités spéciales de police d'intervenir en urgence au domicile familial.

Il existe des bonnes pratiques pour ne pas s'exposer à ce type de vol. Tout d'abord, il est primordial de préserver sa confidentialité en évitant de déclarer qu'on possède des cryptomonnaies, combien on en possède, depuis combien de temps, etc. Ce conseil s'applique également vis-à-vis des plateformes de change, qui connaissent l'identité de leurs clients et leurs adresses de retrait, et qui peuvent dévoiler ces informations suite à une requête étatique ou à une fuite.

Puis, l'utilisateur peut améliorer sa conservation. Il peut éviter de conserver ses sauvegardes dans les lieux les plus sensibles (comme son domicile). Il peut également répartir les fonds dans des portefeuilles gérés différemment afin d'atténuer l'impact d'un vol, bien que cela augmente également le risque de survenue de ce vol.

Il est ensuite possible de mettre en place un compte secondaire caché au sein d'un portefeuille matériel en exploitant l'utilisation de la phrase de passe. C'est une fonctionnalité que Ledger intègre dans ses produits. Cette technique a le mérite de créer un « déni plausible » à présenter à l'assaillant qui menace ou qui torture le détenteur.

On peut enfin rendre la propriété des bitcoins collective, soit de manière explicite par la mise en place d'un compte multisignatures où chaque participant dispose de ses propres clés privées, soit de manière implicite par l'algorithme de partage de clés secrètes de Shamir (*Shamir's Secret Sharing*). Cela permet d'impliquer d'autres personnes pour rendre l'extorsion plus difficile.

De l'autre côté, nous avons la perte de bitcoins, qui représente le risque opposé de la conservation. La perte n'est pas en soi un problème pour le système. En effet, elle ne fait que renforcer le côté déflationniste du bitcoin :

comme le disait Satoshi Nakamoto, la perte ne fait qu'« augmenter légèrement la valeur des pièces des autres » et peut être considérée « comme un don à tous [23] ». Toutefois, il s'agit assurément d'un problème au niveau individuel, et la perte des clés a été pendant longtemps le principal risque pour l'utilisateur.

Certains des premiers mineurs ont ainsi perdu les bitcoins qu'ils avaient extrait. C'est le cas de James Howells, un ingénieur britannique qui a miné 8 000 bitcoins pendant un peu plus de 2 mois en 2009 et qui a perdu la clé permettant d'y accéder [24]. Au cours de l'été 2013, il a en effet jeté son ordinateur contenant le fichier du portefeuille, en le déposant à la décharge publique près de chez lui. Il a réalisé son erreur quelques mois plus tard avec la hausse du cours et la médiatisation associée, mais il était trop tard. Son cas a été rendu public en novembre 2013 dans un article du *Guardian* [25].

Un autre exemple (médiatisé en 2021 [26]) est celui de Stefan Thomas, le programmeur allemand qui a été payé en bitcoins pour produire la première vidéo qualitative sur Bitcoin. Après avoir payé les frais pour cette vidéo, il a conservé le reste sur son portefeuille [27]. Il a procédé à une sauvegarde sur une clé USB chiffrée (IronKey) mais a fini par oublier son mot de passe de chiffrement.

Les pertes sont donc courantes et il est nécessaire de se prémunir contre ce risque. L'adoption des portefeuilles déterministes hiérarchiques (*HD wallets*), où les clés sont dérivées d'une seule phrase secrète, a grandement aidé à raffermir la sécurité contre la perte. Avant, on devait conserver un fichier contenant ses clés privées sur un appareil ; aujourd'hui la simple conservation de cette phrase suffit, ce qui facilite la copie sur un support physique.

La première mesure à prendre pour éviter la perte est la mise en place de sauvegardes multiples. L'utilisateur peut placer la phrase à différents endroits géographiques, si bien qu'il conserve la propriété de ses bitcoins en cas de sinistre de l'un de ces endroits (incendie, inondation, cyclone, etc.) Il peut utiliser une feuille en papier simple ou cartonnée, ou bien il peut également faire le choix de graver ses mots sur une plaque d'acier forgée à cet effet.

L'utilisateur peut même, pour ses portefeuilles les moins fournis, conserver une sauvegarde numérique sur son ordinateur (si possible en la chiffrant) ou sur le *cloud*, ce qui augmente sensiblement le risque de vol mais permet d'être sûr de pouvoir accéder aux bitcoins. Cet usage est généralement déconseillé, mais c'est à l'individu d'arbitrer la situation.

L'aspect programmable de Bitcoin peut également être mis à profit contre la perte. On peut ainsi mettre en place des systèmes de récupération de fonds, comme ce qui est fait par exemple dans le portefeuille Liana [28]. Aucun standard

de contrat de ce type ne s'est pour l'instant imposé, si bien que cette pratique reste déconseillée pour le novice.

Il peut être profitable pour l'utilisateur de tenir un ou plusieurs registres listant ses différents portefeuilles, même les plus anciens, afin de ne pas oublier où sont ses fonds. Cependant, encore une fois, il ne faut pas que ce registre soit trouvé, auquel cas les fonds pourraient être retrouvés plus facilement.

De même, on ne doit jamais supprimer la sauvegarde d'un portefeuille, même si ce dernier paraît vide. Celui-ci pourrait en effet contenir des cryptomonnaies issues de scissions ou pourrait recevoir des paiements à l'avenir (par exemple s'il inclut une adresse de donation publique). Il est en ce sens recommandé « de le mettre de côté et de conserver l'ancienne copie au cas où [29] ».

Enfin, l'utilisateur doit se souvenir qu'il va mourir. À moins qu'il ne veuille emporter ses possessions numériques dans sa tombe, il lui faut mettre en place un plan de succession pour ses bitcoins à destination de ses héritiers. Il existe de multiples manières de faire, mais le modèle le plus réputé est celui présenté par Pamela Morgan dans son *Cryptoasset Inheritance Planning* [30]. Celui-ci consiste à écrire une lettre dans laquelle l'utilisateur inclut les coordonnées de gens de confiance à contacter pour aider ses héritiers (nos proches ne sont *a priori* pas autant à l'aise que nous avec la manipulation de bitcoins) ainsi que l'inventaire de ses avoirs (dans le but de récupérer les sauvegardes et de restaurer les portefeuilles). La lettre est scellée et placée dans un lieu sûr, comme un coffre-fort personnel, un coffre en banque ou chez un notaire.

Bitcoin et l'information

Bitcoin permet donc pour la première fois dans l'histoire d'être propriétaire d'un bien numérique rival. Cette propriété s'exerce par la connaissance exclusive d'informations, les clé privées, qui sont générées et gérées par des outils appelés les portefeuilles. Grâce au procédé de signature numérique, ce sont en effet ces clés privées qui permettent de signer les transactions dépensant les bitcoins.

Couplée à la résistance à la censure, cette assurance de la propriété permet de réaliser des transactions librement sur Internet, sans craindre le gel de compte. Mais elle s'accompagne également d'une responsabilité qui impose à l'utilisateur de prendre un certain de nombres de mesures pour ne pas voir ses fonds disparaître.

Ainsi, le système de signatures numériques « fournit un contrôle fort de la propriété ». Cependant, il « reste incomplet sans moyen d'empêcher la

double dépense [31] ». C'est la résolution de ce problème qui constitue l'objet du prochain chapitre.

8

Le consensus par le minage

Bitcoin est un modèle décentralisé de monnaie numérique issu de l'informatique distribuée, une discipline développée au moment de l'émergence d'Internet. Il se fonde plus précisément sur un réseau pair à pair d'ordinateurs, dans lequel les participants possèdent tous les mêmes responsabilités. En tant que tel, il constitue un *système d'argent liquide électronique pair à pair*.

Tout l'enjeu de Bitcoin est ainsi de se mettre d'accord sur le contenu d'un registre déterminant qui possède quoi, c'est-à-dire d'arriver à un consensus sur la propriété des unités. En particulier, l'établissement d'un tel accord permet de résoudre le problème de la double dépense, qui se pose dans le monde numérique en raison de la facilité de reproduction des données.

Le consensus – accord unanime au sein d'un groupe de personnes – n'est pas une chose facile à atteindre entre les êtres humains. La conciliation sociale peut fonctionner concernant des règles générales, mais n'est pas adaptée quant aux détails particuliers. C'est pourquoi les organisations humaines sont bien souvent obligées de s'en remettre à une autorité centrale chargée de prendre les décisions.

Bitcoin a précisément pour contrainte d'éviter le recours à un tiers de confiance. Il utilise à cette fin un mécanisme de consensus distribué et ouvert, qui repose sur une activité appelée communément le minage, où la confirmation des transactions, c'est-à-dire leur inclusion dans le registre, est assurée

par un procédé nommé la preuve de travail. Dans ce chapitre, nous détaillerons le fonctionnement de cet algorithme de consensus novateur.

Le problème des généraux byzantins

L'enjeu du consensus est illustré par le problème des généraux byzantins, qui est un problème d'informatique distribuée formalisé en 1982 par Leslie Lamport, Robert Shostak et Marshall Pease [1]. Ce problème traite de la remise en cause de la fiabilité des transmissions et de l'intégrité des participants dans les systèmes distribués, et il s'applique dans les cas où les composants d'un système informatique ont besoin d'être en accord.

Le problème est énoncé sous la forme d'une métaphore faisant intervenir des généraux de l'armée de l'Empire byzantin, l'Empire romain d'Orient qui a subsisté jusqu'en 1453 suite à la chute de la partie occidentale en 476 [2]. Ces généraux assiègent une ville ennemie avec leurs troupes dans le but de l'attaquer. Ils ne peuvent communiquer qu'à l'aide de messages relayés oralement et ils doivent trouver un moyen d'établir un plan de bataille commun par ce moyen. Par exemple, les généraux peuvent chercher à coordonner une attaque à l'aube, et partagent leurs intentions entre eux en envoyant le message « attaque » par le biais d'un message pour confirmer l'assaut, et « retraite » pour l'annuler.

Cependant, un petit nombre de ces généraux s'avèrent être des traîtres au service de l'ennemi qui essaient de semer la confusion au sein de l'armée. Ces traîtres envoient ainsi des messages contradictoires à leurs interlocuteurs, pour faire en sorte que certains généraux loyaux attaquent, et que d'autres battent en retraite au moment de l'assaut, causant par là une défaite certaine, comme illustré sur la figure 8.1.

Le problème est de trouver une stratégie (c'est-à-dire un algorithme) permettant de s'assurer que tous les généraux loyaux se mettront d'accord sur le plan de bataille. Les traîtres battront alors en retraite, mais puisque leur nombre est supposément restreint, l'attaque sera quand même un succès.

La situation fait qu'il est difficile de parvenir à un consensus. On ne peut pas désigner un commandant auquel les généraux subordonnés obéiront, car le commandant peut être lui-même un traître. Lamport, Shostak et Pease ont montré que le problème peut être résolu de manière absolue si (et seulement si) les généraux loyaux représentent strictement plus des deux tiers de l'ensemble des généraux [3] ; autrement dit, qu'il ne peut pas y avoir plus d'un tiers de traîtres au sein de l'armée.

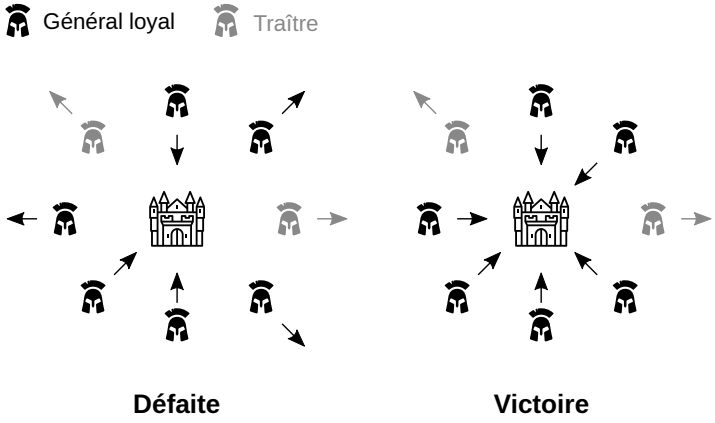

FIGURE 8.1 – Attaque des généraux byzantins contre la ville : succès et échec.

La métaphore des généraux byzantins s'applique directement aux systèmes distribués, c'est-à-dire aux systèmes dont les composants sont séparés et doivent communiquer les uns avec les autres pour se synchroniser. Les généraux représentent les composants du système, les traîtres les composants défaillants, et les messages les données transmises entre les composants. Le but est d'obtenir un algorithme permettant de détecter les défaillances, appelées pannes byzantines, et de permettre aux autres composants de les écarter. La résilience obtenue est appelée la tolérance aux pannes byzantines ; le système est dit BFT, pour *Byzantine Fault Tolerant*.

Le problème a été initialement décrit pour les systèmes informatiques reposant sur des composants présents à différents endroits et dans lesquels la bonne transmission des données est critique, comme les systèmes aéronautiques et spatiaux [4]. Mais il concerne aussi (ce qui nous intéresse ici) les systèmes pair à pair reposant sur un réseau horizontal de participants, et en particulier les systèmes cryptoéconomiques comme Bitcoin, dans lesquels les nœuds du réseau ont besoin de se mettre d'accord sur le contenu d'un registre. L'objectif est alors de trouver un algorithme permettant à tous les nœuds honnêtes de parvenir à un consensus en présence de nœuds traîtres (dits « byzantins »).

Avant Bitcoin, le problème était résolu par des algorithmes dits « classiques » basés sur les idées de Lamport, Shostak et Pease. Le plus connu est probablement l'algorithme de consensus PBFT (pour *Practical Byzantine Fault Tolerance*), mis au point par Miguel Castro et Barbara Liskov en 1999, qui permettait à un nombre donné de participants de se mettre d'accord en

gérant des milliers de requêtes par seconde avec une latence de moins d'une milliseconde.

Bien avant Bitcoin, Wei Dai et Nick Szabo envisageaient d'utiliser ce type d'algorithme pour leurs systèmes de monnaie électronique, b-money et bit gold. De même, de nombreux systèmes cryptoéconomiques en font encore aujourd'hui usage pour des raisons de performance, à l'instar d'Ethereum dont le consensus est basé sur l'algorithme Casper FFG.

Cependant, ces algorithmes impliquent des contraintes fortes : les nœuds doivent connaître l'ensemble des autres nœuds et ils doivent communiquer avec tous les autres. De ce fait, il faut sélectionner les nœuds ayant le droit de participer au consensus avant de lancer l'algorithme, ce qui se fait généralement par preuve d'autorité (*proof of authority*), via une liste blanche de nœuds, ou par preuve d'enjeu (*proof of stake*), via un montant d'unités possédées ou déléguées. Cela implique une moins bonne robustesse du système, car les validateurs sont alors connus de tous et donc davantage exposés aux attaques.

Bitcoin résout ce problème d'une manière différente, grâce à un nouveau type d'algorithme : l'algorithme de consensus de Nakamoto par preuve de travail. Celui-ci est plus robuste dans le sens où les nœuds du réseau n'ont pas besoin de connaître l'ensemble des autres nœuds et où aucune identification n'est requise.

Puisque le rôle principal de Bitcoin est le transfert de valeur, l'objectif est de se mettre d'accord sur qui possède quoi, c'est-à-dire sur l'*état* du système. La solution proposée par Satoshi Nakamoto consiste à employer un registre recensant l'intégralité des transactions réalisées depuis le lancement du système, « la seule façon de confirmer l'absence d'une transaction [étant] d'être au courant de toutes les transactions [5] ». Ce registre formant l'*historique* du système est organisé comme une succession de blocs de transactions, de sorte qu'il est communément appelé la *chaîne de blocs*. Les nœuds du réseau entretiennent chacun une copie complète de la chaîne dont ils transmettent des éléments sur demande.

Les nouveaux blocs sont ajoutés à la chaîne de manière régulière grâce à la production d'une preuve de travail. Les acteurs réalisant cette opération sont appelés des mineurs. Les nœuds du réseau arrivent à un consensus en considérant que la chaîne la plus longue est la chaîne correcte. Ainsi, comme l'a écrit Satoshi Nakamoto :

> « La chaîne de preuves de travail est une solution au problème des généraux byzantins [6]. »

La spécificité novatrice de cet algorithme est qu'il résout le problème de manière probabiliste plutôt que de manière absolue [7]. Par conséquent, les transactions incluses dans le registre ne sont jamais strictement finales, mais sont (probabilistiquement parlant) considérées comme telles au bout d'un temps. Ce fonctionnement permet de n'avoir besoin que de 51 % de validateurs honnêtes, au lieu des 67 % requis par les algorithmes classiques.

La preuve de travail

La preuve de travail, de l'anglais *proof of work*, est un procédé permettant à un appareil informatique de démontrer de manière objective et quantifiable qu'il a dépensé de l'énergie. Ce moyen est utilisé pour sélectionner les ordinateurs dans le cadre de l'accès à un service ou à un privilège.

La preuve de travail est un mécanisme de résistance aux attaques Sybil, qui rend difficile la multiplication des identités à l'excès par un acteur qui chercherait à prendre le contrôle du réseau. Une attaque Sybil est une attaque intervenant au sein d'un réseau ouvert basé sur un système de réputation qui consiste à dupliquer les profils à moindre coût pour en altérer le fonctionnement. C'est par exemple un problème particulièrement présent sur les médias sociaux, où les comptes de robots sont utilisés en masse pour augmenter la visibilité d'un contenu donné.

Le concept de preuve de travail a été décrit pour la première fois par Cynthia Dwork et Moni Naor en 1992, dans un article visant à présenter une méthode permettant de combattre le courrier indésirable (*spam*) dans les boîtes de réception [8]. Le terme « *proof of work* » est quant à lui apparu en 1999 sous la plume de Markus Jakobsson et Ari Juels [9].

L'idée de Dwork et Naor a été implémentée par le cypherpunk britannique Adam Back en 1997 au moyen de Hashcash, un algorithme produisant de manière simple des preuves de travail avec une fonction de hachage, qui devait principalement servir pour le courrier électronique [10]. Cette implémentation a été reprise dans le système de preuves de travail réutilisables (RPOW) de Hal Finney mis en application en 2004.

L'algorithme de preuve de travail de Hashcash consiste à trouver une collision partielle de la fonction de hachage considérée, c'est-à-dire à obtenir deux messages ayant une empreinte commençant par les mêmes bits de données. À partir de la version 1.0 sortie en 2002, il s'agit plus précisément de découvrir une collision partielle pour l'empreinte zéro, à savoir trouver un antécédent dont l'empreinte commence par un nombre de zéros binaires déterminés.

Puisque la fonction de hachage est à sens unique (résistance à la préimage), une telle obtention ne peut être réalisée qu'en testant une à une les différentes possibilités, ce qui demande de l'énergie. L'antécédent obtenu est appelé une preuve de travail.

La preuve de travail est réalisée par le calcul successif d'empreintes d'une chaîne de caractères, composée d'une information de base, et d'un nombre qu'on fait varier, appelé le compteur ou le nonce. L'information de base comporte généralement des indications sur le contexte dans lequel la preuve de travail a été produite (identifiant, date, heure, protocole, etc.) pour démontrer que cette preuve de travail n'a pas déjà été utilisée.

Prenons un exemple pour illustrer le propos. D'abord, on choisit une information de base propre au contexte : pour produire une preuve de travail liée à cet ouvrage et à sa date d'écriture, on peut opter pour l'information de base `20231031181000:BitcoinElegance:`. Puis on détermine le degré de la preuve de travail, c'est-à-dire le nombre de zéros binaires par lequel doit commencer l'empreinte, ici 16. On procède ensuite à la recherche du résultat voulu en incrémentant le nonce : à chaque itération, on le met bout à bout avec l'information de base et on vérifie si l'empreinte de l'ensemble est satisfaisante. Le travail s'arrête enfin lorsque l'empreinte commence avec un nombre suffisant de zéros : ici 95 690 tentatives. Notre preuve de travail est donc :

```
20231031181000:BitcoinElegance:95690
```

Et l'empreinte correspondante, commençant par 4 zéros hexadécimaux (soit 16 zéros binaires), est :

```
0000387b99b1412e3cb6e49548cc0d11bdc797138e1a0f5ff095279a710b895a
```

Les étapes de cette procédure sont décrites dans le tableau 8.1.

Statistiquement, ce type de recherche implique d'essayer 65 536 possibilités (2^{16}) pour tomber sur une solution. En moyenne, la production d'une telle preuve de travail démontre donc qu'un effort approchant a été effectué. De plus, il existe une asymétrie entre la production et la vérification, cette dernière ne nécessitant qu'une seule application de la fonction de hachage et étant par conséquent peu coûteuse.

Le coût de production moyen confère une certaine rareté aux preuves de travail : plus leur degré est élevé, plus elles sont difficiles à produire. D'où le fait qu'on puisse les utiliser en tant que marques de qualité pour le courrier électronique comme dans Hashcash, ou bien en tant que pièces monétaires de base comme dans bit gold et RPOW.

Nonce	Empreinte (SHA-256)
0	`933c448c18e334c1cc5191f035d8581af611417578392b2d695d521c29b396d5`
1	`50530c98d1b171826b3d26fa5442e4ce7aa1f8a1277b71bc74d3adc1cd88b9ae`
2	`fa27ed560df22d676d69966c9a981c5adfc395b4e7f78ca54d2593a98fd2ea38`
3	`011692df53a84ecdddcd154de4f329e7311090580adb189e8360ea1729d75c99`
95 690	`0000387b99b1412e3cb6e49548cc0d11bdc797138e1a0f5ff095279a710b895a`

Tableau 8.1 – Recherche de la preuve de travail à partir de l'information de base `20231031181000:BitcoinElegance:`.

Le minage de Bitcoin intègre le procédé de preuve de travail de Hashcash sous la forme d'une variante : l'objectif est de trouver une empreinte inférieure à une valeur cible précise, et non pas une empreinte commençant par un nombre de zéros déterminés. Ce procédé est appliqué entre les blocs de transactions, de sorte que ces blocs, ou plutôt leurs entêtes comme nous l'expliquerons plus bas, constituent eux-mêmes les preuves de travail.

Dans Bitcoin, le rôle de la preuve de travail est double : exiger un coût pour la fabrication des nouveaux bitcoins et faire en sorte que le réseau puisse arriver à un consensus. D'une part, elle a pour but d'imposer la cherté de l'unité de compte. Cela rappelle les modèles qui ont précédé Bitcoin, et c'est pourquoi Hal Finney a été jusqu'à qualifier les bitcoins de « jetons de preuve de travail [11] » (*POW tokens*) en 2009. Toutefois, les bitcoins ne sont pas exactement des preuves de travail dans le sens où la difficulté de production est variable, évoluant selon la puissance de calcul totale déployée sur le réseau. Ainsi, mis à part dans le cas limite de la difficulté minimale du système, le but est de s'assurer que la production des unités demande de l'énergie, pas d'exiger un coût en travail fixe. D'autre part, la preuve de travail a pour objectif de garantir le consensus sur le réseau, en faisant en sorte que les nœuds honnêtes se mettent d'accord sur qui possède quoi. Elle limite l'accès à la production des blocs : la sélection du validateur (mineur) se fait selon le montant d'énergie dépensé. La preuve de travail joue ici son rôle de défense contre les attaques Sybil en empêchant les attaquants de mettre en place un grand nombre de nœuds pour contrôler le système [12].

Ce fonctionnement fait que la chaîne de blocs forme une chaîne de preuves de travail, qui récapitule l'ensemble du travail effectué depuis le début. De ce fait, la chaîne constitue un historique linéaire difficilement malléable comme nous le verrons.

La chaîne de blocs

La chaîne de blocs, ou *blockchain* en anglais, est la structure de données regroupant l'ensemble des transactions réalisées depuis le lancement du système. Cette structure est une suite de blocs de transactions, liés les uns aux autres par un procédé appelé l'horodatage.

L'horodatage est une technique permettant d'associer une date et une heure à une information, qui a été décrite en 1991 par Stuart Haber et Scott Stornetta dans le cas particulier de l'horodatage de documents. Le principe est simple : il consiste à hacher une information (ou un document) et de partager l'empreinte obtenue pour prouver que l'information (ou le document) existait à la date de partage. Cette méthode est notamment mise en œuvre par l'intermédiaire de serveurs d'horodatage centralisés qui se chargent d'enregistrer les empreintes, auquel cas on parle d'horodatage certifié ou de *trusted timestamping*.

Le principe derrière la chaîne de blocs est de lier les blocs les uns aux autres par ce procédé d'horodatage en inscrivant l'empreinte du bloc horodaté dans le bloc suivant. Cela crée des références récursives : le dernier bloc contient l'empreinte de l'avant-dernier bloc, l'avant-dernier de l'antépénultième, etc. pour remonter jusqu'au bloc de genèse (*genesis block*), c'est-à-dire le premier bloc de la chaîne, considéré comme valide par défaut. Pour la version principale de Bitcoin, ce bloc contient le titre de la une du *Times* du 3 janvier 2009, ce qui prouve que la chaîne n'a pas été lancée avant et empêche par conséquent l'antidatage.

La particularité de cette structure est qu'elle fait reposer la sécurité des maillons précédents sur les nouveaux maillons. Comme l'écrivait Satoshi Nakamoto dans le livre blanc :

> « Chaque horodatage inclut l'horodatage précédent dans son empreinte, formant ainsi une chaîne, au sein de laquelle chaque horodatage supplémentaire renforce le précédent [13]. »

En 2008, l'idée n'était pas nouvelle car elle avait déjà été appliquée en 1995 par les mêmes Haber et Stornetta, qui avaient publié chaque semaine une empreinte cryptographique dans les petites annonces du *New York Times* afin d'authentifier les documents des clients de leur société. C'était alors la manière la plus sûre de garantir l'intégrité des empreintes, le journal étant distribué quotidiennement à plus d'un million de personnes.

Satoshi Nakamoto a reproduit cette idée de diffusion publique des données en faisant de son système un « serveur d'horodatage distribué [14] » reposant sur un réseau pair à pair librement accessible sur Internet. Dans Bitcoin, chaque

bloc comporte en effet une date et une heure inscrites par le mineur, si bien que le résultat obtenu constitue une chaîne temporelle (*timechain* [15]) témoignant de l'avancée du temps dans le monde réel.

Cette chaîne a rapidement été qualifiée de chaîne de blocs par les premières personnes impliquées dans Bitcoin. Si le livre blanc parlait déjà d'une « *chain of blocks* », le terme « *block chain* » (en deux mots) a lui été créé par Hal Finney dans son premier courriel de réponse à Satoshi le 7 novembre 2008 [16]. L'appellation a ensuite été reprise par le fondateur dans le code source de la version 0.1 de Bitcoin et dans ses messages publics [17]. Le mot *blockchain* s'est progressivement popularisé au sein de la communauté pour parler de la chaîne de blocs de Bitcoin, puis, par métonymie, de son mécanisme de consensus. Il a enfin (non sans controverse) été élargi à la communication publique pour désigner (sous le nom de « technologie blockchain » ou de « blockchain » tout court) l'ensemble des techniques de consensus au sein de systèmes distribués, que celles-ci fassent intervenir une chaîne de blocs ou non.

La particularité de Bitcoin est d'avoir combiné l'horodatage d'informations et la preuve de travail produite par Hashcash. Puisque ces deux procédés se fondent tous les deux sur une fonction de hachage, il est en effet possible de les fusionner en un seul. La chaîne de blocs est donc à la fois une chaîne temporelle d'horodatages et une chaîne de preuves de travail.

L'agencement d'un bloc

Comme son nom l'indique, la chaîne de blocs est une structure constituée de blocs, qui sont des ensembles horodatés et travaillés de transactions. Celle-ci débute par un bloc de genèse, valide par défaut, à partir duquel sont comptés les blocs : cet indice est appelé la *hauteur* et indique la position du bloc dans la chaîne dans l'ordre de minage. Les blocs peuvent également être comptés dans l'autre sens à partir du tout dernier bloc miné, auquel cas on parle de *profondeur*.

Chaque bloc possède un identifiant unique qui le démarque des autres. Celui-ci est obtenu par hachage de l'entête du bloc (les données placées avant les transactions) par le double SHA-256. Chaque bloc contient l'identifiant du bloc précédent de sorte que l'ensemble forme une chaîne. Puisque seul l'entête est impliqué dans le calcul de l'identifiant, la chaîne de blocs peut en réalité être réduite à une chaîne d'entêtes, auxquels les transactions sont liées cryptographiquement. L'identifiant commence par un certain nombre de zéros témoignant du fait qu'un travail a été demandé. Ainsi, le bloc lui-même constitue la preuve de travail.

Les blocs sont tous organisés de la même façon, si bien qu'il suffit d'en examiner un seul en détail pour comprendre comment la chaîne se structure. Étudions donc un bloc de la version principale de Bitcoin (BTC) en prenant pour exemple le bloc de hauteur 751 005 miné le 25 août 2022, qui contient 6 transactions.

Chaque bloc se décompose en un entête de 80 octets, qui contient ses informations essentielles, et une succession brute de transactions. Par convention, la première transaction du bloc est la transaction de récompense (*coinbase transaction*) servant à rémunérer le mineur de ce bloc comme nous le verrons plus bas.

L'entête est, lui, divisé en six éléments : la version du bloc, l'identifiant du bloc précédent qui l'associe au bloc présent, une racine de Merkle qui engage cryptographiquement l'ensemble des transactions à l'entête, l'horodatage du bloc, la valeur cible du réseau et le nonce relatif au minage. Les différentes informations contenues dans l'entête sont transmises avec un ordre des octets inverse (dit « *little-endian* » ou « petit-boutiste ») par rapport à l'ordre ordinaire de lecture (qu'on appelle « *big-endian* » ou « gros-boutiste »). Nous les donnons ici dans l'ordre ordinaire.

La version du bloc

La version du bloc indique l'ensemble des règles respectées par le bloc. Historiquement, la version 1 marquait un respect des règles du protocole originellement défini par Satoshi. Les versions 2 à 4 ont servi à imposer l'application de certains changements du protocole entre 2013 et 2015. Depuis 2016, ce champ de version est utilisé pour le signalement des mineurs dans le cadre de l'application d'un soft fork par l'exécution du BIP-9 ou par un mécanisme équivalent. Le champ de version de notre bloc est :

```
0b00100000000000000000000000000100
```

L'identifiant du bloc précédent

L'identifiant du bloc précédent sert à lier l'entête du bloc présent à l'entête du bloc précédent. Dans le cas du bloc de genèse, ce champ est fixé à zéro par convention. Dans notre bloc, il constitue l'identifiant du bloc 751 004, qui est :

```
00000000000000000073ad6c18c81f2f67b2ca5b5ace8d23cce95812af8c7b6
```

La racine de Merkle

Le troisième élément de l'entête est la racine de Merkle, qui correspond à l'empreinte finale de l'agencement des transactions en arbre de Merkle.

Un arbre de Merkle, aussi appelé arbre de hachage, est une structure de données conceptualisée en 1979 par le cryptographe Ralph Merkle permettant de vérifier le contenu d'un volume de données sans avoir besoin de toutes les inspecter. Dans une telle structure, les données (constituant alors les feuilles de l'arbre) sont rangées dans un certain ordre et hachées respectivement. Puis leurs empreintes sont combinées deux à deux pour être hachées à leur tour, et ceci jusqu'à ce qu'il ne reste plus qu'une seule empreinte, qu'on appelle la racine. Les chaînes de hachages qui relient les feuilles à la racine sont appelées les branches.

Dans les blocs de Bitcoin, ce sont les transactions qui sont les données hachées. Elles sont d'abord hachées une première fois (ce qui correspond à leur identifiant) :

$$H_A = \mathrm{SHA256d}(\ \mathrm{tx}_A\ )$$

Puis les empreintes résultantes sont concaténées deux à deux (la deuxième empreinte est placée à la suite de la première) et l'ensemble est passé par la même fonction de hachage :

$$H_{AB} = \mathrm{SHA256d}(\ H_A \parallel H_B\ )$$

Le procédé est ensuite réitéré. Dans le cas où le nombre d'empreintes à combiner est impair, la dernière est concaténée avec elle-même :

$$H_{EFEF} = \mathrm{SHA256d}(\ H_{EF} \parallel H_{EF}\ )$$

Une fois qu'il ne reste qu'une seule empreinte, l'arbre est complet : l'empreinte finale obtenue est la racine de Merkle.

La racine de Merkle du bloc 751 005 est ainsi :

```
268a15b56fe847a067624bd0be186c375baccae9ac6db304438e9da657fe51d9
```

Le fait de placer la racine dans l'entête interdit à quiconque de modifier, d'ajouter ou de supprimer une transaction, sans modifier l'entête lui-même et devoir reproduire la preuve de travail. L'ensemble des transactions est ainsi attaché à l'entête, ce qui assure l'intégrité du bloc.

Cette organisation se révèle particulièrement utile pour les portefeuilles légers (dits à vérification de paiement simplifiée ou SPV) qui ne conservent pas la chaîne de blocs entière mais uniquement la chaîne des entêtes, qui est bien moins volumineuse (un peu plus de 62 Mio en novembre 2023). En effet, pour

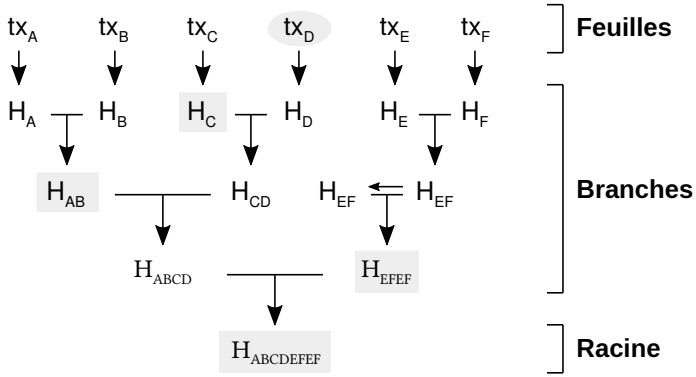

FIGURE 8.2 – Représentation d'un arbre de Merkle à six feuilles.

s'assurer de la présence d'une transaction dans un bloc, ils peuvent se contenter de demander les informations liées à la branche (chemin de Merkle) et procéder aux hachages eux-mêmes [18]. Par exemple, un utilisateur voulant vérifier la confirmation de la transaction tx_D doit simplement demander les informations H_C, H_{AB} et H_{EFEF} aux nœuds du réseau et procéder aux différents hachages pour comparer la racine obtenue avec celle contenue dans l'entête. Cela a pour effet de réduire considérablement la charge des portefeuilles légers.

Depuis l'activation de SegWit le 24 août 2017, chaque bloc contient un arbre de Merkle supplémentaire, subordonné à l'arbre classique des transactions décrit plus haut. Il s'agit de l'arbre témoin qui est l'arbre des transactions intégrant les signatures des transactions SegWit (séparées des transactions classiques). La racine de l'arbre témoin est placée dans la transaction de récompense, de sorte qu'elle est prise en compte dans la racine de Merkle principale, ce qui garantit l'intégrité de l'ensemble.

L'horodatage

L'horodatage indique la date et l'heure de construction du bloc qui sont déclarées par le mineur. D'un point de vue technique, il est donné par l'heure Unix, c'est-à-dire le nombre de secondes écoulées depuis le 1er janvier 1970 00:00:00 UTC. Pour notre bloc, l'horodatage est de 1661407005 ce qui correspond à la date du 25 août 2022 à 5 heures 56 minutes et 45 secondes (UTC).

Le mineur ne peut pas choisir cet horodatage au hasard. L'heure déclarée doit se situer dans le futur par rapport au temps médian passé (MTP) – la

médiane des horodatages des 11 derniers blocs, qui retarde généralement d'une heure sur le temps réel – et ne doit pas dépasser l'horloge des nœuds récepteurs de deux heures. Cette contrainte relativement permissive permet au temps réseau de rester relativement cohérent avec la réalité.

La valeur cible

La valeur cible est la valeur minimale que l'identifiant du bloc peut prendre pour que ce bloc constitue une preuve de travail. Plus cette valeur cible est petite, plus il est facile de trouver une solution et de miner un bloc. Elle est déterminée par le réseau selon les règles de l'algorithme d'ajustement de la difficulté.

La valeur cible est encodée comme un nombre flottant où le premier octet représente un exposant particulier et où la mantisse est déterminée par les 3 octets suivants. Ici, elle est égale à `0x09ed88` $\times\ 256^{(\texttt{0x17}-3)}$ c'est-à-dire :

```
0000000000000000000009ed880000000000000000000000000000000000000000
```

Cette information donne aussi la difficulté de minage du bloc, qui est inversement proportionnelle à la valeur cible. Il s'agit du quotient de la valeur cible maximale du système par la valeur cible du réseau [19]. La difficulté minimale du protocole est donc de 1 et celle de notre bloc (arrondie à l'unité près) est quant à elle de 28 351 606 743 494, ce qui représente un différentiel énorme ! Elle donne également la quantité de travail du bloc, qui est le nombre moyen de hachages nécessaires pour tomber sur une solution [20].

Le nonce

Le nonce désigne le nombre que le mineur fait varier pour produire la preuve de travail. Ce mot provient de l'expression anglaise « *for the nonce* » signifiant « pour la circonstance, pour l'occasion », ce qui indique la spécificité de son rôle [21]. Le mineur fait également varier un nonce supplémentaire au sein de la transaction de récompense, le champ du nonce étant trop petit (8 octets) pour la difficulté de minage actuelle. Le nonce de notre bloc est 4 224 551 499.

Ces deux derniers paramètres (valeur cible et nonce) sont relatifs à la preuve de travail et interviennent dans la formulation du problème mathématique résolu par le mineur. Ce problème se présente sous la forme d'une inégalité mathématique. En notant c la valeur cible du réseau et EB l'entête du bloc, il s'agit de trouver un nonce n tel que :

$$\text{SHA256d}(\ \text{EB}(\ n\ )\ )\ \leq\ c$$

Comme on l'a dit, le résultat est utilisé comme identifiant du bloc. La preuve de travail est facilement vérifiable : chaque membre du réseau peut, à partir des données du bloc, s'assurer que le mineur a bien trouvé une solution valide. Dans notre cas, si on compare l'identifiant et la valeur cible, on obtient bien un résultat qui satisfait l'inégalité exigée :

```
0x00000000000000000065aebf106c8824f4b565d54d6d6df32498b2b041cfd07 ≤
0x00000000000000000009ed880000000000000000000000000000000000000000
```

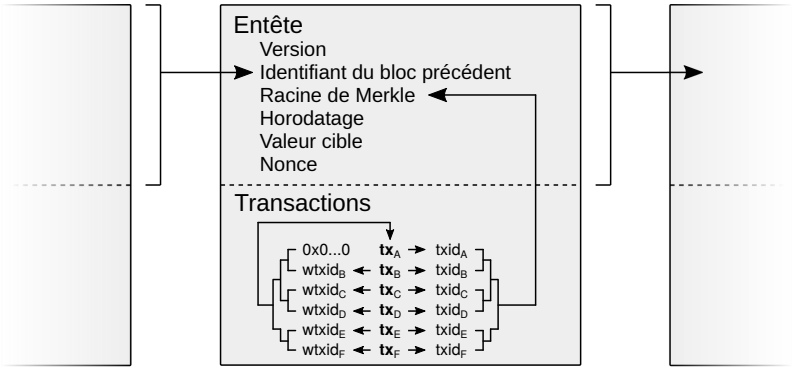

FIGURE 8.3 – Schéma d'un bloc de Bitcoin (avec SegWit).

Le revenu du minage

L'une des innovations de Bitcoin est de récompenser la confirmation des transactions à l'aide de son unité de compte interne. Cette propriété crée une incitation économique poussant les mineurs à bien se comporter, ce qui contribue à la solidité du système.

La récompense liée à l'ajout d'un bloc à la chaîne provient en partie de la création monétaire du protocole, d'où le nom de minage employé pour désigner cette activité. Le procédé est en effet analogue à l'extraction minière de l'or dans le monde réel : les mineurs déploient du capital et dépensent de l'énergie pour obtenir les nouveaux bitcoins. Comme expliqué par Satoshi dans le livre blanc :

> « L'ajout régulier d'une quantité constante de nouvelles pièces est analogue aux mineurs d'or qui dépensent des ressources pour ajouter de l'or à la circulation [22]. »

La deuxième partie de la récompense provient des frais de transaction payés par les utilisateurs, qui sont collectés sur les transactions incluses dans le bloc. Le tout est reversé au mineur lorsque le bloc est vérifié et accepté par le réseau.

Le minage est ainsi l'activité économique consistant à rassembler les transactions au sein d'un bloc, à produire la preuve de travail et à diffuser le résultat sur le réseau. Ici, nous le distinguons ainsi du simple hachage, qui consiste juste à réaliser les calculs pour créer la preuve de travail et qui peut être réalisé indépendamment de la sélection de transactions, notamment au sein des coopératives de minage (*mining pools*). Dans ce cadre, les mineurs sont les personnes ou les groupes de personnes réalisant l'activité complète, et les entités se contentant de mettre en place des machines et de déléguer leur pouvoir sur la sélection des transactions ne sont que des « hacheurs ».

Le minage se déroule de manière cyclique. Tout d'abord, le mineur sélectionne des transactions à partir de la réserve des transactions (appelée *mempool*) de son nœud. Puis, il construit un bloc candidat en imposant un entête, en assemblant les transactions et en prenant soin de construire une transaction de récompense qui le rémunère. Il fait ensuite varier le nonce et d'autres éléments du bloc candidat afin de produire la preuve de travail. Enfin, dans le cas où il trouve une solution, il diffuse le bloc sur le réseau le plus rapidement possible pour que les autres nœuds le vérifient et l'acceptent comme le nouveau bloc de la chaîne. Dans le cas contraire, si un nouveau bloc est trouvé entretemps, le mineur l'accepte et abandonne son bloc candidat. Dans les deux cas, la procédure reprend du début avec des transactions différentes.

La récompense de minage est ainsi récupérée par le mineur via l'inclusion d'une transaction de récompense au sein du bloc. Celle-ci doit être, par convention, la première transaction du bloc. Elle possède une entrée unique spécifique ne faisant référence à aucune transaction existante. La transaction de récompense est aussi appelée la base de pièce ou *coinbase*, car c'est à partir d'elle que sont formés les nouveaux bitcoins. Le mineur dirige cette transaction vers une adresse qu'il contrôle, de sorte qu'il est récompensé si et seulement si son bloc est valide aux yeux du réseau. La récompense que le mineur peut se verser doit être inférieure à la somme de la création monétaire et des frais de transaction. Le mineur peut ainsi se rémunérer moins que ce qui est prévu par le protocole, même si cela n'a aucun sens économique direct [23].

La création monétaire se fait intégralement par le biais de la transaction de récompense. Tous les bitcoins dans le système sont ainsi le résultat d'une série de transferts commençant par une telle transaction.

La particularité de cette création monétaire est qu'elle est fixée dans le temps et qu'elle n'est pas proportionnelle à la puissance de calcul déployée. Cela est rendu possible par l'algorithme d'ajustement de la difficulté, qui dérive du fait que le système constitue un serveur d'horodatage distribué. En effet, les blocs étant horodatés, il est possible de mesurer leur rythme de production passé et d'ajuster la difficulté de minage en conséquence. Ainsi, comme l'écrivait Satoshi :

> « Afin de compenser l'augmentation de la vitesse du matériel et la variation de l'intérêt des nœuds actifs au fil du temps, la difficulté de la preuve de travail est déterminée par une moyenne mobile visant un nombre moyen de blocs par heure. Si ces blocs sont générés trop rapidement, la difficulté augmente [24]. »

Dans la version principale de Bitcoin, l'intervalle de temps entre chaque bloc (temps de bloc) visé est de 10 minutes ou 600 secondes. L'ajustement a lieu tous les 2016 blocs, ce qui correspond environ à deux semaines, selon la moyenne simple du temps de bloc sur cette période. La nouvelle valeur cible est calculée [25] à partir de la valeur cible précédente (c_{k-1}) et du temps écoulé depuis le dernier ajustement (t_{k-1}) :

$$c_k = \frac{c_{k-1} \cdot t_{k-1}}{2016 \cdot 600}$$

Grâce à cet ajustement, le bitcoin possède une politique monétaire déterminée, qui n'est pas soumise à l'arbitraire direct d'un tiers de confiance ou à la quantité de capital déployé. Cette caractéristique le différencie de la monnaie fiat (comme le dollar) qui est émise de manière discrétionnaire par une banque centrale, ou du métal précieux (comme l'or) dont la quantité extraite connaît ses propres variations et suit la demande du marché à long terme. Cette politique monétaire a été décrite précisément pour la première fois par Satoshi Nakamoto dans son courriel de lancement du 8 janvier 2009 où il écrivait :

> « Le nombre total de pièces en circulation sera de 21 000 000. Elles seront distribuées aux nœuds du réseau lorsqu'ils créeront des blocs, la quantité émise étant divisée par deux tous les 4 ans.
>
> les 4 premières années : 10 500 000 pièces
> les 4 années suivantes : 5 250 000 pièces
> les 4 années suivantes : 2 625 000 pièces
> les 4 années suivantes : 1 312 500 pièces
> etc...
>
> Une fois cette somme épuisée, le système pourra prendre en charge les frais de transaction si nécessaire. Il repose sur la concurrence du marché ouvert, et il y aura probablement toujours des nœuds prêts à traiter les transactions

gratuitement [26]. »

Elle est bien évidemment inscrite dans le code, où elle est appelée subvention ou *subsidy* en anglais.

L'originalité principale de cette politique monétaire est que la création monétaire est réduite de moitié de manière brusque tous les 210 000 blocs (soit environ 4 ans) lors de ce qu'on appelle couramment un *halving*. En 2023, trois réductions de moitié avaient déjà eu lieu sur le réseau Bitcoin principal : la première s'est produite le 28 novembre 2012, lorsque la subvention du protocole est passée de 50 bitcoins par bloc à 25 ; la deuxième le 9 juillet 2016, avec une baisse à 12,5 bitcoins par bloc ; la troisième le 11 mai 2020, où la subvention a été réduite à 6,25 bitcoins par bloc. La prochaine réduction de moitié devrait se passer en avril 2024, après laquelle les nouveaux bitcoin émis seront de 3,125 par bloc. Sauf modification des règles de consensus, la dernière réduction de moitié sera la 33e et aura lieu aux alentours de 2140. En effet, le montant de création monétaire par bloc passera alors en dessous du satoshi, soit zéro par troncature à l'unité.

À long terme, cette politique monétaire atypique fait du bitcoin une monnaie à quantité fixe. En effet, le montant maximal de bitcoins en circulation doit tendre, au fil du temps, vers une limite : la fameuse limite des 21 millions. Celle-ci n'est qu'une déduction des conditions d'émission susmentionnées, ce qui s'exprime en termes mathématiques par la convergence de la série des montants minés entre les halvings [27] :

$$N_{\max} = \sum_{i=0}^{+\infty} \left(210\,000 \cdot \frac{50}{2^i} \right) = 21\,000\,000 \cdot \sum_{i=1}^{+\infty} \left(\frac{1}{2} \right)^i = 21\,000\,000$$

La limite des 21 millions est une borne supérieure : en l'absence d'un changement des règles de consensus, elle ne sera jamais formellement atteinte, en raison de la nature optionnelle de la récompense de minage, du caractère discret des unités et de la perte irrémédiable de bitcoins. De plus, les bitcoins dont les propriétaires ont perdu leurs clés privées réduisent considérablement la quantité réelle de bitcoins en circulation sans pour autant que cela ne soit pris en compte dans le calcul.

La création monétaire a ainsi vocation à s'amenuiser et à devenir négligeable, et ce plus rapidement que l'on imagine. En effet, en 2023, le nombre de bitcoins dépensables avait déjà dépassé les 19,5 millions. C'est pourquoi cette subvention doit en toute logique être remplacée par l'autre source de revenu pour les mineurs, à savoir les frais de transaction [28].

Les frais de transaction sont les commissions payées par les utilisateurs pour la confirmation de leurs transactions. Les frais d'une transaction peuvent être versés directement par l'expéditeur (client) ou indirectement par le destinataire (commerçant) par l'intermédiaire d'une remise sur le produit vendu. Ils sont récupérés par le mineur sur chaque transaction du bloc selon une règle implicite : il s'agit de la différence entre le montant en entrée de la transaction et son montant en sortie. Cette différence peut être de zéro (transaction gratuite), mais elle est toujours comptabilisée. Les frais sont ajoutés à la transaction de récompense indistinctement des bitcoins issus de la création monétaire. Bitcoin intègre ainsi un système interne et optimisé de frais de transaction, qui évite l'alourdissement inutile des transactions et des blocs.

L'existence des frais de transaction a vocation à perdurer par conception, même si ceux-ci devenaient très bas. Contrairement à l'opinion exprimée par Satoshi, la confirmation d'une transaction a en général un coût, même marginal [29], et une transaction qui paie trop peu de frais par rapport à la charge apportée n'a aucune raison économique d'être confirmée. De ce fait, il n'y a pas lieu de s'imaginer que la chaîne de blocs s'arrête.

En outre, les règles du protocole restreignent usuellement l'espace de bloc par le biais d'une limite explicite sur la taille (ou le poids) des blocs. Cette restriction crée un plafond de production qui, lorsqu'il est atteint, fait que le mineur rationnel sélectionne les transactions qui paient le taux le plus élevé de frais, toutes choses étant égales par ailleurs. Il existe donc, dans le cas d'une congestion du réseau, un effet d'enchères pouvant faire augmenter le niveau moyen des frais de manière drastique.

Bien que les frais constituent la façon principalement envisagée de rémunérer les mineurs à terme, des méthodes alternatives de financement ont été proposées.

La première est l'émission résiduelle (*tail emission*), qui consiste à maintenir une création monétaire constante au cours du temps, dans le but que le revenu de minage ne tombe pas trop bas [30]. L'instauration de cette caractéristique aurait pour effet de modifier la politique monétaire du bitcoin et de faire disparaître la limite des 21 millions, d'où son caractère hautement controversé.

Pour donner un exemple, l'émission résiduelle est mise en place dans la variante Monero depuis 2015. Elle est devenue effective le 9 juin 2022, date depuis laquelle il se crée 0,3 monero par minute, soit un taux de création monétaire annualisé de 0,87 % à ce moment-là. Une telle émission résiduelle existe également dans Dogecoin depuis 2015, à raison de 10 000 dogecoins par minute, pour un taux annualisé de 3,7 % en novembre 2023.

La deuxième méthode de financement proposée est le demeurage, ou coût de détention, qui consiste à prélever la monnaie demeurée immobile depuis un temps donné [31]. Les bitcoins de Satoshi, qui représentent une manne financière importante, sont notamment concernés. Toutefois, il s'agirait d'une atteinte au système de propriété de Bitcoin et il y a donc peu de chances que cette méthode rencontre le succès.

La chaîne la plus longue

Venons-en maintenant au sujet central de ce chapitre : l'atteinte du consensus par le minage. Comme nous l'avons expliqué ci-dessus, le minage est le procédé permettant aux mineurs d'ajouter des blocs à la chaîne, chose pour laquelle ils sont rémunérés. Mais nous n'avons pas exposé comment il permettait d'arriver à un accord dans un contexte antagoniste, en présence d'acteurs malveillants « byzantins ».

Les nœuds suivent un protocole composé des règles de réseau, qui leur permettent de rentrer en communication, et des règles de consensus, qui concernent la forme des transactions et des blocs, que nous détaillerons dans le chapitre 10. Les nœuds qui enfreignent ces règles voient leurs connexions être fermées par leurs pairs et sont mis sur liste noire si nécessaire. Il est donc impossible de faire accepter une transaction ou un bloc au réseau qui ne soit valide selon les règles de consensus.

Néanmoins, les nœuds byzantins peuvent semer la discorde dans le respect des règles de consensus, en produisant des blocs concurrents. En effet, rien n'empêche *a priori* un attaquant de produire des blocs de transactions qui soient valides mais qui ne soient pas rattachés à la branche principale et de les soumettre au réseau.

Ce problème est résolu par le biais d'un principe simple mais efficace : le principe de la chaîne la plus longue. Celui-ci a été décrit par Satoshi dans le livre blanc :

> « La décision majoritaire est représentée par la chaîne la plus longue, sur laquelle le plus grand effort de preuve de travail a été investi [32]. »

Les nœuds du réseau se mettent d'accord en sélectionnant la chaîne possédant le plus de travail accumulé, ce qui se matérialise généralement par une chaîne plus longue en nombre de blocs [33]. Lorsqu'une chaîne possédant une quantité strictement plus grande de travail est publiée, les nœuds suivent cette chaîne, que celle-ci soit dans la continuité de la dernière ou qu'elle fasse

référence à une branche plus ancienne. Cette règle fait en sorte que les nœuds suivent toujours la chaîne sur laquelle un montant supérieur d'énergie a été investi. L'algorithme de consensus résultant de l'application de ce principe est appelé l'algorithme de consensus de Nakamoto par preuve de travail, en hommage à son concepteur.

La meilleure manière d'appréhender le fonctionnement de cet algorithme est de prendre le cas d'un embranchement (appelé *fork* en anglais) de la chaîne. Celui-ci peut être créé par un acteur malveillant, mais dans la réalité il est généralement engendré de manière accidentelle, lorsque deux mineurs éloignés trouvent chacun un bloc différent dans un intervalle de temps réduit et que les nœuds du réseau ne reçoivent pas le même bloc en premier. Il n'y a alors aucun moyen de départager les deux branches, celles-ci étant également correctes en vertu du principe de la chaîne la plus longue. Ce type d'embranchement accidentel est commun et se produit de temps en temps sur le réseau pour des raisons de latence.

Cette situation et sa résolution ont été décrites par Satoshi dans le livre blanc :

> « Si deux nœuds transmettent simultanément des versions différentes du bloc suivant, certains nœuds peuvent recevoir l'une ou l'autre version en premier. Dans ce cas, ils travaillent sur la première version qu'ils ont reçue, mais conservent l'autre branche au cas où elle deviendrait plus longue. L'égalité est rompue lorsque la preuve de travail suivante est trouvée et qu'une branche devient plus longue ; les nœuds qui travaillaient sur l'autre branche passent alors sur la chaîne la plus longue [34]. »

Le réseau passe par trois étapes. Tout d'abord, il se comporte de manière attendue : les mineurs prolongent la chaîne la plus longue, sur laquelle le reste des nœuds se coordonnent. Puis, le conflit a lieu : deux branches correctes coexistent et les mineurs travaillent pour prolonger la chaîne à partir du bloc reçu en premier. Enfin, l'embranchement est résolu : un mineur trouve un nouveau bloc et sa chaîne, qui devient plus longue, est acceptée par le réseau.

Il se produit alors ce qu'on appelle une recoordination (*reorganization*) qui réconcilie les nœuds du réseau entre eux. Le bloc de la branche faible est considéré comme incorrect et mis de côté. On dit que ce bloc est rendu orphelin (*orphaned*) car il perd son attachement à la chaîne mère [35]. La branche forte (possédant le plus de travail accumulé) est considérée comme la version correcte de la chaîne.

Tout conflit sur le réseau est résolu de la sorte, ce qui a pour conséquence de conférer une nature particulière à l'algorithme de Nakamoto, et par extension

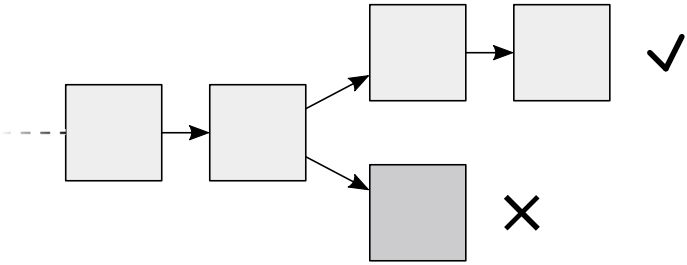

FIGURE 8.4 – Schéma d'un embranchement commun de la chaîne.

à Bitcoin.

Ce fonctionnement impose tout d'abord deux contraintes majeures sur la sécurité. La première est que la sécurité minière du réseau repose sur la supposition qu'une majorité de la puissance de calcul (« 51 % ») se comporte de manière honnête. Comme l'expliquait Satoshi :

> « Le système est sécurisé tant que les nœuds honnêtes contrôlent collectivement plus de puissance de calcul qu'un groupe de nœuds qui coopéreraient pour réaliser une attaque [36]. »

La seconde est que la sécurité d'une transaction donnée est probabiliste et dépend de la profondeur à laquelle elle se trouve dans la chaîne. La transaction est d'abord vérifiée par le réseau (zéro confirmation), puis confirmée au sein d'un bloc (une confirmation) et finit par être considérée comme irréversible, généralement à partir de six confirmations pour les montants ordinaires sur la version principale de Bitcoin. Cela contraint l'utilisateur à estimer le nombre de confirmations qu'il doit attendre en fonction de la sécurité désirée.

Cette particularité se transcrit dans le fonctionnement du minage par la maturité de la base de pièce (*coinbase maturity*), qui est le nombre de confirmations nécessaire pour que la sortie de la transaction de récompense devienne dépensable. Cette contrainte est mise en place pour éviter la mauvaise utilisation des fonds due à une recoordination peu profonde. Le délai sur le réseau BTC est aujourd'hui de 101 confirmations.

L'algorithme de Nakamoto possède également trois avantages principaux. D'abord, il a pour intérêt d'avoir un critère objectif sur lequel se reposer : tout le monde peut reconstituer la chaîne à partir du bloc de genèse et constater qu'il s'agit de la chaîne correcte. Même dans le cas extrême d'un cloisonnement mondial et prolongé du réseau dû à une guerre ou une catastrophe naturelle, le système peut finir par se recoordonner [37].

Ensuite, il permet la participation ouverte au consensus : tout ce qui est requis du mineur est une preuve de travail valide, de sorte que le minage est anonyme par essence.

Enfin, cet algorithme par preuve de travail assure la robustesse du réseau : un mineur n'a pas à connaître tous les autres participants, ce qui permet au réseau d'être composé de dizaines (voire de centaines) de milliers de nœuds.

La résistance à la double dépense

La double dépense est le fait pour un acteur de faire accepter successivement deux transactions au réseau dans le but de déstabiliser l'état du système et d'en bénéficier d'une manière ou d'une autre. La deuxième transaction peut constituer une annulation de la première, dans laquelle l'acteur malveillant réalise un transfert vers lui-même.

La double dépense constitue un problème dans le cas des transactions non confirmées, c'est-à-dire des transactions qui ont été diffusées sur le réseau, vérifiées par les nœuds et placées dans leurs *mempools*, mais qui n'ont pas encore été incluses dans un bloc de la chaîne. Aucun consensus n'a été réalisé à propos de ces transactions, mais le commerçant peut décider de les accepter dans le cas où les montants engagés sont faibles [38]. Le risque est qu'un fraudeur reparte avec la marchandise et réussisse à faire accepter une version alternative de la transaction vue par le commerçant, soit en la diffusant au même moment et en espérant qu'elle arrive en premier au mineur, soit en payant plus de frais (ce qui peut être fait systématiquement avec Replace-by-Fee) pour soudoyer le mineur, soit encore en minant préalablement un bloc contenant la transaction (attaque Finney [39]).

La solution à ce problème est de se mettre d'accord sur la transaction correcte pour faire disparaître la double dépense, *ce qui est précisément le but du minage*. Cependant, le minage n'empêche pas la double dépense de manière absolue, étant plutôt un mécanisme de résistance. Voyons ce qui garantit cette caractéristique.

Un certain nombre de perturbations opportunistes peuvent avoir lieu au niveau de l'activité minière comme l'attaque vector76 [40] ou le minage égoïste [41], mais la plus importante d'entre elles est l'attaque de double dépense par recoordination de chaîne. Celle-ci consiste à utiliser une part importante de la puissance de calcul du réseau (généralement une majorité) afin de réécrire le passé de la chaîne et modifier une ou plusieurs transactions. Cette attaque a été décrite précisément par Satoshi Nakamoto dans le livre blanc [42] et dans son courriel de réponse à John Levine du 3 novembre 2008 [43].

Cette attaque est réalisée en trois étapes. Elle peut être faite à l'aide d'une minorité de la puissance de calcul, auquel cas elle ne possède qu'une certaine probabilité de réussir. Cependant, par souci de simplicité, nous supposerons qu'un mineur a réuni la majorité de la puissance de calcul du réseau. L'attaque constitue donc une attaque des 51 %, aussi appelée attaque de la majorité.

La première étape est l'achat d'un bien ou d'un service auprès d'un commerçant. L'attaquant procède à une transaction en bitcoins (dite « légitime ») en l'échange de quoi le commerçant lui fournit une chose de même valeur. Typiquement, il s'agira d'une autre cryptomonnaie ou du dollar auprès d'une plateforme de change.

La deuxième étape est le minage d'une chaîne parallèle. Une fois que la transaction légitime a été confirmée au sein d'un bloc, l'attaquant construit une chaîne parallèle en secret à partir du bloc précédent, qu'il prend soin de ne pas dévoiler au reste du réseau. Dans le même temps, il crée et signe une autre transaction (dite « frauduleuse ») qui dépense les mêmes bitcoins que la première et qui les renvoie vers une adresse en son contrôle. Il inclut cette transaction frauduleuse dans sa chaîne parallèle. Puisque l'attaquant dispose de la majorité de la puissance de calcul du réseau, il est sûr qu'à un moment ou à un autre, cette chaîne sera plus longue que l'autre.

La troisième étape est la recoordination de chaîne, représentée sur la figure 8.5. L'attaquant a continué de miner sa chaîne parallèle jusqu'à la livraison du bien économique acheté. À ce moment-là, il dévoile sa chaîne au reste du réseau, qui doit accepter celle-ci en vertu du principe de la chaîne la plus longue. Les nœuds procèdent alors à une recoordination : les blocs de l'ancienne chaîne sont écartés (rendus orphelins), leurs transactions sont remises dans la mempool et les nouveaux blocs sont vérifiés et ajoutés à la chaîne. Comme la transaction légitime dépense les mêmes fonds que la transaction frauduleuse, qui est incluse dans la nouvelle chaîne, cette transaction légitime est invalidée en tant que double dépense. Le commerçant ne possède plus les bitcoins, qui reviennent à l'attaquant.

Il s'agit d'une attaque opportuniste : elle est motivée par un gain, c'est-à-dire le bien économique obtenu, qui doit être supérieur au coût (matériel, logistique, électrique et logiciel) nécessaire pour y procéder. Sur le réseau Bitcoin principal, ce coût se chiffre aujourd'hui en milliards de dollars [44].

Cette attaque doit être distinguée de la censure, que nous décrirons dans le chapitre 9, et qui consiste à refuser de confirmer des transactions selon un critère arbitraire. Cette dernière repose en effet sur des incitations *extérieures* à l'économie de Bitcoin, le mineur rationnel n'ayant, au sein du système, aucun

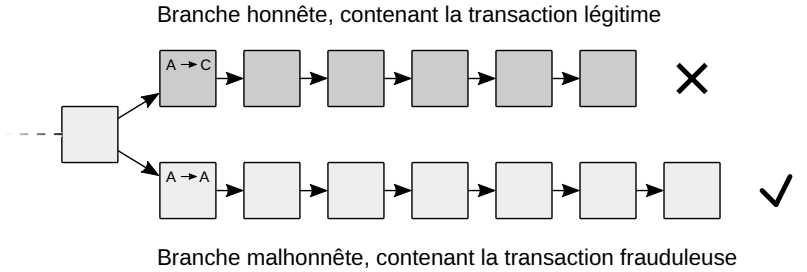

FIGURE 8.5 – Attaque de double dépense par recoordination de chaîne.

intérêt économique à ne pas inclure les transactions payant un taux de frais suffisant dans ses blocs.

Comme souligné par Satoshi, le système est sécurisé tant que la majorité de la puissance de calcul est associée à des nœuds honnêtes, c'est-à-dire des nœuds qui ne cherchent pas à réaliser des doubles dépenses, ni censurer. La sécurité minière repose donc sur une barrière de sécurité, qui représente la charge financière de l'attaquant pour réaliser une double dépense.

Cette barrière n'est pas construite de manière bénévole mais repose sur la récompense du protocole, faisant du minage un procédé essentiellement *économique*. En particulier, la résistance à la double dépense – à savoir la difficulté à effectuer une attaque de double dépense – dérive directement du revenu minier total, qui incite les nœuds à rester honnêtes. Tel que l'écrivait Satoshi dans le livre blanc :

> « L'incitation peut contribuer à encourager les nœuds à rester honnêtes. Si un attaquant cupide est capable de réunir plus de puissance de calcul que l'ensemble des nœuds honnêtes, il aura à choisir entre l'utiliser pour escroquer des gens en leur récupérant ses paiements, ou l'utiliser pour générer de nouvelles pièces. Il devrait trouver plus rentable de respecter les règles du jeu, celles-ci lui permettant d'obtenir plus de nouvelles pièces que tous les autres réunis, plutôt que de saper le système et la validité de sa propre richesse [45]. »

Non seulement la récompense peut être supérieure au gain d'une attaque de double dépense, mais la valeur des bitcoins servant à réaliser la transaction peut aussi être réduite par ladite attaque. En effet, si l'attaque était amenée à être couronnée de succès, on peut imaginer que les différents acteurs diminueraient leur confiance dans le système, arrêteraient de l'utiliser pour le commerce et cèderaient une partie de leur épargne, faisant baisser le revenu de minage et la valeur d'échange du bitcoin. De plus, la spécialisation du matériel de minage (quand elle existe) alourdit le coût de l'attaque, car ce matériel perd dans ce

cas en utilité. D'un point de vue purement opportuniste, il est donc la plupart du temps bien plus rentable d'utiliser son capital de manière honnête.

Il est ainsi arrivé que des agrégats de mineurs rassemblent plus de 51 % de la puissance de calcul, comme la coopérative GHash.io en juillet 2014, sans qu'aucune attaque ne se produise. Et même si une telle attaque avait lieu, celle-ci ne serait pas forcément fatale pour le système à long terme. Comme l'écrivait Satoshi :

> « Même en cas de réussite, cela n'expose pas le système à des modifications arbitraires, comme la création de valeur *ex nihilo* ou l'appropriation d'argent n'ayant jamais appartenu à l'attaquant. Les nœuds ne vont pas accepter une transaction invalide comme paiement, et les nœuds honnêtes n'accepteront jamais un bloc les contenant [46]. »

Ainsi de nombreuses attaques de ce type ont déjà eu lieu sur certaines variantes de Bitcoin au fil des années, réduisant leur réputation au passage, mais sans qu'elles ne soient pour autant anéanties. On peut notamment citer Ethereum Classic qui a subi plusieurs recoordinations agressives entre 2019 et 2020.

L'industrie minière

Le minage est une activité économique à part entière, la récompense de minage servant à rémunérer le service apporté par le mineur. Cette récompense paie pour le coût de l'électricité, de l'infrastructure matérielle et logistique, et de la maintenance logicielle. Elle compense le risque de production de blocs orphelins. Elle rémunère la confirmation des transactions censurées. Et enfin elle récompense la renonciation temporaire à la liquidité (intérêt originaire du prêteur) et le risque économique général (profit de l'entrepreneur).

Du côté de l'infrastructure matérielle, les mineurs ont besoin de déployer un certain nombre d'éléments : les machines de hachage (systèmes de refroidissement compris) pour procéder aux calculs liés à la preuve de travail, le processeur pour traiter les blocs et vérifier les signatures, la mémoire pour conserver la chaîne (l'historique), l'ensemble des sorties transactionnelles non dépensées (l'état) et la réserve des transactions en attente, la bande passante pour envoyer et recevoir les transactions et les blocs, etc. Et force est de constater que tout cela s'est industrialisé au fur et à mesure des années.

L'amélioration de la machine pour procéder au hachage illustre bien cette industrialisation. Initialement les mineurs minaient avec le processeur central (CPU) de leur ordinateur. Puis, en 2010, sous l'impulsion de Laszlo Hanyecz

puis d'ArtForz, le minage par processeur graphique (GPU) s'est développé. En 2011, est apparu le premier circuit logique programmable FPGA consacré au minage, qui donnait un meilleur rendement que les cartes graphiques. Enfin, en 2013, les premiers circuits intégrés spécialisés (ASIC) ont été mis sur le marché, avec la sortie de l'Avalon ASIC. À partir de là, les ASIC sont devenus de plus en plus performants, notamment par le travail de l'entreprise chinoise Bitmain sur ses Antminers.

Certains acteurs se sont mis à miner de manière industrielle en entassant cette puissance de hachage dans des grands entrepôts spécialisés contenant des centaines de machines, appelés des fermes de minage. Ces fermes ont été installées dans des endroits suivant des facteurs spécifiques dont notamment le coût de l'électricité, la température (coût du refroidissement), la bande passante et l'instabilité politique. Cette émergence de fermes de minage composées d'appareils spécialisés avait été prévue par Satoshi qui écrivait dès novembre 2008 :

> « Au début, la plupart des utilisateurs feront fonctionner des nœuds de réseau, mais à mesure que le réseau grandira, au-delà d'un certain point, cette tâche sera de plus en plus déléguée à des spécialistes possédant des fermes de serveurs composées de matériel spécialisé. Une ferme de serveurs n'aura besoin que d'un seul nœud sur le réseau et le reste du réseau local sera connecté à ce nœud [47]. »

La puissance de calcul du réseau a par conséquent explosé. Le taux de hachage [48], mesuré en hachages par secondes (H/s), a ainsi connu une spectaculaire croissance au cours des années. En 2009, il oscillait entre 1 et 7 millions de hachage par seconde (1 MH/s). Durant la première partie de 2010, il a progressé pour atteindre les 200 MH/s début juillet. Puis, il a connu deux hausses majeures coïncidant avec les engouements spéculatifs mais aussi avec l'utilisation de méthodes optimisées. La première a été celle de 2010–2011 où le prix est passé de moins d'un centime à 30 $ et où les premières fermes de cartes graphiques ont été utilisées : entre juillet 2010 et août 2011, le taux de hachage est passé de 200 MH/s à 15 TH/s (soit une multiplication par 75 000). La seconde a été celle de 2013–2014, période durant laquelle le prix a été quasiment multiplié par 100 et où les premiers ASIC ont été déployés : le taux de hachage est passé de 25 TH/s en janvier 2013 à 300 PH/s en décembre 2014 (soit une multiplication par 12 000). Le taux de hachage a enfin lentement progressé pour atteindre environ 450 EH/s en novembre 2023 (ce qui correspond à une multiplication par 1 500 depuis décembre 2014).

Avec cette croissance énorme de la puissance de calcul, la difficulté du minage a suivi. Dès 2010, il devenait difficile d'espérer miner un bloc avec

le processeur de son ordinateur. Cela a eu pour effet de désavantager les petits mineurs. L'augmentation de la difficulté a mis en évidence un défaut inhérent du minage : le défaut de variance. Puisque le minage est soumis aux probabilités, le mineur individuel doté d'un ASIC performant peut ne pas trouver de bloc du tout, tout comme il peut trouver plus de blocs que prévu, faisant reposer son revenu sur le hasard.

C'est pour corriger ce défaut de variance que sont nées les coopératives de minage (appelées *mining pools* en anglais). Ces dernières sont des regroupements de hacheurs qui délèguent leur pouvoir sur la sélection des transactions à un opérateur, afin de participer de manière commune à l'effort de calcul et de lisser leurs revenus. Le fonctionnement par coopératives se base sur la production de preuves de travail partielles (PPoW) mise en place par le protocole Stratum. Il s'agit pour le hacheur de produire une preuve de travail de degré moindre pour un bloc candidat donné, afin de prouver qu'il a dépensé de l'énergie et d'être rémunéré en conséquence par la coopérative. La coopérative reçoit la récompense de minage à chaque fois qu'une preuve de travail partielle produite par le hacheur s'avère être également une preuve de travail complète (FPoW).

La première coopérative de minage a été lancée le 27 novembre 2010 par Marek Palatinus (aussi connu sous le pseudonyme de *slush*). Elle portait initialement le nom de Bitcoin.cz Mining avant d'être plus tard rebaptisée Slush Pool en hommage à son fondateur, puis de devenir Braiins Pool en septembre 2022. Aujourd'hui, les coopératives de minage sont nombreuses et concentrent l'essentiel de la puissance de calcul du réseau. Elles sont généralement basées dans les juridictions où le minage est très présent, comme la Chine (jusqu'en 2021) ou plus récemment les États-Unis.

Les coopératives ont pour habitude de signaler les blocs qu'elles minent dans un souci de transparence. Par exemple, la transaction de récompense du bloc 751 005 contient la chaîne de caractères `poolin.com`, ce qui indique que ce bloc a très probablement été validé par la coopérative chinoise Poolin. Ce signalement n'est pas obligatoire (le minage est anonyme par essence), mais permet d'avoir une idée de la répartition des différentes coopératives (comme on peut le voir sur la figure 8.6) et d'estimer par conséquent la centralisation de l'activité minière.

Un autre défaut inhérent du minage est la latence liée à l'annonce des blocs. Comme expliqué dans la section sur la chaîne la plus longue, cette latence produit des blocs orphelins, qui sont valides mais ne sont pas rattachés à la chaîne principale. Cela fait que des mineurs mal connectés ont une puissance

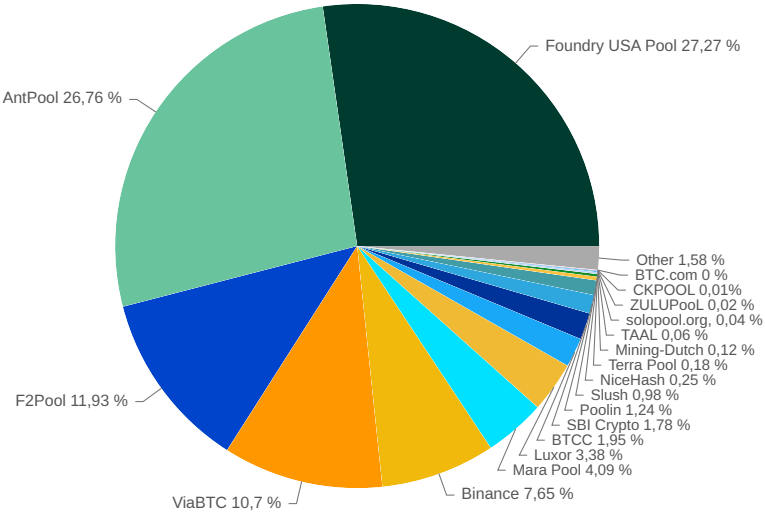

FIGURE 8.6 – Répartition du taux de hachage apparent entre les coopératives de minage de BTC, semaine du 5 au 12 octobre 2023. (source : coin.dance)

de hachage apparente inférieure à leur puissance de hachage réelle.

Pour tenter d'atténuer les effets de ce défaut, les mineurs ont mis en place des relais de communication permettant de s'envoyer des blocs mutuellement de manière plus efficace en supprimant les protections contre le déni de service nécessaires sur le réseau pair à pair ouvert.

Le premier relai a été créé par Matt Corallo sous le nom de *Bitcoin Relay Network*. Il a été lancé en 2013 et est devenu pleinement fonctionnel en 2015. Le réseau était composé de plusieurs nœuds spécialisés hébergés sur l'infrastructure Amazon Web Services. Un concurrent était le réseau Falcon, géré par une équipe de l'université Cornell dirigée par Emin Gün Sirer. Le Bitcoin Relay Network a été remplacé en 2016 par le réseau FIBRE[49] (pour *Fast Internet Bitcoin Relay Engine*), un réseau basé sur UDP (protocole alternatif à TCP) qui implémente l'optimisation `cmpctblock`, toujours géré par Matt Corallo. C'est ce réseau qui est utilisé par la plupart des mineurs aujourd'hui.

Cette industrialisation du minage a mené à la centralisation de l'activité minière, à la fois au niveau de la puissance de hachage (fermes de minage) que de la sélection des transactions (coopératives et relais). Si cette agrégation n'est pas fatale (les hacheurs sont libres de quitter leur coopérative pour une autre et les mineurs sont libres de ne pas utiliser le relai), elle n'en diminue pas moins la sécurité minière de la chaîne.

Certaines améliorations ont été proposées dans le minage pour corriger ce problème. La première est le protocole P2Pool, qui est un protocole de minage coopératif basé sur un réseau pair à pair de mineurs. Celui-ci met en communication les hacheurs en se basant sur une chaîne latérale – la « chaîne de partage » – dont la difficulté est plus faible et qui regroupe les différentes contributions des participants. Le développement de P2Pool sur la version principale de Bitcoin semble avoir été mis en suspens en 2017. Toutefois, le procédé est mis en œuvre sur Monero depuis octobre 2021 au moyen d'une coopérative du même nom.

Le seconde est le protocole Stratum V2 [50], qui permet (entre autres) aux hacheurs de négocier le contenu des blocs. À défaut de corriger complètement la délégation sur la sélection des transactions, cette nouvelle version de Stratum a le mérite de rendre le processus plus transparent. En novembre 2023, elle n'était déployée qu'au sein de la coopérative Braiins Pool (anciennement Slush Pool), qui est à l'origine de sa conception.

Cependant, ces propositions d'amélioration, bien que louables, ne suppriment pas l'avantage économique découlant de la centralisation, qui se retrouve par ailleurs dans toutes les industries (économie d'échelle). La décentralisation a un coût, et celui-ci ne sera justifié que lorsque le bénéfice apporté le surpassera, c'est-à-dire le jour où le réseau sera réellement attaqué.

Un algorithme de consensus novateur

Pour fonctionner en tant que système distribué de monnaie numérique, Bitcoin se base sur un mécanisme de consensus novateur. Celui-ci met en jeu une chaîne de blocs construite par les mineurs, qui sont rémunérés pour leur travail. Chaque bloc est un ensemble horodaté de transactions, qui contient une preuve de travail quantifiant l'énergie dépensée. Le consensus est atteint par la sélection de la plus longue chaîne.

Cet algorithme de consensus a un fonctionnement objectif, ouvert et robuste, ce qui explique le succès de Bitcoin par rapport à ses prédécesseurs. Par son aspect essentiellement économique, il donne au système une très grande résistance à la double dépense opportuniste, notamment grâce à la gigantesque industrie minière qui le soutient.

Il existe cependant une menace plus importante, plus insidieuse : celle de la censure, dont nous parlerons dans le prochain chapitre.

9

La résistance à la censure

L'un des problèmes croissants de notre époque est la censure financière. Avec le développement de l'économie mondialisée, reposant notamment sur Internet, le recours aux intermédiaires financiers est devenu de plus en plus courant. Cette évolution fait que l'entrave de transferts monétaires constitue aujourd'hui une complication générale, expérimentée par une part grandissante de la population.

Bitcoin forme une solution à ce problème. L'une de ses caractéristiques primordiales est en effet sa résistance à la censure, c'est-à-dire le fait qu'il est difficile pour une entité quelconque d'empêcher la réalisation d'un paiement. En permettant « aux paiements en ligne d'être envoyés directement d'une partie à l'autre sans passer par une institution financière », Bitcoin contourne l'arsenal de contrôles financiers qui gangrènent nos moyens de paiement et d'épargne modernes.

La résistance à la censure est, comme la confirmation des transactions, un mécanisme économique. Elle se fonde de manière essentielle sur la preuve de travail ainsi qu'elle est appliquée dans l'algorithme de consensus de Nakamoto. De ce fait, les alternatives proposées comme les algorithmes de preuve d'enjeu montrent une résistance à la censure bien plus faible.

Dans ce chapitre, nous verrons d'abord comment la censure financière intervient dans le monde bancaire aujourd'hui et pourquoi elle devrait se généraliser à l'avenir avec le déploiement des monnaies numériques de banque

centrale. Puis, nous décrirons de quelle façon la censure peut s'exercer dans Bitcoin et comment le système peut y résister. Nous expliquerons enfin en quoi les propositions alternatives ne suffisent pas.

Qu'entendons-nous par censure financière ?

La notion de censure peut paraître étrange de prime abord quand on parle de monnaie. Au sens courant, la censure désigne la restriction de l'expression, notamment par l'interdiction de la diffusion de certaines idées. Néanmoins, il est possible de la comprendre dans un sens plus large, qui mêle paiement et expression.

Le terme de censure vient du latin *censeo* signifiant « évaluer », « estimer », « déclarer », « juger ». Il trouve son origine dans une institution importante de la République romaine, celle des censeurs, deux magistrats qui avaient pour charge de procéder au dénombrement des citoyens et de leurs biens (le *census*), de collecter les impôts, de superviser les travaux publics, de gérer la liste des personnes admises au Sénat (l'*album senatorium*) et de veiller au maintien des « bonnes mœurs » de la population en administrant des blâmes ou des peines temporaires. La première fonction des censeurs a donné sa signification au mot recensement. La seconde aux concepts de cens et de suffrage censitaire. Et la dernière a été à l'origine de ce que nous appelons la censure.

Au Moyen Âge, le mot latin *censura* a été repris par le catholicisme pour prendre un sens religieux et se limiter ainsi au discours, et en particulier aux textes. La censure s'apparentait alors à un blâme (sens encore parfois employé, notamment en matière de critique littéraire) ou à une interdiction. Elle se caractérisait par la relecture et la correction des ouvrages rédigés pour s'assurer que tout était conforme au dogme de l'Église catholique romaine.

Néanmoins, l'apparition de l'imprimerie au XV^e^ siècle a bouleversé les choses : le nombre de livres a explosé, et ce faisant, a retiré le contrôle que la hiérarchie catholique avait sur la publication des écrits, contrôle qui a été transféré à l'État. La censure a par conséquent acquis son sens politique actuel, en désignant l'examen que le pouvoir étatique fait préalablement des livres, journaux, pièces de théâtre, etc., pour en permettre ou en prohiber la publication ou la représentation. Par la suite, le terme a fini par nommer toute atteinte à la liberté d'expression, quel que soit le support, que cela se fasse avant (censure a priori) ou après la diffusion (censure a posteriori).

Avec le développement des médias de masse (journaux, radio, télévision) et surtout des médias sociaux, le terme a acquis un sens élargi et on s'est mis à

parler de censure pour tout choix d'édition pris par une entité privée vis-à-vis de ses clients ou de ses utilisateurs. Cette censure privée n'est pas une atteinte à la liberté d'expression au sens strict, mais elle pose problème lorsque le domaine est monopolisé par un petit nombre d'acteurs bénéficiant souvent d'un avantage légal ou d'une subvention étatique. De plus, cette censure peut être directement l'émanation d'une intervention politique, la plateforme en question ne faisant qu'appliquer les directives générales du pouvoir [1].

Cependant, cette censure de l'expression peut également être réalisée par l'atteinte de l'activité économique de celui qui s'exprime. En effet, en restreignant la capacité à gagner de l'argent d'une personne et en lui faisant comprendre que son discours pose problème, on peut l'amener à taire ce discours. C'est dans ce contexte qu'a émergé le concept de censure financière, ou *financial censorship* en anglais, que l'organisation internationale *Students for Liberty* définit comme le fait de « restreindre l'activité financière d'une entité privée, de manière à inhiber ses opérations, avec l'intention implicite de la réduire au silence [2] ». C'est aussi le sens que lui donne l'*Electronic Frontier Foundation*.

Mais les répercussions du contrôle financier ne s'arrêtent pas à l'expression et peuvent concerner l'action humaine en général. Ainsi, la censure financière peut être saisie dans un sens plus large, une signification par exemple adoptée par trois chercheurs de l'université d'État de San José qui affirment que « la censure financière se produit lorsqu'une institution financière refuse ses services à une partie en raison des opinions exprimées, des actions ou du secteur d'activité de cette partie [3] ».

Enfin, on peut comprendre la censure financière comme la restriction financière elle-même à condition qu'elle repose sur un critère subjectif externe (respect de normes arbitraires) et non pas sur une donnée économique objective, comme par exemple le paiement d'une commission. La censure peut être appliquée de manière publique (interdiction légale d'une transaction), privée (par une banque par exemple) ou les deux. Cette définition conserve toujours en elle l'idée de modeler le comportement extérieur de la personne par l'intervention sur ses finances. C'est notamment cette signification qui est donnée à la censure dans Bitcoin.

Au sens général, la censure financière consiste donc à restreindre directement l'activité financière d'une entité de façon à inhiber son expression ou son action. L'idée est d'influencer l'individu par le contrôle sur la monnaie dont il se sert, un outil qui est essentiel à sa survie économique. Aujourd'hui, la censure s'applique essentiellement au crédit bancaire, dont les transferts

sont hautement réglementés par le pouvoir. Demain, elle pourra concerner la monnaie numérique gérée par la banque centrale.

La banque et la censure

La censure financière s'exerce par la maîtrise sur le transfert de monnaie, de sorte que cette censure peut difficilement s'appliquer à l'argent liquide physique. En effet, ce dernier (qu'il prenne la forme de pièces de métal précieux ou de billets fiduciaires) permet l'échange direct et confidentiel de personne à personne, ce qui empêche la mise en place de toute restriction en dehors de quelques cas particuliers.

En revanche, dans le domaine bancaire, le client dispose d'un compte courant sur lequel la banque inscrit les crédits et gère les transferts. La restriction financière est de ce fait beaucoup plus simple : la banque peut sélectionner les transferts, geler le compte momentanément et même refuser le retrait d'argent. C'est aussi le cas de tous les services construits au-dessus du système bancaire traditionnel, comme PayPal.

C'est donc tout naturellement que l'accroissement de la censure financière a coïncidé avec la bancarisation de la société, qui a eu lieu à partir des années 1960 en Occident, et qui s'est caractérisée par la généralisation de l'usage du compte courant et des moyens de paiement apparentés comme le chèque bancaire, la carte de crédit et le virement. En quelques décennies, le paiement a migré vers le domaine bancaire, favorisé par la loi et bien plus commode à utiliser que les espèces, dont l'utilisation a elle-même été restreinte légalement. D'où la meilleure efficacité de la censure : si le liquide ne permet plus de gérer ses affaires convenablement, alors la possibilité de se retirer complètement du système bancaire n'est plus une option viable.

Cette censure a été mise en place par l'intermédiaire de la surveillance financière, qui est aujourd'hui particulièrement fréquente dans l'industrie bancaire. Les banques ont en effet l'obligation légale de surveiller leurs clients et d'intervenir dans le cas où elles constatent un comportement « suspect » de leur part, en empêchant leurs virements ou en gelant leurs comptes. Elles ne font pas cela de gaieté de cœur : elles ne procèdent pas à la surveillance de leurs clients pour les « protéger », mais pour se protéger elles-mêmes contre les éventuelles complications liées à la réglementation.

Cette réglementation s'est développée à mesure que l'activité bancaire se popularisait. À partir des années 70, le prétexte de la lutte contre le blanchiment d'argent (notamment dans le cadre de la guerre contre la drogue) s'est imposé

comme le principal prétexte derrière les restrictions imposées aux banques. Aux États-Unis notamment, la réglementation bancaire s'est particulièrement durcie suite à l'adoption du *Bank Secrecy Act* de 1970, qui se proposait de lutter contre le blanchiment d'argent.

Puis, avec l'apparition du web dans les années 1990, l'utilisation des banques internationales a demandé une réglementation accrue. Différents organismes de surveillance ont ainsi été créés. Le Groupe d'action financière (GAFI), un organisme intergouvernemental émettant régulièrement des recommandations de normes réglementaires et de sanctions économiques, a été créé en juillet 1989 dans le but de lutter contre le blanchiment d'argent. Le Financial Crimes Enforcement Network (FinCEN), le bureau du département du Trésor des États-Unis qui collecte et analyse les informations sur les transactions financières, a été formé dans ce sens le 25 avril 1990. L'équivalent français, la cellule TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins), est apparu en juillet 1990. Du côté européen, la première directive de l'Union Européenne relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux est datée du 10 juin 1990.

Enfin, après les attentats islamistes du 11 septembre 2001, un autre prétexte est apparu : la lutte contre le financement du terrorisme. Celle-ci s'est matérialisée aux États-Unis par l'adoption du *PATRIOT Act* en octobre 2001, dont le Titre 3 concerne les restrictions financières. En France, la loi du 15 novembre 2001 relative à la sécurité quotidienne a requalifié « le fait de financer une entreprise terroriste » comme un acte de terrorisme en lui-même [4]. La surveillance financière s'est renforcée en conséquence.

Ces deux évolutions forment la base de ce qu'on appelle généralement la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) en France et les normes AML/CFT (pour *Anti-Money Laundering/Combating the Financing of Terrorism*) aux États-Unis. Ce resserrement se caractérise notamment par la connaissance du client (*Know Your Customer* ou KYC), une pratique également appelée vigilance à l'égard de la clientèle, qui consiste à vérifier l'identité, la conformité et les risques liés à chaque client. Cette exigence d'identification s'est insérée dans tous les services financiers aujourd'hui.

En conséquence, le secret bancaire, c'est-à-dire l'obligation pour les banques de ne pas livrer des informations sur leurs clients à des tiers, a fini par disparaître, y compris en Suisse. L'usage d'un compte bancaire aujourd'hui présuppose la surveillance générale des transactions et l'inspection

minutieuse des opérations les moins usuelles. Ainsi, il est aujourd'hui impossible de virer une importante somme d'argent d'un compte à un autre sans devoir fournir une justification.

Cette situation du domaine financier a été résumée en janvier 2009 par Jonathan Thornburg sur la liste de diffusion en réponse à Satoshi Nakamoto qui décrivait les utilisations qu'on pouvait faire de Bitcoin :

> « Dans le monde moderne, aucun État important ne veut autoriser des transactions financières internationales intraçables au-delà d'un certain seuil relativement modeste. (Les mots d'ordre habituels incluent des expressions telles que "blanchiment de l'argent de la drogue", "évasion fiscale", et / ou "financement du terrorisme"). À cette fin, les transactions financières électroniques sont actuellement surveillées par divers États et leurs agences, et toutes les transactions, sauf les plus petites, sont désormais soumises à diverses exigences en matière d'identification pour les personnes se trouvant à chaque extrémité [5]. »

Les cas de censure financière

Au cours des dernières années, les cas célèbres de censure financière se sont multipliés, à tel point qu'il est impossible d'en faire une liste exhaustive. Nous nous contenterons d'en citer les exemples les plus manifestes en Occident, tout en gardant en tête que cette censure n'est généralement pas rendue publique par ceux qui la subissent.

L'exemple le plus connu est probablement le blocus financier contre WikiLeaks mis en place par Mastercard, Visa, Western Union, Bank of America et d'autres acteurs, en décembre 2010, dans le but de faire taire l'organisation. En octobre 2011, un communiqué de WikiLeaks a indiqué que le blocus financier avait fait disparaître 95 % de ses revenus. Cette affaire a eu des répercussions directes dans l'histoire de Bitcoin, comme nous l'avons raconté dans le chapitre 1.

Un autre cas, qui visait cette fois la profession des personnes censurées, est l'opération Choke Point mise en place entre 2013 et 2017 par le département de la Justice des États-Unis. L'opération avait pour but d'« étouffer » certains secteurs d'activité en restreignant leur accès au crédit et à d'autres services bancaires. Ces activités jugées « à haut risque » incluaient le prêt sur gages ou sur salaire, le jeu d'argent, la pornographie, l'escorting, mais aussi la vente de tabac et de produits pharmaceutiques, la vente de pièces de monnaie, les services de rencontre ou encore l'organisation des clubs de voyage. La vente d'armes et de munitions était aussi concernée : Defense Distributed,

l'entreprise du crypto-anarchiste libertarien Cody Wilson, spécialisée dans la diffusion de schémas de conception d'armes à feu fabriquées par imprimante 3D, en a fait les frais en 2015 en subissant une fermeture de ses comptes par Chase, PayPal et Stripe.

En 2018, c'est l'opinion politique qui a dû endurer la censure. De nombreuses personnalités et organisations d'*alt-right* américaine ont ainsi été bannies des divers réseaux sociaux et ont perdu l'accès à divers services financiers. L'exemple le plus emblématique était Alex Jones, fondateur du site de réinformation InfoWars, qui, outre sa purge des médias sociaux durant l'été 2018, a vu son compte PayPal être clôturé. On peut aussi citer les cas du média social Gab (chassé de PayPal, Stripe Cash App et Coinbase), de Milo Yiannopoulos (banni de PayPal pour avoir fait un salut nazi) ou encore de Robert Spencer (chroniqueur du blog anti-islam Jihad Watch, chassé de Patreon suite à la pression de Mastercard). En France, cette censure s'est manifestée à l'encontre d'Égalité et Réconciliation, l'association de l'antisioniste Alain Soral, qui a été exclue de PayPal en août 2018, dans le cadre d'une purge similaire à celle des militants américains. L'association a également vu plusieurs de ses comptes bancaires (Banque postale, BNP Paribas, Banque populaire) être fermés au cours des années.

Toujours dans le domaine politique, mais en Chine cette fois-ci, on peut citer le cas du mouvement contre l'amendement de la loi d'extradition par le gouvernement de Hong Kong, série de manifestations ayant eu lieu entre mars 2019 et juillet 2020, qui a dû subir les interventions du conglomérat bancaire international HSBC, probablement sous pression de l'État central chinois. En novembre 2019, la filiale de Hong Kong a en effet décidé de fermer un compte utilisé pour soutenir le mouvement de protestation. Puis, elle a gelé le compte du démocrate Ted Hui en décembre 2020. Par ailleurs, on a appris en 2023 qu'elle refusait aux Hongkongais ayant fui au Royaume-Uni d'accéder légitimement à leurs fonds de pension, pour un montant s'élevant à 2,2 milliards de livres sterling.

Plus récemment, la pandémie de Covid-19 a fourni d'autres occurrences de censure financière. De nombreux activistes opposés aux mesures coercitives comme le confinement, le port du masque et la vaccination obligatoire, ont ainsi été largement censurés, généralement accusés de propager la désinformation. Le groupe d'action néerlandais Viruswaarheid – s'opposant à la distanciation sociale, au confinement, au couvre-feu et au programme de vaccination – a ainsi vu son compte bancaire utilisé pour recevoir des donations être fermé par ING Bank en février 2021.

Mais l'exemple qui ressort du lot est le mouvement canadien du « Convoi de la liberté » de février 2022, initié par les camionneurs qui s'opposaient à l'obligation vaccinale imposée pour entrer sur le territoire par voie terrestre et qui ont manifesté leur mécontentement en faisant route jusqu'à Ottawa pour occuper la ville. Ce mouvement a fait face à une censure financière drastique. Il a dans un premier temps été victime des plateformes de financement participatif, qui ont annulé ses différentes campagnes qui avaient pour objectif de payer le déplacement des camionneurs : celle de GoFundMe, ayant réuni 10 millions de dollars canadiens, a été retirée le 4 février ; tandis que les fonds récupérés par les campagnes organisées sur la plateforme chrétienne GiveSendGo (9 millions de dollars environ) ont été gelés par le gouvernement ontarien, et n'ont pas pu être distribués. La répression financière s'est considérablement amplifiée lorsque, suite à l'entrée en vigueur de l'état d'urgence déclaré par Justin Trudeau le 14 février, le gouvernement canadien a décidé de geler des comptes bancaires personnels ou professionnels en lien avec le mouvement : 280 comptes contenant 8 millions de dollars au total ont été gelés de la sorte. L'année suivante, le juge Paul Rouleau, chargé de la Commission sur l'état d'urgence, a déclaré que le gel des comptes bancaires était un « outil puissant pour décourager la participation [aux manifestations] et inciter les manifestants à abandonner[6] ».

Un autre évènement important survenu durant le mois de février est le durcissement des sanctions économiques mises en place par les États occidentaux contre la Russie, suite à son invasion de l'Ukraine. Les sanctions financières incluaient l'exclusion de certaines banques russes du système SWIFT, la prohibition du financement en Russie et de l'achat de roubles, et l'interdiction de la fourniture de services de portefeuille, de compte ou de conservation de crypto-actifs. De manière générale, les virements vers la Russie ont été interdits, de sorte que les citoyens russes exilés ne pouvaient plus envoyer d'argent à leur famille. C'est aussi le cas des ressortissants ukrainiens dont les proches sont restés sur le territoire occupé par l'armée russe, comme cette Ukrainienne réfugiée en France qui ne pouvait pas envoyer un virement bancaire de 100 euros à ses parents à Donetsk.

Du côté occidental, des mesures financières ont également été prises dans le but de faire respecter la censure des médias financés par le Kremlin. En janvier 2023, la chaîne d'information RT France, qui était déjà interdite de diffusion en Europe, mais qui continuait d'être accessible sur Internet, a ainsi subi le gel de ses avoirs, ce qui l'a contrainte à fermer définitivement.

Enfin, pour finir à propos des différentes occurrences de censure finan-

cière, on ne peut pas ne pas évoquer les activités liées aux cryptomonnaies, qui ont subi et continuent de subir des restrictions de la part des organismes financiers. L'achat de cryptomonnaies est entravé par les banques qui interdisent régulièrement à leurs clients (toujours en prétendant les « protéger ») d'envoyer des fonds vers les plateformes de change. De plus, les entreprises du secteur peinent régulièrement à ouvrir un compte bancaire en raison de la méfiance des acteurs traditionnels [7].

La censure financière est donc de plus en plus fréquente dans notre société. Elle touche de nombreuses personnes de bords politiques opposés, de nationalités diverses et de professions variées. Elle s'exerce bien souvent sans décision juridique spécifique, ce qui donne un caractère ésotérique, caché, arbitraire à l'application du pouvoir réel. C'est ce qui en fait un problème subtil et difficile à expliciter.

L'intervention plus prononcée de cette censure a pour effet de pousser les gens à s'intéresser à Bitcoin. En effet, l'expérience d'une telle restriction provoque nécessairement le désir de trouver un moyen de la contourner, quand bien même celle-ci serait légère. Lorsqu'une personne prend pleinement conscience de la censure comme une réalité concrète et non plus comme un risque abstrait, elle ressent le besoin de s'en libérer et de se prémunir de ce danger, ce qui lui démontre (ou lui confirme) la proposition de valeur de Bitcoin [8]. C'est le cas de l'auteur de cet ouvrage qui a vu son compte bancaire être gelé sans préavis, sans que la banque ne mentionne la raison derrière cette suspension, et qui n'a pu récupérer ses fonds que six mois plus tard.

Censure et monnaie numérique de banque centrale

La tendance est donc claire : avec l'utilisation intensive des comptes bancaires en lieu et place des espèces, le pouvoir de censure financière est devenu de plus en plus important. Ainsi, même si cette censure reste aujourd'hui occasionnelle, nous pouvons nous attendre à ce qu'elle constitue un problème grandissant à l'avenir. Plus précisément, elle pourrait devenir une contrainte générale dans les décennies à venir avec le déploiement progressif des monnaies numériques de banque centrale (MNBC) et la disparition conjointe de l'argent liquide.

Tel que nous l'avons vu dans la section dédiée à la monnaie numérique de banque centrale dans le chapitre 4, la numérisation de la monnaie constitue la prochaine étape dans l'évolution de la monnaie étatique. Depuis 2016, les banques centrales autour du monde s'efforcent de concevoir des systèmes qui

pourraient être utilisés par le grand public et les communications à ce sujet se multiplient depuis 2020.

Une telle monnaie numérique permettrait de récupérer un revenu de seigneuriage supplémentaire en supprimant le coût de la production de l'argent liquide remplacé et en reprenant une part de l'activité monétaire qui a lieu aujourd'hui par l'intermédiaire du crédit émis par les banques commerciales. Mais elle permettrait aussi (ce qui nous intéresse ici) d'exercer un contrôle financier total sur les transactions des citoyens en centralisant la gestion du système entre les mains de la banque centrale et des organismes agréés.

Ce contrôle s'accompagnerait bien entendu d'une surveillance financière accrue, qui serait justifiée par les mêmes prétextes utilisés aujourd'hui, comme la lutte contre le blanchiment d'argent et le financement du terrorisme. Ceci pourrait conduire à l'instauration d'un système panoptique, où la surveillance se ferait à l'insu du surveillé. Les banques centrales nient vouloir aller dans cette direction, mais le fait est qu'elles ne rendront jamais leurs systèmes strictement confidentiels, réservant toujours un droit de regard aux autorités compétentes.

Cette surveillance financière pourrait être affermie par la disparition progressive de l'argent liquide, qui a déjà commencé à certains endroits du monde. C'est le cas de la Suède, où la question de la fin des espèces est déjà discutée et où l'État fait tout pour mettre à disposition des moyens de paiement numérique innovants. C'est aussi le cas de la Chine, où l'essentiel des transferts se fait par l'intermédiaire de systèmes de paiement mobile comme WeChat Pay et Alipay. Ce n'est pas un hasard si ces deux pays ont été les premiers à envisager sérieusement de développer une monnaie numérique.

La guerre contre l'argent liquide sévit déjà dans certains pays par le biais de la démonétisation de certains billets en circulation, qui peuvent être échangés contre d'autres billets ou être déposés sur un compte bancaire, à condition d'attester de la provenance des fonds. En Inde en novembre 2016, le gouvernement de Narendra Modi a ainsi démonétisé les billets de 500 et 1 000 roupies, équivalant à 7,5 et 15 $, et représentant à eux seuls 86 % de la monnaie en circulation, dans le but affiché de lutter contre la contrefaçon de faux billets, l'évasion fiscale et l'économie informelle. Au Nigéria, début 2023, le gouvernement a tenté (sans grand succès) d'appliquer une mesure similaire, par la limitation des retraits et la démonétisation des grosses coupures, dans le but de contrôler l'inflation, de lutter contre la contrefaçon et de promouvoir le naïra électronique (eNaira) lancé par la banque centrale en octobre 2021. Cette pratique de la démonétisation n'est cependant pas nouvelle puisqu'elle

avait été utilisée en Europe après la Seconde Guerre mondiale pour enrayer les effets inflationnistes du faux-monnayage et pour détruire les profits du marché noir, ce qui avait fait d'ailleurs dire au personnage du Dabe dans *Le cave se rebiffe* qu'« en matière de monnaie, les États ont tous les droits et les particuliers aucun ! ».

Une fois la monnaie numérique en place et l'argent liquide largement limité, les gens respectueux de la loi n'auraient d'autre choix que d'utiliser ce système surveillé. Le système pourrait limiter le montant que les gens dépensent, ce pour quoi ils l'utilisent et avec qui ils commercent. De plus, en tant que système informatique, il pourrait être facilement programmé de façon à imposer des conditions de dépense pour chaque montant de monnaie possédé par l'utilisateur. Une telle programmabilité permettrait aux autorités en charge d'orienter le comportement politique, économique et moral des individus dans le sens désiré, ce qui donnerait à la censure financière une portée jamais vue auparavant.

Au niveau économique d'abord, cela permettrait d'améliorer ce que les banquiers centraux appellent la transmission de la politique monétaire, c'est-à-dire le processus par lequel les décisions de politique monétaire affectent l'économie en général et le niveau des prix en particulier. Aujourd'hui cette transmission est essentiellement assurée par la modification des taux d'intérêt directeurs. Demain, elle pourrait se faire par la programmation de la monnaie. Cela permettrait notamment de transformer le système d'aides sociales en un système de subvention directe exigeant la dépense rapide dans un secteur économique précis, dans le but de le stimuler.

Ensuite au niveau moral, cette programmabilité permettrait d'orienter massivement les paroles et les actions des gens dans un sens déterminé, dans la droite lignée des censeurs de la Rome antique. Dans notre société moderne, cela pourrait être fait dans le cadre de la lutte contre le changement climatique, en récompensant le comportement « écologique », tel que la location d'un vélo pour se déplacer, et en punissant l'attitude « pollueuse », telle que la consommation de viande. Cette possibilité fait ainsi entrevoir l'instauration d'un système de crédit social à la chinoise.

Enfin d'un point de vue politique, ce système permettrait de réduire l'opposition au pouvoir en sanctionnant ceux qui pensent mal, ceux qui s'expriment trop, ceux qui manifestent contre, etc. Le pouvoir politique pourrait raffermir sa position en appliquant les interventions, non plus de manière publique et légale (conformément à l'idée d'état de droit au sens de *Rechtsstaat*), mais de façon cachée et discrétionnaire. Cela pourrait constituer les prémices d'un

régime totalitaire où l'État saurait tout, contrôlerait tout, et où il n'y aurait plus besoin de lois formelles. La MNBC serait un outil puissant de surveillance financière de masse, pouvant œuvrer à la réalisation d'un avenir orwellien dans lequel les individus n'auraient plus aucune vie privée et dont le pouvoir de résistance à l'autorité serait réduit au minimum.

Cette censure financière aurait lieu à une échelle jamais vue auparavant. Par conséquent, il serait difficile de la mettre en place par une gestion manuelle des êtres humains. C'est pour cette raison qu'elle serait probablement déléguée à un algorithme doté d'une intelligence artificielle, qui détecterait les mauvais paiements et les bloquerait instantanément. Le système de MNBC pourrait ainsi nous mener à une situation qui rappellerait celle décrite par saint Jean dans son Apocalypse :

> « Par ses manœuvres, tous, petits et grands, riches ou pauvres, libres et esclaves, se feront marquer sur la main droite et sur le front, et nul ne pourra rien acheter ni vendre s'il n'est pas marqué au nom de la Bête ou au chiffre de son nom [9]. »

Dans ce monde dystopique dont nous pouvons à peine imaginer les ramifications, l'espoir serait représenté par Bitcoin, dont la promesse fondamentale est d'échapper à de telles interventions. Par sa résistance à la censure, Bitcoin constituerait ainsi un oasis de liberté dans le désert de la servitude généralisée. Il serait, en substance, le dernier recours pour une population qui aurait sombré dans l'asservissement par la technique.

La censure dans Bitcoin

Pour bien comprendre comment Bitcoin s'oppose à la censure, il est nécessaire de comprendre comment cette dernière peut s'exercer sur la chaîne. En effet, si le modèle de Nakamoto est réputé *résistant* à la censure, ceci ne signifie pas pour autant qu'il est « incensurable ». La censure dans Bitcoin est non seulement possible, mais elle est aussi probable au-delà d'un certain stade d'adoption.

Lorsqu'on parle de Bitcoin, le terme de censure possède un sens précis : il désigne l'action d'empêcher une transaction d'être réalisée sur une base économiquement irrationnelle, en entravant son inscription pérenne dans la chaîne de blocs. Cette définition rejoint l'idée de restreindre l'activité financière d'une entité dans le but de modeler son comportement. En un sens, cette censure ressemble également à de la censure du discours, car il s'agit d'empêcher indirectement l'individu d'écrire une transaction signée dans un registre.

La façon dont peut s'exercer la censure dans Bitcoin peut être extrapolée à partir de ce qui existe déjà dans le monde bancaire et dans le secteur des cryptomonnaies, à commencer par les prétextes utilisés pour la défendre. D'une part, les justifications utilisées dans la finance traditionnelle sont largement applicables à Bitcoin, comme la lutte contre le blanchiment d'argent, le financement du terrorisme et la protection des épargnants : la cryptomonnaie permet en effet d'éviter l'impôt, de financer tous les projets imaginables et de participer à des escroqueries. D'autre part, de nouveaux prétextes émergent comme la dévaluation de la monnaie locale (un instrument déflationniste représente une concurrence déloyale) ou la lutte contre le changement climatique (le minage émet du CO_2).

De ces prétextes, les autorités tirent des réglementations générales qui s'appliquent à l'échelle internationale, comme c'est déjà le cas dans le système bancaire mondial. Les différentes juridictions se basent sur les recommandations du GAFI, dont le rôle premier est la lutte contre le blanchiment d'argent et le financement du terrorisme. Comme nous l'avons expliqué en parlant de l'arbitrage juridictionnel (voir chapitre 4), elles sont fortement poussées à appliquer ces recommandations sous peine de subir les sanctions économiques des États-membres. Le FMI peut également être mis à profit, celui-ci ayant pour but d'assurer la stabilité du système monétaire mondial (donc de protéger les monnaies des États-membres).

Cette coopération permet de constituer des listes noires d'adresses ne rentrant pas en conformité avec les réglementations, listes qui sont distribuées aux divers acteurs financiers réglementés. On peut citer par exemple la liste dressée par l'*Office of Foreign Assets Control* (OFAC), l'organisme dépendant du Trésor étasunien en charge d'appliquer les sanctions internationales des États-Unis dans le domaine financier, qui fait autorité dans le domaine financier en raison de l'extraterritorialité du droit étasunien.

La censure s'applique ainsi déjà dans une partie de l'économie basée sur Bitcoin. Tous les acteurs qui se conforment aux réglementations bloquent les bitcoins (et autres cryptomonnaies) provenant des adresses présentes sur les listes noires et gèlent les comptes de l'utilisateur jusqu'à ce qu'il se justifie. Toutefois, cette pratique conserve un caractère partiel et implicite : les transactions en elles-mêmes ne sont pas encore explicitement interdites, mais les fonds ne doivent pas être envoyés aux intermédiaires financiers réglementés, comme les plateformes de change ou les processeurs de paiement. Cette situation pousse certaines plateformes à faire beaucoup de zèle dans le domaine en refusant des bitcoins provenant de mélanges de pièces et geler les comptes

des personnes le faisant, en l'absence d'une réglementation explicite [10].

La réglementation peut également s'étendre à l'industrie du minage. L'activité minière tend naturellement à se centraliser, par l'agrégation de la puissance de hachage en fermes de minage, par le rassemblement des hacheurs en coopératives minières et par l'utilisation de relais de communication par ces coopératives. Ces gros acteurs sont généralement identifiables et se soumettent donc plus facilement aux réglementations concernant les transactions à traiter. C'est ce qui pourrait amener une censure sur le réseau.

Les mineurs peuvent dans un premier temps pratiquer une censure passive en refusant systématiquement de confirmer des transactions, pour des raisons économiquement irrationnelles, typiquement sous la pression du régulateur. Ce type de censure a notamment été envisagé par la coopérative du groupe Marathon, qui avait déclaré en 2021 vouloir pratiquer le « minage de blocs propres [11] », avant de se rétracter sous la pression populaire. Ce filtrage est mis en place sur Ethereum avec les validateurs qui utilisent des relais d'optimisation de MEV qui respectent les normes de l'OFAC et par conséquent n'incluent pas les transactions considérées comme sales [12]. Les participants à ces relais étaient principalement des plateformes de change en 2023.

Cette censure passive n'est pas très problématique car elle demande que 100 % de la puissance de calcul s'y conforme pour être effective. Les mineurs dissidents, c'est-à-dire ceux qui ignorent délibérément les réglementations, débloquent la situation en validant les transactions ignorées par les autres. Seuls les délais de confirmation sont affectés.

Cependant, cette situation peut devenir autrement plus grave si les mineurs conformistes, à savoir les mineurs suivant méticuleusement les réglementations, commencent à refuser les blocs contenant les transactions « sales ». C'est ce que nous appelons ici la censure active, qui consiste à empêcher des transactions d'être confirmées en rendant orphelins tous les blocs qui les contiennent. Pour être maintenue dans le temps de manière certaine, elle nécessite de disposer de la majorité de la puissance de calcul du réseau : il s'agit donc d'une attaque des 51 %. Les branches faibles formées par l'attaque de censure sont mises de côté en vertu du principe de la chaîne la plus longue, comme illustré sur la figure 9.1.

Le coût d'une telle attaque peut être colossal suivant la puissance de calcul déployée sur le réseau [13]. Mais ce coût serait justifié par le développement des activités illégales évitant l'impôt et le seigneuriage. En effet, comme montré dans le chapitre 4, le profil-type de l'attaquant est l'État dont le pouvoir de prélèvement repose grandement sur son contrôle de la monnaie : c'est pourquoi

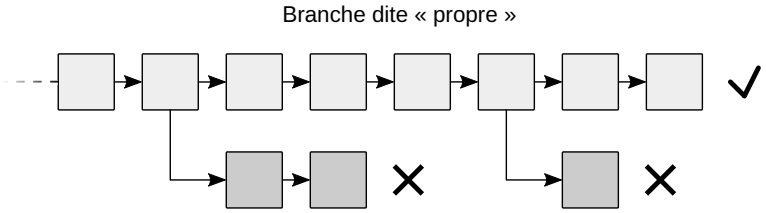

FIGURE 9.1 – Attaque de censure active.

il se moque de réduire (voire de détruire) l'utilité de Bitcoin ce faisant.

Cette attaque hypothétique serait précédée d'une déclaration de guerre contre Bitcoin. Toute la tolérance vis-à-vis des utilisateurs disparaîtrait, et ce qui n'était pas officiel le deviendrait : toutes les transactions qui ne sont pas explicitement autorisées seraient déclarées interdites. L'utilisation libre serait criminalisée d'une manière ou d'une autre, et le minage honnête aussi.

Ce durcissement permettrait de coopter plus largement les regroupements miniers auxquels les directives étatiques seraient transmises. L'État pourrait aussi réquisitionner ou acheter son propre matériel de hachage. En somme, il disposerait à un moment donné d'une puissance de calcul majoritaire. Une fois la puissance de calcul rassemblée, l'attaque serait mise à exécution.

La censure active est insidieuse car il suffit que 51 % l'applique pour qu'elle continue. Son prolongement dans le temps peut finir par constituer une nouvelle normalité. Par conséquent, les mineurs économiquement rationnels ont tout intérêt à appliquer la censure, comme l'a montré un article de Juraj Bednar sur le sujet [14]. L'attaquant ne doit donc pas nécessairement disposer en permanence de la majorité du taux de hachage.

La confidentialité n'empêche pas la censure d'avoir lieu, mais la rend simplement plus coûteuse. Dans le cas où l'intégralité des utilisateurs refuserait de se conformer aux normes de surveillance, les censeurs devraient refuser l'ensemble des transactions et ne pas recevoir les frais correspondants. L'attaque prendrait alors la forme d'une destruction totale de l'utilité de la chaîne par le minage de blocs vides, c'est-à-dire une attaque Goldfinger. Le nom de cette dernière fait référence au principal antagoniste du film de James Bond éponyme sorti en 1964, qui souhaitait irradier le stock d'or américain sécurisé au dépôt de Fort Knox dans le but de le rendre durablement inutilisable et d'augmenter la valeur du reste de l'or [15].

De ce fait, il est tout à fait possible d'exercer de la censure dans Bitcoin.

Toutefois, ce n'est ni facile, ni définitif, car il existe un mécanisme au sein du protocole permettant de lutter contre ce type d'attaque : la résistance à la censure.

Le mécanisme de résistance à la censure

La résistance à la censure désigne la difficulté à entraver arbitrairement les transactions. Elle est couramment citée comme l'une des deux grandes promesses de Bitcoin : permettre à quiconque d'envoyer des fonds à n'importe qui d'autre, quel que soit le moment, où que se trouve le destinataire dans le monde, pourvu qu'il dispose d'un accès à Internet.

La résistance à la censure constitue un élément essentiel de Bitcoin. Si elle n'existait pas, le système ne pourrait tout simplement pas survivre en tant que tel : il deviendrait un système contrôlé centralement par une autorité décidant des bonnes et des mauvaises transactions. Il devrait s'adapter, tel GoldMoney ou PayPal, ou périr, à l'instar de e-gold ou de Liberty Reserve. De plus, le pouvoir absolu sur la sélection des transactions permettrait à cette autorité d'exercer *de facto* une influence irrésistible sur le protocole par le biais de l'application de soft forks (comme nous le verrons dans les chapitres 10 et 11), ce qui mènerait *in fine* à la destruction de la politique monétaire originelle. Sans résistance à la censure, la proposition de valeur de Bitcoin s'effondrerait.

Cependant, cette résistance n'a jamais été décrite explicitement par Satoshi Nakamoto. Dans ses interventions, le père de Bitcoin a expliqué comment son système était sécurisé économiquement contre la double dépense, ce qui était déjà une grande évolution par rapport aux modèles décentralisés précédents. Mais il n'a en revanche pas indiqué comment le système pouvait s'opposer à la censure, c'est-à-dire au blocage partiel ou total de l'activité transactionnelle par une entité hostile. Il semblait se reposer sur la bonne volonté des mineurs « honnêtes », pensant même qu'il y aurait « probablement toujours des nœuds prêts à traiter les transactions gratuitement [16] », cette résistance allant de soi.

Le mécanisme de résistance à la censure de Bitcoin a été mis en lumière en 2018, par le développeur et auteur Eric Voskuil, qui a montré qu'il reposait de manière essentielle sur les frais de transaction [17]. Comme dans le cas de la résistance à la double dépense, la propriété de résistance à la censure n'est pas absolue mais économique : c'est une régulation financée par les frais des transactions prohibées.

La sécurité minière, on le rappelle, repose sur un principe majoritaire : la quantité de puissance de calcul contrôlée par les mineurs honnêtes doit

être supérieure par rapport à celle des attaquants. L'important n'est pas que le taux de hachage de Bitcoin soit le plus haut possible ; c'est que les mineurs disposant d'une puissance de calcul non négligeable soient prêts à miner systématiquement toutes les transactions payant un montant correct de frais et à toujours construire leurs blocs à partir de la plus longue chaîne.

Ainsi, cette sécurité ne dépend pas uniquement de la puissance de calcul. Elle est aussi fonction de la distribution de cette puissance de calcul et de la fraction de mineurs par rapport au reste de l'humanité [18]. En effet, un taux de hachage qui serait concentré dans les mains d'un seul mineur créerait une sécurité équivalente à celle d'un système centralisé, dépendante du mineur en question. Aussi, un réseau équitablement distribué et déployant une grande quantité de puissance de calcul aura plus de risque d'être coopté s'il comporte un petit nombre de mineurs que s'il en comporte un grand nombre.

La solution au problème de la censure provient des mineurs dissidents, qui sont prêts à confirmer des transactions litigieuses ou décrétées comme illégales par le pouvoir. Le risque pris par ces mineurs doit alors être compensé économiquement.

Le mineur dissident a besoin de rester anonyme afin de pouvoir miner dans la clandestinité. Cette possibilité est assurée par le fait que les mineurs ne sont jamais contraints de s'identifier au sein du protocole. Le signalement des blocs minés par les coopératives minières est en effet une démarche purement optionnelle et volontaire, ayant pour but de rassurer les utilisateurs (leurs clients) sur la distribution du système.

La part du revenu du minage provenant de la création monétaire joue un rôle accessoire dans la lutte contre la censure, que cette dernière soit passive ou active. D'une part, cette partie de la récompense est la même pour tous les mineurs, ce qui fait qu'elle n'influe pas sur leur choix économique d'inclure une transaction ou non dans un bloc. D'autre part, la potentielle chute de l'utilité (et donc du revenu de minage) du système provoquée par une censure active (attaque), ne saurait empêcher l'autorité à l'origine d'arriver à ses fins. Les motivations de cette dernière sont en effet particulières : elle ne cherche pas à réaliser un profit direct mais à contrôler, voire détruire, le système en décrétant quelles transactions sont autorisées et lesquelles ne le sont pas.

En revanche, les frais de transaction sont, eux, essentiels au mécanisme de résistance à la censure. Par leur intégration dans le protocole, ces commissions sont chacune associées publiquement à une transaction. Ainsi, les frais luttent d'une part contre la censure passive en incitant les mineurs à confirmer les transactions, et découragent d'autre part la censure active en donnant à la

branche censurée une importance économique plus grande.

Dans le cas d'une attaque de censure active, les censeurs acquièrent plus de la moitié de la puissance de calcul du réseau et rejettent ouvertement un groupe de transactions défini (par une liste noire par exemple) en refusant les blocs qui contiendrait l'une d'entre elles. La chaîne des censeurs est considérée par les nœuds honnêtes comme la chaîne correcte car elle est plus longue.

C'est dans ce contexte que le mécanisme des frais intervient. Les initiateurs des transactions censurées, voyant que leurs transactions ne sont pas confirmées, augmentent leurs commissions. C'est un comportement naturel que l'on observe déjà lors des périodes de congestion du réseau, comme au sommet de la bulle de 2017, lorsque les frais médians par transaction ont dépassé les 30 $. En outre, il est logique de payer une grande quantité de frais pour transférer de fortes sommes, celles-ci étant plus à risque que les petits transferts [19].

Cette augmentation crée un supplément de frais, qui constitue la différence entre les frais de toutes les transactions et ceux des transactions non autorisées qui se retrouvent dans les mempools des nœuds honnêtes. C'est ce supplément (et ce supplément uniquement) qui incite les mineurs dissidents à déployer plus de puissance de calcul au cours du temps : plus l'économie supprimée est importante, plus le différentiel de puissance de calcul résultant est grand.

Les mineurs dissidents se coordonnent en privé ou par la voie d'un signalement pour planifier une riposte. Une fois que la puissance de calcul est jugée suffisante, ils se mettent à confirmer les transactions censurées. Puisque leur puissance de calcul est majoritaire, leur chaîne devient la plus longue et la chaîne des censeurs est invalidée. De cette manière, la censure est vaincue, du moins jusqu'à une nouvelle offensive de l'ennemi.

Ainsi, le mécanisme de résistance à la censure est ancré profondément dans le protocole. La preuve de travail, le caractère anonyme du minage, le système de frais intégré : ce sont autant d'éléments permettant de coordonner un marché des frais afin de repousser les censeurs. Il est impossible d'estimer quelle serait la part de l'économie censurée, l'envergure de l'attaque étatique ou le montant de frais que les utilisateurs seraient prêts à payer, de sorte qu'on ne peut pas garantir l'incensurabilité de Bitcoin. Mais le mécanisme n'en est pas moins fonctionnel.

Il est à noter que le rôle des frais de transaction, explicité en 2018 par Eric Voskuil, a été négligé par certains protocoles cryptoéconomiques. C'est en particulier le cas d'Ethereum qui a fait le choix de brûler une partie des frais du réseau dans le but de rendre l'éther déflationniste au sens monétaire avec

l'activation de l'EIP-1559 en août 2021. La communauté d'Ethereum a également choisi de passer en preuve d'enjeu en septembre 2022, ce qui constitue un autre pas vers l'acceptation de la censure comme nous l'expliquerons plus bas.

L'importance de la confidentialité

La censure financière est étroitement apparentée à la surveillance des transactions. Cette dernière permet en effet d'affiner la sélection des transferts et d'exercer un pouvoir subtil sur l'économie, sans brusquer les personnes les plus dociles. La chose vaut pour le monde bancaire comme nous l'avons constaté, mais elle vaut aussi pour Bitcoin.

Il existe deux manières de protéger sa richesse et sa liberté : par la force physique et par la dissimulation. La première méthode consiste à se prémunir contre le vol directement en défendant soi-même ses biens (si besoin à l'aide d'une arme à feu), ou bien indirectement par le recours aux services de police étatiques ou aux services de protection privés (gardes du corps, quartiers sécurisés, agence de protection), très prisés des personnes très fortunées. Cette méthode est importante et utile contre les criminels communs, mais elle est relativement inefficace contre la puissance dominante locale dont nous sommes à la merci – l'État.

C'est pourquoi les individus ont plus souvent recours à la seconde méthode, qui consiste à dissimuler leur richesse pour ne pas qu'autrui en ait connaissance et puisse s'en emparer directement. Cela permet de dissuader le voleur usant la menace de violence d'aller plus loin : il pourrait nous interroger pour savoir où se trouve notre richesse, mais cette action représenterait un coût supplémentaire (proportionnel à notre refus de lui livrer cette information) qui freinerait sa recherche.

Cette méthode est directement liée à la confidentialité (aussi appelée *privacy* ou protection de la vie privée) qui est le fait de réserver des informations à un petit nombre de personnes déterminées. La confidentialité est distincte du secret dans le sens où la personne peut choisir de révéler sélectivement des informations (confidence). Dans le contexte financier, il s'agit généralement de faire en sorte que les détails d'une transaction ne soient connus que des participants.

La confidentialité forme la base de la liberté individuelle dans la société et constitue une caractéristique essentielle pour tout le monde. Elle sert en effet à *créer une asymétrie* entre le faible et le fort, entre l'individu et l'État, de sorte que ce dernier ne puisse pas empiéter absolument sur les droits du premier.

L'État veut vous persuader du contraire, en vous disant que vous n'avez rien à craindre si vous n'avez rien à cacher [20], mais il n'y a rien d'historiquement plus faux, comme l'ont montré les exemples des totalitarismes du xx^e siècle.

De ce fait, puisque la censure financière est issue de l'initiative étatique, la résistance à la censure est en général intrinsèquement liée à la confidentialité.

D'une part, la résistance à la censure de l'utilisateur individuel repose sur la confidentialité du système. Si l'État connaît toutes les transactions, il peut sanctionner l'utilisateur pour avoir effectué une transaction non autorisée, quand bien même celle-ci serait confirmée par le réseau. Certains promoteurs de BTC mettent en avant la transparence du protocole, en la présentant comme un avantage par rapport aux systèmes bancaires opaques, en insistant sur le pseudonymat et en réservant la propriété d'anonymat aux « cryptomonnaies confidentielles » comme Monero. Mais il s'agit d'une mécompréhension du rôle de cette transparence : les données dans Bitcoin sont publiques dans le but unique d'assurer le consensus et l'audit, et Monero ne fait qu'implémenter un compromis différent sur le degré de transparence des transactions.

D'autre part, la confidentialité de l'utilisateur dépend de la résistance à la censure du système. En effet, si l'État dispose d'un contrôle total sur la sélection des transactions, alors il peut choisir de ne confirmer que les transactions qui dévoilent l'identité de l'expéditeur et celle du destinataire. Cette dépendance est souvent remise en question par certains partisans de Monero qui estiment que la confidentialité par défaut du système protège les utilisateurs de la censure, considérant que l'État ne peut pas censurer une transaction qu'il ne connaît pas. Néanmoins, cette vision est plutôt naïve car les utilisateurs ont la possibilité technique de révéler les informations relatives à leurs adresses aux organismes de surveillance [21] ; la seule barrière à cela est le coût supplémentaire qu'une telle surveillance représente.

La confidentialité et la résistance à la censure sont donc interdépendantes dans Bitcoin. Sans confidentialité, il n'y a pas de résistance à la censure individuelle ; et sans résistance à la censure, il n'y a pas de confidentialité individuelle. C'est pour cette raison que la surveillance généralisée, loin d'être anodine, constitue un problème majeur.

La surveillance s'est étendue dans Bitcoin au cours de son développement économique par la réglementation des intermédiaires financiers. Les plateformes de change entre monnaies traditionnelles et cryptomonnaies ont été progressivement contraintes d'appliquer des normes de connaissance du client (KYC) et de lutte contre le blanchiment (AML) similaires au système bancaire classique. Cette récupération d'informations s'est accompagnée de

l'émergence de sociétés d'analyses de chaîne, telles que Chainalysis ou CipherTrace, qui croisent les données d'identification avec les évènements de la chaîne de blocs de façon à en dégager une interprétation probable, et qui fournissent les résultats à leurs clients qui sont les agences étatiques, les institutions financières et les grandes entreprises du domaine. En outre, l'étau est encore en train de se resserrer, avec l'apparition d'une version modifiée de la « règle du voyage » (*Travel Rule*), recommandée par le GAFI et déjà imposée par la FINMA suisse, qui consiste pour un intermédiaire à vérifier systématiquement l'adresse de retrait du client [22].

Cette évolution crée une réelle menace sur Bitcoin en général. C'est pourquoi il se forme en face une résistance visant à déjouer la surveillance, notamment par l'intermédiaire de techniques d'amélioration de la confidentialité. C'est le cas par exemple du mélange de pièces, ou CoinJoin, qui permet de brouiller les pistes. C'est aussi le cas des méthodes intégrées dans Monero. Nous développerons cet aspect dans le chapitre 12.

Ainsi, la confidentialité est essentielle pour préserver sa richesse et son autonomie. On ne peut pas être réellement libre sans protéger sa vie privée. Comme l'écrivait le fabuliste Florian : « Pour vivre heureux vivons cachés [23]. »

Les interventions humaines dans le consensus

La possibilité de censure dans Bitcoin provoque généralement une volonté de trouver une solution, s'inscrivant dans la démarche d'ingénieur qui caractérise les amateurs de cryptomonnaie. Beaucoup de personnes sont en effet séduites par une alternative à la régulation par les frais : l'intervention humaine directe sur la chaîne. Celle-ci consiste à recourir au « consensus social », c'est-à-dire au mécanisme de détermination du protocole. Deux idées de ce type semblent avoir un certain succès : l'UASF anti-censure et l'UAHF de changement de preuve de travail. Il s'agit cependant d'une tentation dangereuse comme nous allons essayer de le montrer.

La première idée est de rejeter la censure en invalidant la branche des censeurs partiellement ou totalement, c'est-à-dire en portant atteinte au principe de la chaîne la plus longue. Le rejet peut se faire en rendant les blocs de la chaîne des censeurs invalides ou en imposant la validité de la chaîne concurrente par un point de contrôle temporaire. Une telle mesure constitue un soft fork (à savoir une restriction des règles de consensus) et doit être activée par les utilisateurs à un horodatage ou à une hauteur de bloc donné, d'où le fait qu'on la désigne comme un *User Activated Soft Fork* (UASF). Elle provoque une scission car elle n'est pas, dans le cas précis de la censure, soutenue par

la majorité de la puissance de calcul.

L'idée d'invalider la censure par consensus social était déjà évoquée par Vitalik Buterin en 2016 dans le cas de la preuve d'enjeu :

> « *Sur des échelles de temps moyennes à longues, les humains sont assez bons pour le consensus.* Même si un attaquant avait accès à une puissance de hachage illimitée, et qu'il parvenait à réaliser une attaque des 51 % contre une chaîne de blocs majeure en inversant ne serait-ce que le dernier mois d'histoire, il aurait beaucoup plus de mal à convaincre la communauté de la légitimité de la nouvelle chaîne. Il faudrait qu'il subvertisse les explorateurs de blocs, tous les membres de confiance de la communauté, le New York Times, archive.org et de nombreuses autres sources sur Internet ; en somme, qu'il convainque le monde que sa nouvelle chaîne est celle qui est apparue en premier [...]. *Ces considérations sociales sont ce qui protège finalement toute chaîne de blocs à long terme*, que la communauté de cette chaîne de blocs l'admette ou non (notez que Bitcoin Core admet cette primauté de la couche sociale) [24]. »

Cette mesure peut être mise en place par une invalidation directe mais celle-ci n'est facile à implémenter que si les censeurs marquent leurs blocs d'une manière ou d'une autre. Cela a été réalisé par Bitcoin ABC le 1er décembre 2020 sur sa chaîne nouvellement créée pour contrer la censure active d'un mineur mécontent de la scission avec Bitcoin Cash [25].

Il est aussi possible d'inclure un point de contrôle (*checkpoint*) dans le protocole. Un point de contrôle est un bloc considéré comme valide par défaut. Ce mécanisme a été implémenté dans le logiciel de Bitcoin dès juillet 2010 dans le but d'éviter une recoordination de chaîne et certains de ces points de contrôle sont encore présents dans Bitcoin Core [26]. Dans cette logique, il suffit d'imposer un bloc comme obligatoire pour invalider la chaîne des censeurs. Cela a été réalisé par Bitcoin SV en août 2021, qui subissait alors une censure active [27].

Toutefois, même si ce type de recours peut effectivement fonctionner de manière ponctuelle et temporaire, il ne constitue en rien un mécanisme robuste de résistance à la censure. En effet, il crée beaucoup trop d'instabilité en faisant en dernier lieu reposer le consensus sur l'accord social. Il offre ainsi la possibilité pour une puissance hostile de déstabiliser durablement le système en semant la zizanie dans la communauté (notamment par la pression exercée sur les relais d'opinion) et en créant par là des scissions multiples impossibles à départager par un facteur objectif.

L'intervention directe de l'accord social dans la confirmation des transactions est par conséquent une très mauvaise idée. Même dans les cas où les

participants sont d'accord pour dire qu'un tel évènement est indésirable, ils sont souvent en total désaccord sur la manière de traiter le problème, ainsi qu'on l'a observé lors de la scission entre Ethereum et Ethereum Classic. Les être humains sont capables de se mettre d'accord à long terme, comme le témoigne la convergence vers un petit nombre de langues, de religions, de monnaies, etc. Néanmoins, à court terme ce n'est très certainement pas le cas. D'où le recours au mécanisme de consensus automatisé qu'est le minage.

Une autre mesure proposée, moins subjective mais plus perturbatrice, est la modification de la fonction de preuve de travail. Celle-ci permet de faire cesser l'attaque à court terme puisqu'elle rend le matériel spécialisé des censeurs obsolète, leur faisant supporter une lourde perte au passage. Il s'agit d'un hard fork (à savoir une modification incompatible des règles de consensus) qui doit être activé par les utilisateurs à un horodatage ou à une hauteur de bloc donné, c'est-à-dire un *User Activated Hard Fork* (UAHF). Cette option extrême a été soutenue par les développeurs Luke-Jr et Gregory Maxwell lors de la guerre des blocs en 2015 – 2016. Elle a également été défendue par le développeur en chef de Bitcoin ABC Amaury Séchet en novembre 2018 qui l'a qualifiée d'« option nucléaire [...] de dernier recours [28] ».

De même que dans le cas de l'invalidation de la censure par intervention sociale, il s'agit d'une mesure plus néfaste à long terme que le statu quo. Premièrement, la perte subie par les censeurs est aussi encaissée par les mineurs honnêtes et dissidents. Deuxièmement, l'économie est répartie entre deux chaînes distinctes, réduisant l'utilité monétaire totale. Troisièmement, le coût d'une attaque est drastiquement réduit à court terme. Quatrièmement, les mineurs perdent confiance dans le protocole et doivent s'assurer contre le risque d'un nouveau changement, réhaussant le coût de la sécurité minière par rapport au coût de l'attaque. Et cinquièmement, la nouvelle distribution du minage n'est pas forcément meilleure que l'ancienne, les gros mineurs pouvant déployer du capital plus facilement.

De manière générale, l'intervention humaine à court terme est loin d'être désirable. Si la chaîne subit une attaque minière, il est probable qu'elle soit aussi attaquée au niveau social. Les interventions ont ainsi toutes les chances de se multiplier, faisant sombrer la chaîne dans une spirale de scissions et la menant à l'insignifiance économique. Le cas de Bitcoin Cash est le plus éclairant : en raison de hard forks programmés tous les six mois, la chaîne a subi deux scissions majeures après sa séparation avec Bitcoin-BTC (en 2018 avec BSV et en 2020 avec XEC), ce qui a mené l'ensemble à être valorisé à moins de 1 % de la valeur agrégée du BTC. En outre, si ce caractère néfaste est

valable pour les cryptomonnaies en construction, qui peuvent se permettre ces interventions en raison de la petitesse et de l'homogénéité de leur économie, elle l'est d'autant plus pour une version mature de Bitcoin qui soutiendrait une économie plus grande et plus diversifiée.

Les variantes des consensus par preuve de travail

Le risque de censure a également inspiré le développement d'algorithmes de consensus alternatifs à celui de Bitcoin. L'alternative la plus connue est la preuve d'enjeu, qui sera décrite dans la section suivante. Les autres alternatives sont des variantes de l'algorithme de Nakamoto par preuve de travail, dont les trois principales sont le minage combiné, la preuve d'espace et la finalisation anticipée.

La première proposition est le minage combiné. Le minage combiné, ou *merge mining* en anglais, est l'action de miner plusieurs chaînes en simultané par la réutilisation du travail fourni sur une chaîne mère pour la validation des chaînes filles ou auxiliaires.

Le procédé a été décrit par Satoshi Nakamoto en décembre 2010, dans un message concernant BitDNS, le projet de système distribué de noms de domaine à l'origine de Namecoin. Le créateur de Bitcoin écrivait ainsi sur le forum :

> « Je pense qu'il serait possible que BitDNS forme un réseau complètement séparé et possède une chaîne de blocs distincte, tout en partageant la puissance de calcul avec Bitcoin. Le seul chevauchement consisterait à faire en sorte que les mineurs puissent rechercher des preuves de travail pour les deux réseaux simultanément.
>
> Les réseaux n'auraient besoin d'aucune coordination. Les mineurs adhéreraient aux deux réseaux en parallèle. Ils scanneraient SHA de telle sorte que s'ils obtenaient un résultat, ils pourraient résoudre les deux en même temps. Une solution pourrait concerner un seul des réseaux si l'un d'eux présentait une difficulté moindre.
>
> Je pense qu'un mineur externe pourrait appeler getwork sur les deux programmes et combiner le travail. Peut-être appeler Bitcoin, en tirer un travail, le remettre à getwork sur BitDNS pour le combiner en un travail commun.
>
> Plutôt que de fragmenter l'ensemble, les réseaux partageraient et augmenteraient la puissance de calcul totale de chacun. Cela résoudrait le problème des réseaux multiples, qui constituent un danger les uns pour les autres si la puissance de calcul disponible se concentre sur l'un d'entre eux. Au lieu de cela, tous les réseaux du monde partageraient la puissance de calcul combinée, augmentant ainsi la puissance totale. Il serait plus facile pour les petits réseaux de

se lancer en puisant dans une base existante de mineurs [29]. »

Le minage combiné consiste à réutiliser des preuves de travail partielles d'une chaîne mère comme des preuves de travail valides sur une chaîne fille. Ces preuves de travail, dites « auxiliaires » et abrégées en AuxPOW, sont des sous-produits du minage de la chaîne mère, et ne nécessitent pas de dépense d'énergie supplémentaire. La seule charge imposée par le minage combiné est la gestion de la chaîne fille.

Les mineurs de la chaîne fille reçoivent des récompenses supplémentaires qui sont constituées de la création monétaire locale (si la chaîne utilise une nouvelle unité de compte) et des frais de transaction. Les mineurs de la chaîne mère sont donc incités à tirer profit de cette nouvelle manne. La chaîne fille peut de ce fait disposer d'un taux de hachage conséquent assez rapidement.

Le minage combiné a été mis en avant comme une méthode permettant de faciliter l'amorçage d'une nouvelle cryptomonnaie, en bénéficiant de l'industrie minière établie. Ce type d'algorithme de consensus a ainsi été mis en place sur Namecoin par rapport à Bitcoin et sur Dogecoin par rapport à Litecoin. Il a aussi été suggéré comme mécanisme de synchronisation des chaînes latérales. Il est ainsi implémenté de manière hybride dans RSK. Il est plus largement envisagé par Paul Sztorc dans sa proposition de Drivechain (voir chapitre 14).

Cependant, l'apport en sécurité du minage combiné par rapport au minage classique est relativement faible. Le procédé permet d'augmenter le nombre d'acteurs impliqués et de restreindre les attaquants possibles (ceux-ci devant être des mineurs de la chaîne principale), mais il ne modifie pas le coût de l'attaque, qui dépend du revenu minier de cette chaîne et, dans le cas de la censure, des frais de transaction.

Une illustration éclatante de ce fait est l'exemple de Coiledcoin (CLC), une cryptomonnaie alternative créée en janvier 2012 qui a subi une attaque de censure fatale peu de temps après son lancement. L'attaque a été réalisée par le développeur de Bitcoin Luke-Jr par le biais de sa coopérative de minage, Eligius, sans qu'il n'en informe les hacheurs. Dans son message d'explication, il précisait qu'aucun membre de la coopérative n'avait subi de perte, le coût étant surtout le temps qu'il avait passé à configurer le logiciel [30].

Le minage combiné a deux effets sur la sécurité minière de la chaîne mère. D'une part, il augmente artificiellement la puissance de calcul déployée pour miner des blocs, ce qui paraît bénéfique de prime abord. Cependant, cette hausse artificielle n'agit en rien contre la censure des transactions. D'autre part, le minage combiné entraîne une centralisation de l'activité minière, en raison de la charge que représente la gestion des chaînes auxiliaires : si les

chaînes auxiliaires deviennent importantes économiquement, les mineurs de la chaîne mère n'ont d'autre choix que de les miner pour rester rentables.

La deuxième alternative est la preuve d'espace (de l'anglais *proof of space*), parfois aussi appelée preuve de capacité ou preuve de stockage, qui se base, non pas sur le calcul informatique, mais sur la capacité à garder des données en mémoire. La ressource n'est plus la puissance de calcul, mais l'espace disque.

Cette idée a été partiellement incluse dans certains algorithmes hybrides de preuve de travail, dans le but de décourager le développement de matériel spécialisé (ASIC) et de favoriser le minage par processeurs accessibles au grand public (CPU et GPU). C'est le cas de la fonction scrypt (ou S-Crypt), une fonction de dérivation de clé coûteuse en mémoire adaptée par le mineur ArtForz pour être intégrée au sein de Tenebrix en septembre 2011. Celle-ci a été héritée plus tard par Litecoin. C'est également le cas de l'ancienne fonction de minage d'Ethereum utilisé entre 2015 et 2022, ETHash, qui est une variante de l'algorithme Dagger-Hashimoto et qui rend le calcul de la preuve plus coûteux en mémoire par la nécessité de stocker un graphe acyclique orienté de plusieurs gigaoctets. Ethereum utilisait de plus une version modifiée de l'algorithme de Nakamoto, GHOST, qui avait pour intérêt de sélectionner la chaîne la plus lourde en prenant en compte les blocs orphelins. Depuis novembre 2020, Ethereum Classic utilise une variante de ETHash nommée ETCHash. Un dernier exemple est l'algorithme RandomX, actif sur Monero depuis 2019, qui est conçu spécialement pour favoriser le minage par CPU.

Au-delà des fonctions de preuve de travail coûteuses en mémoire, il existe des algorithmes de preuve d'espace pure. C'est en pratique le cas du système Chia Network, projet de Bram Cohen, qui se base sur les « preuves d'espace et de temps » pour déterminer la chaîne correcte.

Ces algorithmes fondés à des degrés divers sur la mémoire informatique sont censés être plus résistants à la censure en facilitant la participation du grand public et en améliorant de ce fait la distribution de la validation. Mais ils ne font que déplacer le problème. Ce qu'il faut comprendre avec la preuve d'espace, c'est qu'il s'agit de dépenser de l'énergie extérieure d'une autre manière. La preuve d'espace est une preuve de travail déguisée : elle revient en fin de compte à effectuer une autre forme de travail, qui peut être optimisée. Cette optimisation peut avoir lieu tant au niveau de la conception du matériel (ASIC) qu'au niveau de l'organisation industrielle (économie d'échelle), ce qui fait que les pressions centralisatrices ne disparaissent pas complètement. Tout ce qu'on peut espérer, c'est de rapprocher l'efficacité du matériel spécialisé

de celle d'un outil utilisé par tous, comme ce qui est fait par RandomX avec le CPU.

La troisième alternative est la finalisation anticipée des blocs. Celle-ci consiste à mettre en place des points de contrôle mobiles au sein du protocole, de façon à considérer comme final tout bloc qui se trouverait en dessous d'une certaine profondeur. Vitalik Buterin parle de « subjectivité faible [31] » pour décrire ce type de mécanisme.

Un tel algorithme a été mis en place par Bitcoin ABC le 20 novembre 2018 au sein de Bitcoin Cash, face à la menace d'attaque de la part du camp de Bitcoin SV, sous la forme d'une protection contre la recoordination profonde, qui consistait à considérer un bloc comme final au bout de 11 confirmations. Ce procédé est encore présent dans certaines implémentations de Bitcoin Cash et de XEC, et est appliqué par les grandes plateformes de change, ce qui en fait *de facto* une règle de consensus.

Dans Ethereum Classic, qui a subi de multiples attaques de double dépense en 2019 et en 2020, une variante de cette finalisation a été intégrée le 11 octobre 2020. L'algorithme en question est appelé *Modified Exponential Subjective Scoring* (MESS) et consiste à attribuer différents scores aux branches concurrentes, privilégiant les segments vus les premiers aux segments vus ultérieurement. Il permettrait de diviser le coût d'une attaque par 31.

Ces algorithmes réduisent effectivement la probabilité d'une attaque opportuniste, car ils empêchent les recoordinations. Cependant, ils ont le résultat inverse sur les attaques de censure dont le but est de détruire l'utilité fondamentale de la chaîne. Ces algorithmes sont en effet sujets au problème de la subjectivité. Un nouveau nœud qui se synchronise avec le réseau peut être trompé par un attaquant en suivant la chaîne la plus longue et non la chaîne considérée comme valide par le reste du réseau. De ce fait, un attaquant (réalisant une attaque Goldfinger) peut facilement tirer profit de cette caractéristique en créant des chaînes concurrentes plus longues pour causer la confusion [32].

Idéalement, le concept de Bitcoin n'intègre aucun point de contrôle à l'exception du bloc de genèse défini préalablement, et la chaîne correcte est déterminée uniquement par la quantité de travail accumulée. Bien qu'il ait lui-même ajouté des points de contrôle manuels, Satoshi Nakamoto expliquait :

> « Le logiciel n'a aucun moyen de savoir automatiquement si une chaîne est meilleure qu'une autre, sauf en se fiant à la plus grande preuve de travail. Dans le modèle, il était nécessaire qu'il se tourne vers la chaîne plus longue, quelle que soit la distance à parcourir [33]. »

La preuve d'enjeu

L'autre alternative à l'algorithme de Nakamoto par preuve de travail est le recours à un autre mécanisme de résistance aux attaques Sybil : la preuve d'enjeu. La preuve d'enjeu, de l'anglais *proof of stake*, est un procédé permettant à quelqu'un de démontrer son implication dans un système par le biais d'un algorithme de signature, dans le cadre de l'accès à un privilège. Dans le cas des systèmes cryptoéconomiques gérant une unité de compte numérique, elle intervient dans le choix des validateurs chargés de produire les blocs de transactions. Le validateur d'un bloc donné est alors sélectionné par le réseau selon le nombre d'unités qu'il met en jeu (ou selon un autre paramètre lié). La preuve d'enjeu est parfois décrite comme du « minage virtuel » car les jetons numériques jouent le même rôle que l'énergie électrique dans les algorithmes basés sur la preuve de travail, la probabilité de valider un bloc étant la plupart du temps proportionnelle au nombre d'unités en possession du validateur.

Les unités du validateur sont mises en jeu dans le sens où elles sont bloquées par le système et où elles sont détruites en cas de comportement hostile au réseau. Cette dernière propriété permet d'éviter le problème du « rien à perdre » (*nothing-at-stake problem*) qui se poserait dans le cas d'une mise en œuvre naïve du procédé, dans laquelle les validateurs peuvent valider plusieurs chaînes concurrentes en même temps, contrairement à la preuve de travail où l'énergie ne peut pas être dupliquée. Par exemple, l'algorithme de consensus d'Ethereum, Casper FFG, met en place une « coupe des fonds » (ou *slashing*) pour sanctionner progressivement les validateurs qui ne respectent pas les règles de bonne conduite [34]. Cela permet au réseau de se prémunir contre les attaques de courte portée. De plus, la preuve d'enjeu étant subjective, elle nécessite des points de contrôles, qui séparent différentes « époques », pour contrer les attaques de longue portée.

L'idée de la preuve d'enjeu est une vieille idée puisqu'on la retrouve dans la conception de b-money, le système imaginé par le cypherpunk Wei Dai en 1998 et décrit dans le chapitre 6. Dans son modèle, chaque serveur devait déposer un certain montant de b-money sur un compte spécial pour participer aux opérations du réseau. Le montant servait de garantie pour pénaliser le serveur en cas de mauvaise conduite.

Le terme « *proof of stake* » a été inventé en juillet 2011 par un membre du forum de Bitcoin utilisant le pseudonyme QuantumMechanic, qui décrivait comment le concept pouvait être adapté aux systèmes cryptomonétaires [35]. Cette idée a été mise en œuvre un an plus tard, en août 2012, par Sunny King et Scott Nadal, par le biais de leur protocole PPCoin. Ce dernier se basait

sur un modèle hybride combinant énergie électrique et âge des pièces (preuve de conservation) pour sa validation. Il est aujourd'hui connu sous le nom de Peercoin.

De même que la preuve de travail peut être étendue en preuve de mémoire, la preuve d'enjeu peut être dérivée en plusieurs variantes. La preuve d'enjeu déléguée prend ainsi en compte les unités possédées mais aussi les unités déléguées aux validateurs. Il s'agit de la variante la plus répandue. Elle permet de mettre en place une preuve d'enjeu liquide (à la Tezos), mais a néanmoins pour inconvénient de centraliser la validation. Il existe également d'autres variantes comme la preuve de conservation (Peercoin), la preuve de vélocité (Reddcoin) ou la preuve d'importance (NEM).

De manière générale, on peut regrouper les mécanismes de résistance aux attaques Sybil des systèmes ouverts en deux catégories de preuve : les preuves externes, basées sur l'utilisation de l'énergie dans le monde physique, et les preuves internes, basées sur l'état du registre virtuel. Il y a ainsi une auto-référence dans le cas de la preuve d'enjeu, ce qui peut poser problème.

Les défenseurs de la preuve d'enjeu prétendent que la preuve d'enjeu est plus sécurisée, car le coût d'une attaque est un ordre de grandeur plus élevé. Une attaque de censure pourrait en outre faire baisser le prix de l'unité de compte, ce qui provoquerait une baisse de valeur du capital de l'attaquant. Nous affirmons l'inverse : la preuve d'enjeu offre une résistance à la censure moins forte que la preuve de travail.

Tout d'abord, réunir les unités nécessaires est loin d'être une tâche impossible. Premièrement, tous les détenteurs ne sont pas impliqués dans le consensus, ce qui veut dire que seule la portion des unités mises en jeu est concernée. Deuxièmement, contrairement à la preuve de travail qui exige 51 % de la puissance de calcul pour perturber le système, la plupart des algorithmes par preuve d'enjeu sont des algorithmes classiques dont l'attaque ne nécessite que 34 % des fonds en jeu. Troisièmement, une grande partie des unités sont conservées par des acteurs centralisés qui offrent généralement des services de *staking* (incitant l'accumulation), et qui sont réglementés et donc particulièrement sensibles à la cooptation étatique.

Ensuite, un défaut de la preuve d'enjeu est qu'elle permet une meilleure identification du validateur, associé à une clé publique liée aux fonds sous séquestre, que dans le cas de la preuve de travail, où les mineurs peuvent diriger leur puissance de calcul vers la chaîne libre plus discrètement. La validation par preuve d'enjeu est donc moins confidentielle que le minage qui est complètement anonyme par conception.

Enfin, et surtout, la principale raison pour laquelle la preuve d'enjeu produit une résistance à la censure plus faible est le caractère interne de la preuve. Dans le cas de la preuve de travail, il est toujours possible de combattre la censure : il suffit de réunir une puissance de calcul supérieure aux censeurs, en construisant des machines et en apportant une énergie supplémentaire. Dans le cas de la preuve d'enjeu, il n'est pas possible de créer des unités additionnelles sans modifier les règles de consensus, de sorte que les censeurs, qui contrôlent une majorité des unités existantes et reçoivent par conséquent une majorité de la création monétaire, sont intouchables.

Pour répondre à ce problème, les partisans de la preuve d'enjeu sur Ethereum prônent généralement le recours à l'accord social. Il ne s'agit pas seulement de sélectionner la chaîne valide manuellement comme nous l'avons expliqué précédemment, mais de rééquilibrer la distribution des unités de façon à retrouver un système de validation qui ne censure pas. Puisque la création d'unités supplémentaires pose la question épineuse de la destination desdites unités, ce rééquilibrage consiste plutôt à détruire les fonds mis en jeu par les censeurs, une mesure appelée le *slashing* social [36]. Ce recours est notamment soutenu par Vitalik Buterin, qui écrivait la chose suivante en 2020 :

> « Pour d'autres attaques plus difficiles à détecter (notamment une coalition de 51 % censurant tous les autres), la communauté peut se coordonner pour réaliser un soft fork activé par les utilisateurs (UASF) minoritaire dans lequel les fonds de l'attaquant sont [...] largement détruits (dans Ethereum, cela se fait via le "mécanisme de fuite d'inactivité"). Aucun "hard fork pour supprimer les pièces" explicite n'est nécessaire ; à l'exception de la nécessité de coordonner l'UASF pour sélectionner un bloc minoritaire, tout le reste est automatisé et suit simplement l'exécution des règles du protocole [37]. »

À l'heure d'écriture de ces lignes, la mesure n'a jamais été appliquée sur Ethereum. Le cas qui s'en rapproche le plus est le contentieux entre la Fondation Tron de Justin Sun et la communauté historique de Steem qui s'est conclu par le gel des fonds de la première par une intervention externe de la communauté en mars 2020. Cette intervention a provoqué une scission entre le protocole Steem contrôlé par la Fondation Tron et la plateforme Hive.

Le recours à l'accord social paraît une nouvelle fois être une bonne idée. Cependant, il s'agit clairement de jouer avec le feu : le risque de créer la confusion et de provoquer une scission est largement sous-estimé. De manière générale, c'est ce qui différencie la philosophie derrière la preuve d'enjeu de celle de la preuve de travail. Les défenseurs de la preuve d'enjeu ne modélisent pas la menace de la même manière, et c'est pourquoi le modèle de sécurité de

Bitcoin est bien plus exigeant que celui d'Ethereum.

Consommation d'énergie et résistance à la censure

Ainsi, la preuve de travail joue un rôle essentiel dans la résistance à la censure de Bitcoin. Tout le génie de Nakamoto réside dans le fait d'avoir découvert un mécanisme de consensus basé sur une grandeur objective extérieure au système, qui permette la résolution de la censure sans intervention humaine au niveau du protocole, même face à une attaque étatique.

Il s'avère que la mise en œuvre de cette preuve de travail consomme une importante quantité d'énergie électrique. Mais c'est cette consommation qui ancre le protocole dans le réel et c'est donc le prix à payer pour disposer d'un système réellement résistant à la censure. Elle peut être réduite, mais elle ne peut pas être évitée.

La consommation d'énergie est l'un des arguments d'opposition à Bitcoin les plus récurrents, en raison de son supposé impact écologique [38]. Au vu de ce que nous avons dit dans ce chapitre, cette opposition de façade, loin de lutter contre la consommation d'énergie de la cryptomonnaie, contribue à renforcer le conflit qui existe entre le contrôle financier et la résistance à la censure, et par conséquent à augmenter l'énergie consommée des deux côtés. C'est pourquoi une bonne façon de réduire la consommation d'énergie de Bitcoin serait de prôner une plus grande concurrence monétaire et bancaire en vue de diminuer son utilité réelle et potentielle.

La proposition de l'abandon de la preuve de travail, telle que celle faite par Greenpeace en 2022, s'inscrit donc dans la deuxième catégorie d'attaques contre Bitcoin, à savoir les attaques sociales. Heureusement, Bitcoin dispose également d'un mécanisme de défense à ce niveau-là. Dans les chapitres suivants, nous décrirons comment le protocole peut être modifié et quels principes sous-jacents sont à l'œuvre dans sa détermination.

10

Le changement de la monnaie

Une monnaie est un accord concernant un moyen mutuellement acceptable dans le commerce. Cet accord peut porter sur des propriétés physiques, auquel cas le support monétaire est une marchandise, ou des propriétés numériques, auquel cas le support monétaire est un protocole informatique. Bitcoin appartient à cette seconde catégorie.

Par sa nature ouverte et libre, le code informatique de Bitcoin peut être copié, modifié et réutilisé à volonté. Par conséquent, le protocole (et la monnaie qu'il définit) peut lui aussi être changé, grâce à l'application d'un code différent sur le réseau. Bitcoin n'est ainsi pas un système figé qui serait géré par une autorité centrale, mais une structure ouverte qui connaît une évolution organique au cours du temps.

Le protocole

Bitcoin est par essence un protocole de communication informatique, c'est-à-dire un ensemble de règles permettant à différentes parties d'un réseau d'échanger des informations. Ce protocole permet aux nœuds du réseau pair à pair de s'échanger des transactions et des blocs et de se mettre d'accord sur le registre de propriété considéré comme correct. Le résultat est un système monétaire.

Bitcoin se rapproche, de façon plus ou moins manifeste, de protocoles existants. C'est par exemple le cas d'autres protocoles construits sur Internet,

comme HTTP (*HyperText Transfer Protocol*) qui est utilisé pour l'affichage des pages web, SMTP (*Simple Mail Transfer Protocol*) qui est utilisé pour le courrier électronique, ou encore BitTorrent, qui permet le partage de fichiers de pair à pair. C'est également le cas des protocoles qui soutiennent Internet, appelés protocoles de la suite TCP/IP en référence aux deux premiers qui la composent : IP (*Internet Protocol*) qui assure la communication au niveau de la couche réseau, et TCP (*Transmission Control Protocol*) qui assure la transmission au niveau de la couche transport, en surcouche de la couche réseau.

Plus éloigné de Bitcoin, on peut citer la catégorie des langages de programmation. Ces langages permettent d'écrire du code (texte spécifique encodé en UTF-8), qui est transformé en fichier exécutable par un compilateur (par exemple dans le cas du C, du C++ ou du Java) ou qui est directement exécuté par un interpréteur (comme c'est le cas pour Python ou Javascript). Dans le même ordre d'idées, les langues humaines comme le français ou l'anglais sont aussi des protocoles de communication, dont les règles sont moins formelles et moins bien définies, mais qui permettent aux hommes d'échanger des informations.

Enfin, les monnaies peuvent être vues comme des sortes de protocole, en constituant des moyens communs de communiquer de la valeur et de formaliser l'échange économique. La monnaie se définit en particulier par le support accepté dans le commerce : pour une marchandise comme l'or ou l'argent, ce support est un élément chimique ; pour la monnaie fiat, il s'agit d'un certificat émis par une autorité.

Dans le cas de Bitcoin, le protocole est formé de l'ensemble des règles qui permettent au réseau de communiquer et de se coordonner. Ce protocole se divise en deux parties distinctes : le protocole de transmission, constitué des règles de réseau, et le protocole régissant le contenu transmis, constitué des règles de consensus.

Les règles de réseau sont les règles qui permettent aux nœuds d'entrer en communication sur Internet. Ces règles concernent le protocole de transport sous-jacent (TCP, Tor, UDP pour FIBRE), le port réseau (8333 pour le réseau principal BTC), la procédure de découverte de pairs, la syntaxe des messages de transmission de données, etc. Elles peuvent différer selon les nœuds sans briser formellement le consensus : il suffit qu'un nœud acceptant les deux ensembles de règles fasse la liaison. De même, les nœuds sont libres de restreindre (temporairement ou définitivement) leur connexion avec un autre nœud, notamment dans le but d'éviter le spam.

Les règles de consensus sont les règles de construction et d'organisation des blocs et des transactions. Elles régissent la validité du registre sur lequel les membres du réseau arrivent à un accord, d'où leur nom. Ces règles sont critiques : un nœud qui transmettrait une transaction ou un bloc invalide aux autres nœuds verrait sa transaction ou son bloc être rejeté par le reste du réseau.

Les règles de consensus sont nombreuses. Certaines d'entre elles sont largement connues et explicites. En voici quelques-unes ici :

— Le montant en entrée d'une transaction doit être supérieur (ou égal) au montant en sortie, la différence représentant les frais collectés par le mineur ;
— Chaque entrée doit contenir un script de déverrouillage (contenant la ou les signatures) qui correspond au script de verrouillage (l'adresse d'envoi) de la sortie dépensée ;
— Une sortie transactionnelle ne peut être dépensée qu'une seule fois, en raison de l'interdiction de double dépense ;
— Chaque bloc doit comporter une preuve de travail, produite par hachages répétés de l'entête par la fonction SHA-256, de degré supérieur à la difficulté du réseau ;
— La subvention dans chaque bloc doit être inférieure à une limite, qui est divisée par deux tous les 210 000 blocs (4 ans environ) ;
— La difficulté du minage est ajustée tous les 2016 blocs (2 semaines environ), de sorte à garantir un temps moyen de 10 minutes entre chaque bloc ;
— Le poids des blocs est limité à 4 millions d'unités de poids (telles que définies par SegWit), ce qui restreint la capacité transactionnelle du système.

Les règles de consensus sont trop nombreuses pour être toutes explicitées. Quand elles ne le sont pas, ces règles sont implicitement définies dans l'implémentation logicielle de référence, qui est Bitcoin Core dans le cas de BTC.

Les implémentations logicielles

Les implémentations logicielles sont les programmes informatiques qui mettent en œuvre le protocole. Dans le cas des implémentations de nœud complet, la totalité des règles de consensus sont appliquées. Les implémentations peuvent également être partielles, auquel cas elles ne mettent pas en œuvre

l'intégralité des règles de consensus : c'est par exemple le cas des portefeuilles légers, qui procèdent à une vérification simplifiée de leurs transactions.

Dans BTC, il existe plusieurs implémentations, dont Bitcoin Core, Libbitcoin, btcd et Bitcoin Knots. La plus connue est Bitcoin Core, qui est à la fois l'implémentation historique créée par Satoshi Nakamoto (« *Satoshi client* ») et reprise par Gavin Andresen en 2010, l'implémentation principale utilisée par plus de 99 % des nœuds en novembre 2023, et l'implémentation de référence, qui définit les règles de consensus implicites.

D'autres protocoles possèdent des implémentations différentes. Bitcoin Cash présente une multiplicité d'implémentations dont les deux principales sont Bitcoin Cash Node (l'implémentation de référence issue de Bitcoin ABC, elle-même issue de Bitcoin Core) et Bitcoin Unlimited. Ethereum repose également sur une diversité d'implémentations, qui gèrent la transmission et la vérification des transactions (Geth, Nethermind, etc.) ou celles des blocs (Prysm, Lighthouse, etc.)

Une implémentation est en règle générale un logiciel libre, c'est-à-dire un logiciel dont le code est publié en accès libre sous une licence permettant l'utilisation, la modification et la reproduction. Cette caractéristique, technique et juridique, est *essentielle* à Bitcoin, car elle permet non seulement de vérifier le fonctionnement du logiciel [1], mais aussi de reprendre la main sur le code dans le cas où les développeurs iraient dans une direction non désirée.

L'action de copier et de modifier un logiciel est appelé un *fork* ou embranchement. Il s'agit de créer un nouveau logiciel à partir du code source d'un logiciel existant, dont l'existence découle d'une vision différente du développement de ce logiciel. Les distributions Linux sont ainsi formées de distributions antérieures. On peut aussi citer OpenOffice.org qui a donné LibreOffice et Apache OpenOffice.

Bitcoin Core descend directement de la première implémentation codée par Satoshi Nakamoto et partagée publiquement par ce dernier le 8 janvier 2009. Initialement appelé simplement « Bitcoin », le logiciel a été renommé bitcoind / Bitcoin-Qt en 2011, puis rebaptisé Bitcoin Core le 19 mars 2014.

Bitcoin Core est un logiciel codé en C++. Initialement hébergé sur SourceForge, le code est aujourd'hui présent sur GitHub [2]. Il est publié sous licence libre MIT, de sorte que quiconque peut le copier et le modifier à sa guise. En particulier, la licence MIT est permissive : elle n'empêche pas la réutilisation du code comme partie ou comme base d'un logiciel soumis à une licence privative. Cette licence a été choisie par Satoshi, au détriment de la licence GPL, en raison de sa compatibilité avec les autres licences [3].

Le développement de Bitcoin Core se fait de manière ouverte et méritocratique. Le dépôt GitHub est ouvert à tous et n'importe qui peut contribuer au maintien et à l'amélioration du logiciel en faisant une demande de modification du code (*pull request*). Les contributeurs fréquents sont appelés des « *core developers* ». Pour faciliter le développement, les contributeurs communiquent par différents moyens, mais les deux principaux sont le canal IRC bitcoin-core-dev où ont lieu la plupart des discussions et la liste de diffusion bitcoin-dev.

Toutefois, Bitcoin Core dispose d'une certaine hiérarchie. Le dépôt est en effet géré par des mainteneurs qui sont responsables de fusionner les demandes de modification créées par les contributeurs. L'inclusion dans le code dépend ainsi de différents critères évalués par ces mainteneurs, comme l'utilité démontrable du changement, le format correct suivant les lignes directrices du projet, la revue par les pairs ou la réputation du contributeur [4].

La charge du logiciel était initialement allouée à un mainteneur principal, qui avait pour rôle de nommer les mainteneurs normaux, de décider du cycle de sortie du logiciel, de fusionner l'ensemble des modifications et de modérer les débats. Cette mission était assurée au début par Satoshi Nakamoto qui s'occupait d'intégrer les contributions sur le dépôt SourceForge. Puis, le 23 février 2011, Satoshi a transmis la responsabilité à Gavin Andresen, avant de disparaître définitivement. Gavin s'est ensuite chargé du projet pendant plus de trois ans avant de laisser sa place à Wladimir J. van der Laan le 7 avril 2014. Enfin, le 7 février 2023, ce dernier a démissionné après neuf ans de service. La fonction de mainteneur principal a alors été supprimée et remplacée par la responsabilité collective des mainteneurs [5].

En novembre 2023, les mainteneurs de Bitcoin Core étaient au nombre de cinq : Michael Ford, Hennadii Stepanov, Andrew Chow, Gloria Zhao et Ryan Ofsky. Ils suivent la voie de mainteneurs emblématiques (hors mainteneurs principaux) comme Martti Malmi, Laszlo Hanyecz, Chris Moore, Pieter Wuille, Jeff Garzik, Nils Schneider, Gregory Maxwell, Jonas Schnelli, Samuel Dobson ou Marco Falke. Parmi les contributeurs actifs qui n'ont jamais été mainteneurs, on retrouve Matt Corallo, practicalswift, Luke-Jr et John Newbery. Les empreintes PGP des mainteneurs sont disponibles publiquement sur le dépôt.

Ce fonctionnement ouvert donne au logiciel une sûreté plus grande que la plupart des programmes informatiques. En effet, au vu des sommes en jeu, la récompense pour l'exploitation réussie d'une faille majeure serait énorme, si bien qu'on peut supposer qu'une telle faille n'a pas été découverte. S'il y a

effectivement des vulnérabilités dans le logiciel, celles-ci sont très rares et très subtiles, de sorte qu'elles sont généralement découvertes par des développeurs bienveillants, à l'instar du développeur Awemany qui avait, en septembre 2018, divulgué de manière responsable une faille inflationniste dans le code [6]. Ainsi, le passage du temps renforce la confiance qu'on peut avoir dans le logiciel (ainsi que dans le système) conformément à l'effet Lindy [7].

Les propositions d'amélioration de Bitcoin

Les implémentations peuvent être mises à jour par leurs développeurs, auquel cas elles ont chacune leur modèle de décision. Dans Bitcoin Core, comme on l'a dit, tout le monde peut proposer une modification du code mais le dernier mot est laissé aux développeurs. De même, les changements internes liés aux portefeuilles sont gérés par leurs développeurs propres.

Il existe néanmoins une façon de proposer des modifications pouvant s'appliquer à toutes les implémentations : les propositions d'amélioration de Bitcoin (en anglais *Bitcoin Improvement Proposals* ou BIP), qui sont des documents décrivant des changements possibles du protocole ou fournissant des informations générales à la communauté. Ce système des BIP a été formalisé par Amir Taaki en 2011, sur la base des *Python Enhancement Proposals* (PEP) qui servent à améliorer le langage de programmation Python. Initialement défini par le BIP-1, le procédé est aujourd'hui décrit par le BIP-2, rédigé par Luke-Jr. Il est hébergé sur un dépôt GitHub géré par Bitcoin Core.

Les BIP peuvent être répartis en trois types : le BIP de suivi de standard (*standards track BIP*), qui concerne les changements qui affectent la plupart ou toutes les implémentations de Bitcoin ; le BIP informationnel (*informational BIP*), qui décrit un problème dans la conception de Bitcoin ou donne des directives générales ou des informations à la communauté de Bitcoin, mais ne propose pas de nouvelle fonctionnalité ; le BIP de procédure (*process BIP*), qui décrit une procédure ou un changement de procédure à adopter. Les BIP de suivi de standard sont les plus courants. Ils peuvent concerner différents aspects : les règles de consensus, le protocole de transmission (*Peer Services*), l'interface logicielle (*API/RPC*) ou les conventions utilisées dans les applications [8].

Avant d'être adopté, un BIP doit passer par de nombreuses étapes. D'abord, il est assigné à un ou plusieurs auteurs qui se chargent d'en rédiger une première version respectant le format défini et prenant en compte l'état de l'art correspondant. Puis, le BIP est partagé dans la communauté des dévelop-

peurs de Bitcoin, généralement par l'intermédiaire de la liste de diffusion de développement (bitcoin-dev). Les discussions ont lieu sur cette mailing list. Ensuite, le BIP est officiellement proposé au système sous la forme d'une demande de modification du code (*pull request*) sur le dépôt GitHub, qui doit être approuvée par l'éditeur désigné par Bitcoin Core (Luke-Jr depuis 2016). Enfin, un numéro lui est assigné et il est intégré au dépôt sous la forme d'une ébauche. Il peut par la suite changer de statut au cours du temps, selon l'adoption de la communauté, l'objectif étant qu'il devienne définitif ou actif.

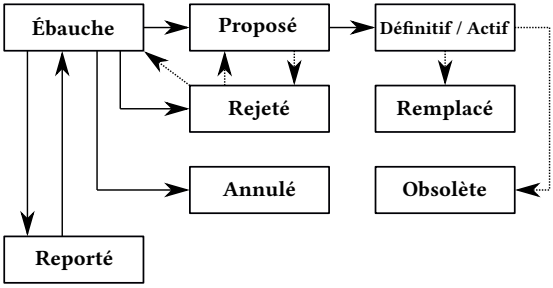

FIGURE 10.1 – Schéma de la procédure d'adoption d'un BIP, inspiré du BIP-1.

Notez que ces documents sont utilisés pour BTC mais également pour d'autres protocoles. Par exemple, les BIP décrivant le fonctionnement des portefeuilles (BIP-32, BIP-39, BIP-44) sont valides pour la grande majorité des cryptomonnaies. Le SLIP-44 recense les cryptomonnaies compatibles avec le BIP-44. Les autres protocoles cryptoéconomiques disposent même parfois de leurs propres systèmes de propositions. Ethereum utilise les EIP (*Ethereum Improvement Proposals*), Bitcoin Cash les CHIP (*Cash Improvement Proposals*), Litecoin les LIP, etc.

La vérification des règles de consensus

Bitcoin se base sur un réseau public d'ordinateurs accessible librement sur Internet. Ce réseau suit un modèle pair à pair, c'est-à-dire un modèle dans lequel tous les membres du réseau, appelés des nœuds, possèdent les mêmes privilèges. Ce sont ces nœuds qui s'assurent que les règles de consensus sont respectées. Si un bloc est invalide (en contenant une transaction invalide par exemple), alors il est rejeté par les nœuds appliquant les règles.

Dans Bitcoin, le rôle des nœuds est d'entretenir une copie du registre des transactions (la fameuse chaîne de blocs) et, ce faisant, de s'assurer de la validité des transactions et des blocs. Pour cela, ils communiquent avec les

autres nœuds du réseau et relaient les nouvelles transactions et les nouveaux blocs, qui émanent respectivement des utilisateurs et des mineurs.

La vérification des règles de consensus peut être complète. Dans ce cas, on utilise parfois le pléonasme « nœuds complets » ou « *full node* » pour insister sur le fait qu'ils vérifient l'intégralité de la chaîne. Ils téléchargent l'intégralité de la chaîne de blocs, vérifient les règles de consensus et relaient les blocs et les transactions. C'est une charge, que ce soit au niveau de la conservation des données (en novembre 2023, la chaîne de Bitcoin pesait environ 530 Go de données et l'ensemble des UTXO plus de 8,5 Go) que de la bande passante (la taille moyenne des blocs minés toutes les 10 minutes gravitait autour de 1,7 Mo en novembre 2023).

Les nœuds réduits (*pruned nodes*), qui conservent l'état du réseau mais pas l'entièreté de la chaîne, sont des nœuds à part entière puisqu'ils ont vérifié la conformité des règles sur l'intégralité de la chaîne. Ils ne sont juste pas en mesure d'accéder à l'historique de la chaîne précédant une certaine date.

La vérification peut aussi être partielle, auquel cas on parle de client léger (ou de « nœud léger » par abus de langage). Cela est utile pour les personnes qui n'ont pas l'intérêt de faire tourner un nœud complet. C'est par exemple le cas dans les logiciels de hachage (mettant en œuvre Stratum) et dans les portefeuilles légers. Ils utilisent en particulier une méthode conceptualisée dans le livre blanc de Bitcoin en 2008 : la vérification de paiement simplifiée [9].

La vérification de paiement simplifiée (nommée en anglais *Simplified Payment Verification* et abrégée en SPV) est une méthode astucieuse, qui permet aux utilisateurs néophytes et occasionnels de pouvoir interagir facilement avec le protocole sans devoir gérer un nœud complet, ni devoir faire aveuglément confiance à un dépositaire. Elle permet de réduire considérablement la charge des portefeuilles légers.

La vérification de paiement simplifiée se fonde sur la façon dont les blocs de transactions sont chaînés et structurés comme nous avons pu le voir dans le chapitre 8. Premièrement, la chaîne de preuve de travail n'est pas à proprement parler une chaîne de blocs, mais une chaîne d'entêtes. Cela fait que les clients légers n'ont qu'à conserver cette chaîne des entêtes pour déterminer la chaîne possédant le plus de travail accumulé. Puisque chaque entête pèse 80 octets, la taille des données à conserver reste modeste pour des appareils modernes : elle augmente d'environ 4 Mio par an, ce qui représentait un peu plus de 62 Mio en novembre 2023.

Deuxièmement, les transactions sont agencées dans un arbre de Merkle, de sorte que les clients légers peuvent se contenter de demander les informations

liées à la branche qui les intéresse pour s'assurer de la confirmation d'une de leurs transactions. Le nombre d'empreintes à obtenir et de hachages à effectuer dépend du logarithme binaire ($\log_2$) du nombre de transactions présentes dans le bloc. Pour un bloc de 3 000 transactions (moyenne haute sur BTC), la charge correspond à demander 12 empreintes de 32 octets et à calculer 12 hachages pour procéder à la vérification.

Cette vérification simplifiée permet d'alléger la charge des portefeuilles, mais elle présente des défauts majeurs. D'abord, elle manque de fiabilité : les nœuds ne peuvent pas mentir en inventant une transaction, mais peuvent omettre de transmettre des informations nécessaires. Ce défaut peut être partiellement contrebalancé en augmentant la diversité des connexions sur le réseau. Cependant, même dans ce cas, la vérification est vulnérable si la chaîne est attaquée par une entité disposant de la puissance de calcul majoritaire [10].

Ensuite, la vérification simplifiée possède aussi une insuffisance de confidentialité, car le client doit dévoiler une partie de son activité transactionnelle par les requêtes réalisées auprès des nœuds du réseau. Une façon de corriger partiellement ce problème est d'accroître le nombre d'informations demandées pour dissimuler les informations essentielles, mais cette méthode est plus qu'imparfaite [11].

Enfin, elle présente un défaut de vérification, en étant par définition partielle. Toutes les règles de consensus ne sont pas vérifiées, ce qui fait que les nœuds complets peuvent convenir d'un changement de règle qui ne sera pas remarqué par le client léger. Par exemple, les clients SPV ne vérifient pas les contraintes appliquées sur la taille des blocs, et le réseau pourrait donc subir une modification de cette limite sans qu'ils s'en rendent compte. C'est ce qui explique la stratégie des promoteurs de SegWit2X en 2017, qui prévoyaient de doubler la taille limite des blocs sans protection contre la rediffusion afin que les portefeuilles à vérification de paiement simplifiée suivent simplement la chaîne la plus longue.

Satoshi pensait que le système pourrait perdurer avec une vérification centralisée entre les mains de quelques nœuds vérificateurs (dont les mineurs) et que le reste des utilisateurs ferait usage des clients légers. Dans sa première réponse à James A. Donald en novembre 2008, il indiquait ainsi :

> « Bien avant que le réseau n'atteigne cette taille, les utilisateurs pourront utiliser la vérification de paiement simplifiée (section 8) pour contrôler les doubles dépenses, ce qui ne nécessite que la chaîne des entêtes de bloc, soit environ 12 Ko par jour. Seules les personnes essayant de créer de nouvelles pièces auront besoin de faire fonctionner des nœuds de réseau [12]. »

En cela, il se trompait. La vérification des règles de consensus a besoin d'être intégrale pour que celles-ci soient appliquées.

C'est donc au niveau du nœud complet que se joue cette vérification, une réalité qui est parfois retranscrite par l'adage « pas ton nœud, pas tes règles [13] ». Ne faites pas confiance, vérifiez ! Un peu comme une langue résulte des choix que font ses locuteurs, un protocole informatique résulte des règles appliquées par les nœuds complets. Cette vérification joue donc un rôle crucial dans la détermination du protocole.

Les hard forks

Puisque Bitcoin est ouvert et libre, les règles de consensus peuvent être modifiées à volonté par les nœuds du réseau au moyen d'un changement d'acceptation des blocs et des transactions. Ces modifications peuvent mener à des conflits sur le réseau, et éventuellement à la séparation en deux réseaux distincts gérant chacun sa propre chaîne et sa propre monnaie. D'où l'utilisation du mot *fork*, qui signifie « embranchement », « bifurcation » ou « fourche » en français, pour parler de ce phénomène.

Les modifications des règles de consensus sont couramment rangées en deux catégories : celle des *hard forks*, qui constituent des mises à niveau brutes et incompatibles, et celle des *soft forks*, qui présentent une certaine rétrocompatibilité. Voyons comment ces changements se manifestent, en commençant par les hard forks, avant de décrire les soft forks.

Dans Bitcoin, il existe une polysémie au sujet du mot *fork*, qui possède quatre significations différentes : le fork logiciel, le fork de règles de consensus, le fork de chaîne commun et le fork de chaîne persistant. Cette polysémie prête à confusion de sorte qu'on préfère utiliser un terme différent pour chacun de ces sens.

Comme on l'a dit, le mot fork est d'abord utilisé dans le développement logiciel, notamment dans le cadre du logiciel libre qui autorise et encourage ce type de pratique. Il désigne la création d'un programme dérivé du code source d'un programme existant et aussi, par abus de langage, le programme dérivé en lui-même. En ce sens, l'implémentation de référence peut subir un embranchement, créant un logiciel alternatif. Ce logiciel peut respecter les règles de consensus (comme par exemple Bitcoin Knots), mais il peut aussi les faire dévier, en créant un nouveau protocole qui partage l'historique de la chaîne (Bitcoin ABC, devenu Bitcoin Cash Node) ou non (Litecoin).

Le fork peut ensuite désigner l'embranchement commun de la chaîne de blocs, par analogie avec le développement logiciel. La chaîne de blocs n'est

en effet pas une structure linéaire, mais une « structure en forme d'arbre [14] » qui peut posséder de multiples branches de blocs, pareillement compatibles avec les règles de consensus acceptées par le réseau, la sélection de la branche correcte se faisant par la plus longue (possédant le plus de travail accumulé). Ce type d'embranchement se produit régulièrement dans Bitcoin de manière tout à fait normale et bénigne, lorsque deux mineurs trouvent simultanément un bloc différent de leur côté, et est résolu lorsqu'un nouveau bloc est trouvé.

Le fork peut aussi se rapporter à une scission de la chaîne de blocs causée par une incompatibilité des règles de consensus. On parle alors de hard fork ou d'« embranchement divergent ». Cette scission est généralement permanente dans le sens où les deux branches ne peuvent pas se réconcilier par le mécanisme de consensus de Nakamoto, sauf dans un cas très précis : si les règles de la branche majoritaire forment une sous-partie restrictive des règles de la branche minoritaire. Les deux chaînes résultantes sont, à terme, vouées à exister sur des réseaux séparés.

Enfin, le terme fork peut, par métonymie, désigner une modification des règles de consensus, qui est toujours susceptible de provoquer une scission de chaîne et une séparation du réseau. Une restriction des règles de consensus est appelée un soft fork, ou « embranchement convergent », en vertu de sa capacité à résulter en une branche unique. Toute autre modification des règles de consensus, qu'il s'agisse d'une extension ou d'une modification strictement incompatible, est appelée un hard fork, en référence à sa propension à créer une scission de chaîne. C'est de ces deux modifications dont nous voulons parler ici [15].

Le hard fork est le concept le plus ancien si on le compare au soft fork. Il était auparavant qualifié de « changement incompatible [16] ». Le hard fork est une modification non restrictive des règles de consensus. Il provoque un conflit sur le réseau entre les nœuds qui appliquent les anciennes règles et les nœuds qui appliquent les nouvelles.

Un hard fork peut être extensif, c'est-à-dire élargir les règles de consensus sur les blocs et les transactions. Les anciens peuvent ainsi produire des blocs valides sur la nouvelle chaîne, mais pas l'inverse. L'exemple typique de ce genre de hard fork est l'augmentation de la taille limite des blocs, qui consiste à accepter des blocs ayant une taille ou un poids plus grand, comme 2 Mo au lieu de 1 Mo ou 8 MWU à la place de 4 MWU. Ce hard fork extensif est illustré sur la figure 10.2.

Dans le cas où le hard fork extensif n'est pas soutenu par une majorité de la puissance de calcul du réseau, celui-ci risque de ne pas créer une branche

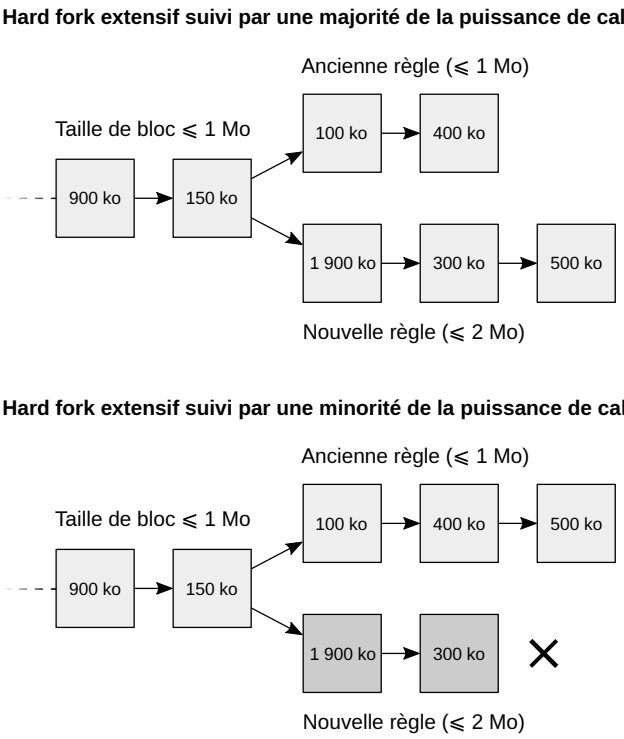

FIGURE 10.2 – Schéma d'un hard fork extensif : si la chaîne suivant la nouvelle règle est plus longue que celle suivant l'ancienne, les deux chaînes persistent ; dans le cas contraire, seule la deuxième survit.

persistante. Par exemple, les blocs de la branche imposant une limite de taille plus petite sont entièrement compatibles avec les nouvelles règles, de sorte que, si elle est plus longue, c'est elle qui sera sélectionnée comme la branche correcte. C'est pour éviter cette situation problématique que les hard forks sont généralement bilatéraux.

Le hard fork bilatéral est un hard fork qui crée une incompatibilité totale entre les nouvelles règles et les anciennes. Il peut s'agir d'une règle ajoutée comme l'exigence que le premier bloc de l'embranchement inclue un changement incompatible. Dans notre cas de l'augmentation de la taille limite des blocs, il s'agirait d'imposer au premier bloc d'être strictement plus gros que la taille limite précédente, comme on le voit sur la figure 10.3. Cette règle supplémentaire est appelée protection contre la destruction par recoordination (ou *wipeout protection* en anglais).

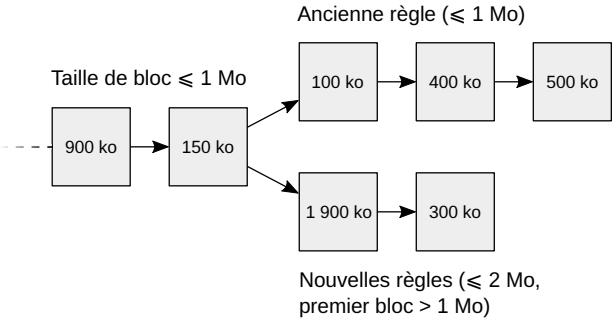

FIGURE 10.3 – Schéma d'un hard fork bilatéral : les nouvelles règles sont strictement incompatibles avec les anciennes règles, de sorte que les deux chaînes persistent.

Un autre exemple est le changement de l'algorithme de signature des transactions, qui rend l'intégralité des transactions signées et des blocs non vides strictement incompatibles. Ce changement a pour effet de permettre en plus une protection contre la rediffusion des transactions (*replay protection*), dans le cas où deux chaînes concurrentes persisteraient.

Deux situations peuvent découler d'un hard fork : soit la quasi-totalité de l'économie procède au changement, auquel cas une seule chaîne subsiste ; soit l'économie se fragmente, auquel cas les deux chaînes persistent. La première situation est visée par le hard fork de mise à niveau qui n'a pas vocation à créer deux chaînes distinctes. La seconde est désirée par le hard fork contentieux, résultant d'une division de la communauté au sujet du changement. Le hard fork accidentel, créé par une modification non désirée des règles de consensus implicites, est écarté ici [17].

Le hard fork de mise à niveau est un hard fork qui nécessite une synchronisation de la quasi-totalité de la communauté. Il résulte généralement en une seule chaîne, de sorte qu'on peut considérer que le protocole a été mis à niveau, alors qu'il s'agit essentiellement d'une utilisation économique qui passe d'un protocole à un autre. Il peut pour cela être extensif, même si la bilatéralité est préférée pour des raisons de sécurité.

Le premier hard fork de mise à niveau connu est probablement l'ajout des codes opération `OP_NOP` à la version 0.3.6 de Bitcoin par Satoshi Nakamoto en juillet 2010. L'augmentation de la taille des blocs était également pensée comme un hard fork de mise à niveau, notamment par Satoshi lui-même [18], jusqu'au hard fork contentieux de Bitcoin Cash en 2017.

En dehors de BTC, les mises à niveaux par hard fork sont nombreuses, notamment en raison d'une économie moins grande et / ou plus centralisée.

On peut citer les cas de Bitcoin Cash, de Monero, d'Ethereum Classic et d'Ethereum, où des mises à niveau de ce type sont réalisées régulièrement.

Le hard fork contentieux est un hard fork visant délibérément à créer une nouvelle chaîne. Il est issu d'une dissension dans la communauté, qui est si forte qu'elle pousse à la sécession. Il est généralement bilatéral.

Le premier exemple de hard fork contentieux majeur est celui qui a eu lieu sur Ethereum en juillet 2016, dans le contexte du piratage de TheDAO. Ce hard fork consistait à reprendre les fonds du pirate par un « changement d'état irrégulier ». Celui-ci était rendu bilatéral par la règle imposant aux 10 premiers blocs d'inclure la chaîne de caractères `dao-hard-fork`. Puisque la majorité économique se trouvait du côté de l'annulation, la chaîne altérée a gardé le nom d'Ethereum et le sigle boursier ETH, tandis que l'autre chaîne a pris le nom d'Ethereum Classic et le sigle boursier ETC.

Le second exemple de hard fork contentieux est celui qui a mené à la création de Bitcoin Cash en août 2017 suite au débat sur la scalabilité et à la guerre des blocs. Ce hard fork n'intégrait pas SegWit, augmentait la taille limite des blocs à 8 Mo et améliorait l'algorithme de signature. Il était rendu bilatéral par une règle qui imposait au bloc suivant l'activation d'avoir une taille strictement supérieure à 1 Mo. Il offrait aussi *de facto* une protection contre la rediffusion des transactions. Ce changement ayant dû se faire sans l'accord de la majorité économique, la chaîne qui ne modifiait pas les règles a pu conserver le nom de Bitcoin et le sigle boursier BTC, tandis que la nouvelle chaîne a dû adopter un nouveau nom, Bitcoin Cash, et un nouveau sigle, BCH.

Notez qu'un tel hard fork peut être amené à modifier l'algorithme d'ajustement de la difficulté. En effet, si la puissance de calcul est trop faible pour le soutenir, il est possible que l'ajustement n'arrive pas à terme. C'est pour cette raison que Bitcoin Cash a dû implémenter un *Emergency Difficulty Adjustment* (EDA) qui a permis de procéder à l'adaptation sur une période plus courte. Ethereum Classic n'a cependant pas dû le faire, car l'ajustement sur Ethereum avait déjà lieu à tous les blocs.

Les soft forks

Passons maintenant au soft fork, qui est un procédé de mise à niveau souvent mal compris. Le soft fork est une restriction des règles de consensus. Il consiste ainsi par essence à rendre l'ensemble des blocs et des transactions valides plus petit, en ajoutant une règle ou en modifiant une règle existante de façon plus restrictive. L'exemple typique de ce genre de fork est la diminution de la taille limite des blocs. L'ajout de la limite explicite des 1 Mo en octobre

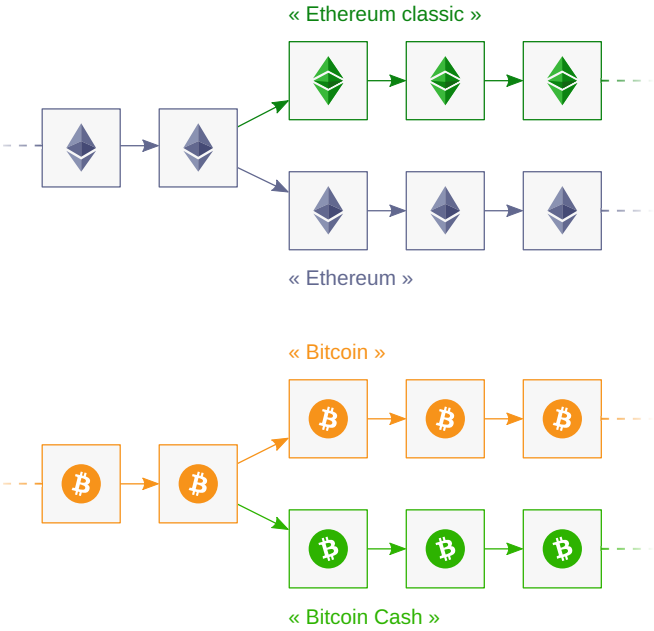

FIGURE 10.4 – Exemples de hard forks bilatéraux : ETH / ETC et BCH / BTC.

2010 était de ce fait un soft fork.

Le soft fork peut être appliqué en conservant une seule et même chaîne. S'il est imposé par la majorité de la puissance de calcul du réseau, il n'y a aucun risque de scission. En effet, l'ensemble des blocs créés par les mineurs qui appliquent les nouvelles règles est entièrement compatible avec les anciennes règles, de sorte que la branche appliquant les nouvelles règles sera considérée comme la branche correcte par tous les nœuds si elle est majoritaire. Si l'application du soft fork est en revanche minoritaire, alors ce dernier résulte en deux chaînes persistantes distinctes. Les deux cas de figure sont illustrés sur la figure 10.5.

Le concept de soft fork est postérieur à celui de hard fork. Il a été formellement découvert par Gavin Andresen en octobre 2011 qui, suite à son étude de la proposition d'ajout du code opération `OP_EVAL` par Nicolas van Saberhagen [19], s'est aperçu que la mise à niveau pouvait se faire grâce au code opération `OP_NOP1` sans nécessairement provoquer de scission [20].

Les codes opération `OP_NOP` sont des instructions du langage de script de Bitcoin qui ont été ajoutés dans le code par Satoshi en juillet 2010 avec pour seul commentaire « expansion [21] ». Le changement a été rendu effectif

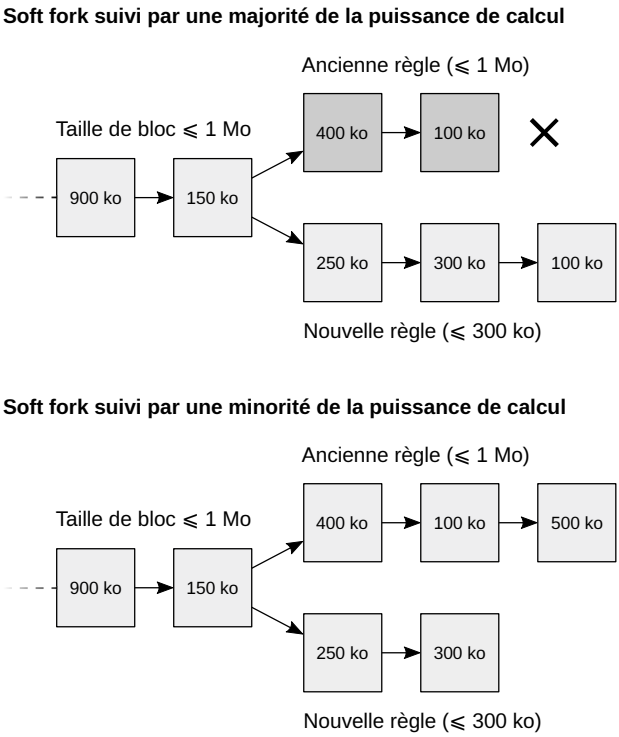

FIGURE 10.5 – Schéma d'un soft fork : si la chaîne suivant la nouvelle règle est plus longue que celle suivant l'ancienne, seule la première survit ; dans le cas contraire, les deux chaînes persistent.

avec la version 0.3.6 du logiciel qui corrigeait également le 1 RETURN bug, publiée le 29 juillet. Leur rôle est initialement muet : s'ils sont présents dans un script, ils ne font rien mais ils n'invalident pas la transaction non plus. La conséquence directe est qu'on peut modifier le comportement de ces codes opération sans rendre les scripts incompatibles avec les anciennes règles de consensus. L'ajout de cette caractéristique indique donc que Satoshi avait saisi le mécanisme du soft fork.

Le soft fork possède un caractère « rétrocompatible » – ou postcompatible à proprement parler, car la compatibilité est ascendante et non descendante – dans le sens où les anciennes versions du logiciel peuvent continuer d'interagir avec le système. En effet, les nœuds non miniers suivant les anciennes règles continuent de voir les blocs produits comme valides. Cette caractéristique est un avantage majeur par rapport au hard fork.

Mais cette compatibilité ascendante ne veut pas dire qu'un soft fork est « doux ». Il possède un côté pernicieux dans le sens où il rend la modification difficile à appréhender. Le soft fork présente ainsi plusieurs inconvénients.

D'abord, il n'est pas optionnel. S'il est appliqué par la majorité de la puissance de calcul, un soft fork s'apparente en effet à une attaque de censure pour les utilisateurs qui suivent les anciennes règles. Le soft fork possède donc un caractère coercitif que le hard fork n'a pas.

Puis, le soft fork est difficilement réversible. Les fonctionnalités ajoutées ne peuvent pas être désactivées simplement : une fois adopté, il n'y a pas de retour en arrière facile. Les développeurs de Bitcoin SV ont ainsi désactivé P2SH en février 2020 exposant les utilisateurs les moins attentifs à des vols.

Ensuite, le soft fork n'est pas limité quant à ce qu'il peut faire. Il peut augmenter la limite effective de taille des blocs (via un bloc auxiliaire aussi appelé bloc d'extension ou soft fork généralisé). Ce bloc d'extension peut également inclure des fonctionnalités supplémentaires (comme MimbleWimble dans Litecoin). Il peut même modifier la politique monétaire du protocole en redéfinissant l'unité de base [22].

Enfin, le soft fork, s'il est profond, crée une complexité supplémentaire, liée aux contraintes de son application. En effet, il ajoute de nouvelles exceptions aux règles de consensus, ce qui génère de la dette technique pour les développeurs.

L'archétype du soft fork profond et complexe a été la mise à niveau SegWit, ou *Segregated Witness*, qui consistait à déplacer les données de signature des transactions (appelées témoin ou *witness*) vers une structure de données séparée (*segregated*) afin de supprimer la malléabilité des transactions. Cette mise à niveau, qui a eu lieu le 24 août 2017, devait être initialement un hard fork, avant que le développeur Luke-Jr ne décrive en 2015 comment en faire un soft fork. La rétrocompatibilité était assurée par la liaison du témoin au bloc via un arbre de Merkle dont la racine était placée dans la transaction de récompense et par l'utilisation de sorties transactionnelles dépensables par n'importe qui (*anyone-can-spend*). Outre la correction du problème de malléabilité, elle a instauré un système de versionnage (qui a permis l'intégration de Schnorr-Taproot par la suite) et a modérément augmenté la capacité transactionnelle du réseau, de sorte que la taille effective des blocs pouvait dépasser 1 Mo, jusqu'à 4 Mo en théorie. Elle a également ajouté quatre nouveaux types d'adresse au protocole.

De plus, le soft fork requiert la majorité de la puissance de calcul du réseau pour préserver son intérêt. S'il n'est pas suivi à moyen terme par 51 % de la

puissance de calcul, alors son application provoque une scission. C'est ce qui explique pourquoi l'activation par les mineurs est généralement préférée à l'activation par les utilisateurs, même si le pouvoir de décision revient à ces derniers comme on le verra dans le chapitre 11.

D'une part, le soft fork activé par les utilisateurs (en anglais *user activated soft fork* ou UASF) consiste à implémenter le soft fork dans le code source du logiciel de sorte à ce qu'il rentre en application à une hauteur de bloc ou à un horodatage donné. Cette méthode s'appuie sur la confiance que l'économie appliquant la mise à niveau sera largement majoritaire et que l'activité minière suivra à moyen terme en raison d'une récompense de bloc plus élevée.

D'autre part, le soft fork activé par les mineurs (en anglais *miner activated soft fork* ou MASF) consiste à faire dépendre l'activation du signalement des mineurs au sein des blocs validés. Il est activé lorsqu'un certain seuil de signalement (95 % par exemple) est dépassé. Cette méthode, dont la procédure a été notamment décrite dans le BIP-9, permet de s'assurer autant que possible que les mineurs appliquent la mise à niveau et qu'il ne subsiste qu'une seule chaîne.

La même distinction existe dans l'activation des hard forks, mais celle-ci a peu de pertinence, la puissance de calcul ne pouvant pas empêcher la scission. Ainsi, le hard fork activé par les mineurs ou MAHF, longtemps soutenu par les partisans de l'augmentation de la taille limite des blocs, n'a pas d'intérêt particulier. Comme les hard forks, les soft forks peuvent être rangés en deux catégories plus ou moins distinctes : le soft fork de mise à niveau et le soft fork contentieux. Le soft fork est idéal pour mettre à niveau le protocole. Cela permet aux nœuds de ne pas se mettre à niveau tout de suite. Même s'il demande une certaine synchronisation, celle-ci n'est pas aussi contraignante que pour les hard forks.

Dans BTC, le soft fork est ainsi privilégié par les développeurs depuis sa découverte. De nombreuses mises à niveau en étaient, comme *Pay to Script Hash* (BIP-16), ou l'obligation de spécifier la hauteur du bloc dans la transaction de récompense (BIP-34), ou encore l'ajout d'un standard d'encodage des signatures (BIP-66). Les ajouts des codes opération `OP_CHECKLOCKTIMEVERIFY` et `OP_CHECKSEQUENCEVERIFY` permettant l'usage de verrous temporels dans le langage de script par l'utilisation respective des codes `OP_NOP2` et `OP_NOP3` ont également été des soft forks. Enfin, plus récemment, l'adoption de Schnorr-Taproot (ou Taproot pour faire court) a été une mise à niveau par soft fork.

Litecoin fait aussi usage de ce type de transition. Le protocole a notamment

intégré SegWit en mai 2017, ainsi que Schnorr-Taproot et MimbleWimble (MWEB) en mai 2022.

Le soft fork contentieux a pour objectif de contraindre la minorité de la communauté à suivre la majorité. S'il réussit, il n'y a qu'une seule chaîne, les opposants ayant le choix d'accepter les règles ou de procéder eux-mêmes à un hard fork. S'il échoue, il en résulte deux chaînes concurrentes.

SegWit est l'exemple typique d'un soft fork contentieux réussi. Il n'était pas approuvé par l'ensemble des acteurs importants (les partisans des gros blocs d'une part, les puristes du protocole comme Mircea Popescu d'autre part [23], s'y opposaient), mais il a recueilli un soutien majoritaire de sorte qu'il a pu perdurer et que les *big blockers* mécontents ont dû migrer vers Bitcoin Cash.

Un exemple de soft fork contentieux ayant échoué est la tentative de l'équipe de Bitcoin ABC d'imposer une redirection de 8 % de la subvention de minage de Bitcoin Cash à son propre profit le 15 novembre 2020 [24]. Cette tentative, qui était un soft fork en raison de son caractère restrictif, a provoqué la scission entre une branche majoritaire sans redirection (BCH) et une branche minoritaire avec, qui a été par la suite renommée en « eCash » (XEC).

Ainsi, le soft fork, qu'il soit approuvé à l'unanimité ou bien seulement par une majorité, est une méthode supérieure au hard fork. Bien qu'il soit parfois plus complexe, il permet de ne pas requérir une synchronisation de l'économie entière, cette dernière pouvant s'y adapter progressivement, ce qui est un bienfait non négligeable dans le cas d'un système ouvert utilisé par une grande diversité de personnes comme Bitcoin. Le signalement supermajoritaire des mineurs permet de minimiser le risque de scission et de conserver l'effet de réseau au maximum.

Mais cet avantage majeur se fait au prix d'un sacrifice : celui de la clarté du consentement. Dans le cas du hard fork, le consentement est clair : les personnes qui souhaitent la modification se retrouvent sur la chaîne qu'elles ont choisie. Dans le cas du soft fork, le consentement est plus ambigu : le fait d'opérer sur la chaîne n'indique pas nécessairement une acceptation active du changement, mais une résignation passive et un refus de réaliser un hard fork minoritaire. Comme l'écrivait brillamment Vitalik Buterin en mars 2017 :

> « Les soft forks favorisent clairement la coercition par rapport à la sécession d'un point de vue systémique, alors que les hard forks ont le penchant inverse [25]. »

Ainsi, même s'ils sont supérieurs de manière générale, les soft forks ne sont pas adaptés à toutes les situations.

L'évolution plurielle de Bitcoin

Le fonctionnement ouvert et libre de l'évolution de Bitcoin fait que le protocole peut être modifié à volonté. Bitcoin évolue de manière organique, lentement mais sûrement : il n'est pas un système figé, dont les règles seraient dictées par une autorité centrale. Et, par là, il s'améliore avec le temps.

Cette ouverture implique aussi que la mise en œuvre de Bitcoin est nécessairement plurielle. Bitcoin n'est pas un système unique, mais un modèle ouvert qui est appliqué de façon plus ou moins fidèle par plusieurs protocoles. L'ensemble des mises en œuvre de Bitcoin constitue un arbre dont les branches proviennent d'un même tronc et des mêmes racines.

Toutefois, toutes les branches ne sont pas équivalentes : toutes les mises en œuvre n'ont pas la même importance. L'une d'entre elles (BTC) est aujourd'hui supermajoritaire, de sorte que nous l'appelons naturellement Bitcoin, et sa modification est (heureusement) difficile. Dans le prochain chapitre, nous examinerons le mécanisme sous-jacent qui fait que Bitcoin est ce qu'il est aujourd'hui et comment l'évolution du protocole est gouvernée.

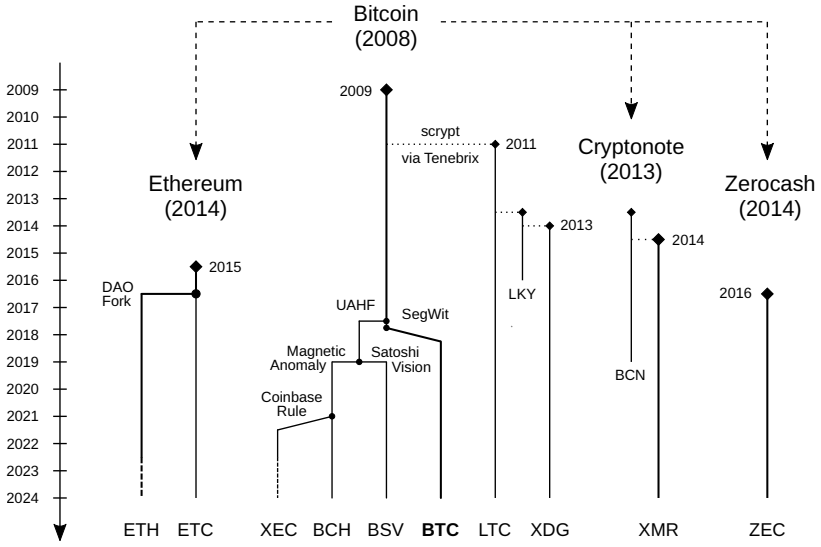

FIGURE 10.6 – Variations conceptuelles, modifications logicielles et forks de consensus de Bitcoin.

11

La détermination du protocole

Dans Bitcoin, le protocole est l'ensemble ouvert de règles qui interviennent dans la formation et la transmission des blocs et des transactions sur le réseau. Il est notamment constitué des règles de consensus qui régissent la validité du registre sur lequel les nœuds du réseau se mettent d'accord. Ces règles sont mises en œuvre par des implémentations logicielles, qui peuvent être librement copiées, modifiées et réutilisées à volonté.

Cette nature ouverte et libre fait qu'il n'y a pas d'autorité centrale qui décrète quelles sont les règles comme cela se fait dans les modèles centralisés, mais que cette prise de décision est répartie au sein de la communauté. C'est pourquoi la détermination du protocole n'est pas un mécanisme technique mais économique, conformément à la nature essentiellement monétaire de Bitcoin.

Il s'agit d'un thème d'importance majeure, car ce mécanisme de détermination garantit l'intégrité des règles de consensus et, par conséquent, le bon fonctionnement du système. En particulier, c'est de lui que provient la fameuse résistance à l'inflation, à savoir la difficulté à créer plus de bitcoins. Il est donc fondamental d'avoir une bonne conception de ce mécanisme si nous voulons nous convaincre de la viabilité de Bitcoin.

La résistance à l'inflation

L'une des deux grandes promesses de Bitcoin est de résister à l'inflation monétaire, c'est-à-dire de rendre difficile la création supplémentaire d'unités par rapport à ce qui est accepté par le marché. Cette promesse est énorme : comme nous l'avons vu dans le chapitre 4, l'État fait tout ce qu'il peut pour profiter de la création monétaire, phénomène qu'on appelle le seigneuriage. De prime abord, il paraît ainsi étonnant qu'un objet numérique puisse posséder une telle propriété.

La politique monétaire classique du bitcoin a été établie par Satoshi Nakamoto lors du lancement du prototype le 8 janvier 2009. Celle-ci possédait un caractère simple : la création monétaire devait être réduite de moitié tous les quatre ans, de façon à devenir négligeable au fil du temps. Il devait se créer 10,5 millions d'unités de manière linéaire les quatre premières années, 5,25 millions les quatre suivantes, 2,625 millions les quatre d'après, et ainsi de suite, ce qui limitait le nombre d'unités en circulation à 21 millions. Le bitcoin devait finir par devenir une monnaie à quantité fixe, quelque chose qui n'a jamais été vu dans l'histoire.

Cette politique monétaire a été l'un des arguments de vente de Bitcoin, si bien que certaines personnes se sont imaginées qu'il s'agissait d'une chose immuable, gravée dans le marbre, et que l'application mathématique de ce décret de Satoshi Nakamoto était ce qui garantissait la résistance à l'inflation du système. Par exemple, Tyler Winklevoss, ayant investi dans le bitcoin avec son frère jumeau Cameron, se convainquait en 2013 qu'il avait acheté un actif dépourvu d'intervention humaine :

> « Nous avons choisi de placer notre argent et notre confiance dans un cadre mathématique exempt de politique et d'erreur humaine [1]. »

Toutefois, cette conception est au mieux une approximation maladroite. Il ne suffit pas qu'une règle ait été décrétée par quelqu'un dans le passé pour qu'elle se manifeste dans la réalité présente ; il faut aussi que d'autres personnes l'acceptent et l'appliquent. Et cette acceptation est précisément soumise à la politique et à l'erreur humaine.

Il existe au sujet de la politique monétaire fixe du bitcoin une certaine confusion. Il faut dire que Satoshi Nakamoto n'a jamais précisé comment elle pouvait être protégée. Plusieurs théories ont été proposées, allant de l'intervention des mineurs à l'exigence d'unanimité communautaire, en passant par le caractère juridique du décret de Satoshi. Dans tous les cas, il s'agissait de traiter la question de la « gouvernance [2] » ou du « consensus social [3] »,

c'est-à-dire de la façon dont les règles sont décidées dans Bitcoin. C'est cette problématique que nous appelons ici la détermination du protocole.

Le pouvoir des commerçants sur le protocole

Tel que nous l'avons laissé entendre, la détermination du protocole est accomplie par l'économie. Puisque Bitcoin est un système économique, il est naturel que les règles qui le composent résultent du marché, et non d'un décret fixe passé ou d'une autorité centrale actuelle.

L'idée que l'économie permet de déterminer les règles n'est pas nouvelle. Elle remonte au moins au printemps 2012 lorsque Meni Rosenfeld écrivait sur Stack Overflow qu'un changement du protocole nécessitait « une majorité économique, c'est-à-dire l'adoption par les utilisateurs et les entreprises qui donnent de la valeur à la monnaie [4] ». Gavin Andresen lui-même a mis en avant cette idée en mai 2015, alors que la question d'augmenter la taille limite des blocs se posait :

> « Si nous ne parvenons pas à un consensus ici, l'autorité ultime pour déterminer le consensus est le code utilisé par la majorité des commerçants, des plateformes de change et des mineurs [5]. »

Mais la clarté de cette conception n'est arrivée qu'après les évènements de la guerre des blocs, au cours de laquelle les mécanismes sous-jacents ont pu s'exprimer. Ce n'étaient pas les développeurs qui décidaient des règles, ce n'étaient pas les mineurs non plus, mais plutôt les utilisateurs, et plus précisément les *commerçants*. Eric Voskuil écrivait ainsi en novembre 2018 :

> « Bitcoin ne repose pas sur un dépositaire, mais dans l'intérêt d'établir un principe général, on peut considérer l'ensemble de tous les commerçants comme le dépositaire collectif de Bitcoin [6]. »

Les commerçants, au sens large, sont les personnes qui fournissent des biens, des services ou d'autres monnaies contre du bitcoin, à des prix acceptables sur le marché. Cette prestation se manifeste par les échanges effectifs avec les clients et s'estime par les recettes perçues. En cela, les commerçants contribuent à l'utilité du bitcoin, qui se mesure à la quantité de biens et de services qu'il permet d'acquérir, et par conséquent à l'importance économique de la chaîne [7]. Par l'utilisation d'un nœud permettant de vérifier les règles de consensus, ils participent ainsi à la détermination du protocole en proportion de leur activité économique potentielle.

Parler d'un protocole unique qui changerait est une inexactitude : en tant qu'ensemble de règles, les protocoles sont tous fixes, mais leur utilisation (et

leur utilité) varie. Modifier le protocole consiste donc à constituer un nouveau protocole dont la chaîne résultante sera économiquement plus importante que toute autre branche concurrente, y compris celle liée au protocole originel [8]. Par exemple, SegWit a été un soft fork contentieux, mais le protocole résultant a été beaucoup plus valorisé que les protocoles concurrents (BTC pré-SegWit et Bitcoin Cash), de sorte qu'on peut dire que le protocole BTC a été mis à niveau par cette modification.

Bitcoin-le-concept englobe par nature une multiplicité de protocoles, en raison de son caractère libre et ouvert. Il n'y a pas un seul protocole Bitcoin, mais plusieurs, comme il y a plusieurs distributions Linux ou plusieurs dollars. Et ces protocoles sont en concurrence pour acquérir une utilité en étant adoptés par les commerçants.

Ce qui compte, c'est donc l'importance économique des chaînes créées par ces protocoles. Chacun peut bien définir Bitcoin comme il le souhaite, notamment en décrétant qu'il n'y a qu'un seul protocole et qu'il ne peut pas être modifié sans unanimité, mais cette attitude ne change pas la réalité économique des choses. Si la chaîne créée par une modification rassemble 80 % de l'activité économique, la chaîne suivant les règles du protocole originel continuerait d'exister, mais serait lourdement déclassée et perdrait en pertinence. Comme l'écrivait Arthur Breitman en 2014, « l'option de s'en tenir au protocole originel n'est pas du tout pertinente si la valeur de ses jetons est annihilée par un changement de consensus [9] ».

Tout ceci explique les usages qui se sont développés naturellement dans l'écosystème. On appelle usuellement Bitcoin la mise en œuvre principale et dominante économiquement du concept. En cas de scission, le nom et le sigle boursier du protocole originel sont généralement conservés par la branche majoritaire, que celle-ci garde les règles initiales (Bitcoin-BTC) ou qu'elle les modifie (Ethereum-ETH) ; tandis que la branche minoritaire doit modifier son propre nom, soit en le rallongeant pour insister sur la continuité (Bitcoin Cash, Bitcoin SV, Ethereum Classic), soit en le remplaçant par une nouvelle marque (« eCash » / XEC).

Cette mécanique économique fait que la résistance au changement provient des commerçants qui refusent d'intégrer les règles. Ainsi, une modification qui amoindrirait les propriétés fondamentales de Bitcoin, comme une introduction de censure ou d'inflation, ne serait effective que si les commerçants l'acceptaient. Or ceux-ci sont récompensés par ces propriétés en bénéficiant de la liberté liée à l'absence de censure (permettant notamment l'évasion fiscale) et de l'augmentation en pouvoir d'achat des fonds reçus, et sont par

conséquent incités à ne pas accepter un tel changement. En particulier, la « déflation naturelle [10] » du bitcoin forme l'incitation économique qui maintient sa politique monétaire singulière.

À l'instar de la sécurité minière, la sécurité commerciale d'une chaîne, c'est-à-dire la difficulté à en modifier les propriétés fondamentales, ne dépend pas uniquement de l'activité économique de la chaîne (les recettes), mais aussi de la distribution de cette activité économique et du nombre de commerçants par rapport au reste de la population mondiale [11]. Une activité économique concentrée dans les mains d'un seul acteur rend très facile toute modification du protocole. De même, si l'activité économique est élevée et équitablement répartie entre un petit nombre de commerçants, alors le protocole a plus de chances d'être modifié qu'en présence d'un grand nombre de commerçants.

Tout comme les mineurs qui délèguent leur pouvoir sur la sélection des transactions (« hacheurs »), les commerçants peuvent déléguer leur pouvoir sur la vérification des règles de consensus. Les commerçants abandonnent ce pouvoir aux services délégataires à qui ils versent une commission dans le but de réduire la difficulté d'utilisation (le déploiement d'un nœud) et le coût de transaction (lié aux remises des frais). Ces services délégataires peuvent être des fournisseurs de portefeuille (Electrum, Acinq, Edge, Ledger, Trezor), des processeurs de paiement (BitPay, Coinbase Commerce) ou même des explorateurs de blocs (Blockchair, Mempool.space).

La délégation de la vérification pose un problème évident de centralisation. Même si l'économie peut s'adapter rapidement et redevenir saine à moyen terme par le déploiement de nouveaux nœuds, la sécurité commerciale instantanée de la chaîne est affectée par cette délégation et une attaque de modification ou de suppression du protocole peut causer des dégâts à court terme non négligeables.

Cet impact peut être d'autant plus fort si la délégation s'accompagne d'une délégation de la propriété auprès d'un dépositaire, auquel cas le réel commerçant devient le dépositaire en question, celui-ci ayant un contrôle total sur les fonds. C'est notamment le cas des places de marché en ligne qui achètent et vendent d'autres monnaies en bitcoins, tout en mettant en place des carnets d'ordres internes pour résoudre l'offre et la demande.

À l'heure d'écriture de ces lignes, la situation dans Bitcoin est particulière, car l'activité économique est dominée par le change entre le bitcoin et les monnaies officielles. Déjà à l'époque de Satoshi, les changeurs constituaient les premiers commerçants de Bitcoin : la première chose achetée avec du bitcoin n'était pas une pizza comme on aime le penser, mais de la monnaie,

à savoir 5,02 dollars sur PayPal [12]. Aujourd'hui, les plateformes de change centralisées telles que Kraken, Coinbase et Binance ont pris la relève, ce qui fait que l'économie est aujourd'hui extrêmement centralisée et sensible aux attaques.

Comme dans le cas de l'attaque de censure, l'attaque d'altération des propriétés fondamentales de Bitcoin ne risque pas de provenir d'un acteur économique rationnel, qui n'a aucun intérêt à le faire, mais plutôt d'agents politiques agissant au nom de l'État. La nature d'une telle attaque répondrait donc aux prérogatives étatiques comme la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) ou bien l'opposition à la spéculation contre la monnaie nationale. Les plateformes de change, hautement réglementées seraient les premières concernées par une telle attaque.

Ainsi, ce sont les commerçants qui déterminent le protocole en choisissant les règles de consensus qui leur conviennent, qu'ils vérifient systématiquement par l'intermédiaire de leurs nœuds. Le pouvoir individuel du commerçant est pondéré par son offre économique susceptible d'être acceptée, qui est estimée par son activité économique réelle. Cependant, ce pouvoir n'est pas linéaire, dépendant en particulier de l'effet de réseau.

L'effet de réseau

Le pouvoir direct d'un commerçant n'est pas purement individuel. Bitcoin étant une monnaie, il est soumis à des effets économiques, dont le principal est l'effet de réseau. Ce dernier fait qu'il y a un nombre moins élevé de mises en œuvre de Bitcoin que ce qu'on attendrait pour un produit matériel classique.

L'effet de réseau est le phénomène par lequel l'utilité réelle d'une technique ou d'un produit dépend de la quantité de ses utilisateurs. Il s'agit d'un effet qui s'auto-alimente, qui fonctionne comme un cercle vertueux : plus un système compte d'utilisateurs, plus il a tendance à en attirer de nouveaux.

Une monnaie est un réseau social et est donc soumise à l'effet de réseau. L'utilité globale du réseau n'évolue pas de façon linéaire par rapport à la taille de son économie, mais de façon superlinéaire. C'est ce qu'exprime la loi de Metcalfe qui stipule que « l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs [13] ».

Lors de l'émergence d'Internet, la demande pour un protocole commun a fait que TCP/IP a prévalu sur le modèle concurrent de l'époque, le modèle OSI. De même, seul un nombre réduit de langues peut exister en raison des contraintes induites par la communication. En ce qui concerne les relations

commerciales et diplomatiques internationales, il n'y a ainsi généralement qu'une seule langue véhiculaire (« *lingua franca* ») au sein d'une aire géographique donnée. C'était le cas de l'araméen et le grec de la koinè au Proche-Orient durant l'Antiquité, de l'italien en Europe au début de la Renaissance, du français comme langue diplomatique aux XVIII^e^ et XIX^e^ siècles, et c'est le cas de l'anglais dans le monde aujourd'hui.

Pour la monnaie, cet effet provient de la préférence personnelle pour une seule monnaie, qui s'explique d'une manière interne par le coût (mental) du calcul économique qui découle de la gestion de plusieurs monnaies, et d'une manière externe par le coût de change qui est payé pour la conversion d'une monnaie en une autre. De ce fait, les individus ont tendance à privilégier l'usage de la monnaie la plus populaire, quand bien même celle-ci serait défectueuse. C'est également ce qui fait qu'une monnaie utilisée par un petit nombre de personnes doit présenter un avantage non négligeable par rapport aux autres si elle veut perdurer. Avec le temps, les monnaies tendent à se consolider en une seule, même s'il subsiste des barrières à ce résultat.

Dans Bitcoin, l'effet de réseau monétaire prédomine. Même s'il n'est pas le seul effet de réseau, il est celui qui conduit les autres effets (liés à la liquidité, au développement informatique, à la sécurité économique et à la communication mercatique) à s'exprimer [14].

L'effet de réseau joue ainsi un rôle *capital* dans la détermination du protocole. L'existence d'un nombre limité de mises en œuvre viables de Bitcoin et leur stabilité provient de cet effet. C'est ce qui explique pourquoi l'existence d'une supermajorité économique est souvent exigée avant de procéder à une modification du protocole. C'est également ce qui encourage l'ossification du protocole qui se bâtit face à la multiplication des propositions de changement. Il existe un point de Schelling naturel qui s'oppose à l'altération des règles de consensus [15] : en l'absence de volonté claire de modifier les règles ou dans le cas d'une dispute, l'option de ne rien faire est privilégiée.

L'existence de l'effet de réseau explique la tendance au maximalisme qui se manifeste au sein de communautés liées à des protocoles et unités de compte particulières. Puisqu'il ne doit y avoir (logiquement) qu'un seul Bitcoin, toute tentative de faire varier le concept s'apparente à une démarche vaine et contreproductive, sinon à une escroquerie. Mais le maximalisme ignore en cela l'effet de substitution.

L'effet de substitution

Le second effet économique principal qui agit sur le pouvoir individuel des commerçants est l'effet de substitution. Celui-ci s'oppose diamétralement à l'effet de réseau, et a pour conséquence de créer un nombre plus élevé de mises en œuvre de Bitcoin que ce à quoi on pourrait s'attendre si le concept n'était pas naturellement limité.

Un produit de substitution est, en économie, un bien ou un service qui peut être utilisé dans le même but qu'un autre, mais qui présente des caractéristiques différentes de ce dernier. L'idée est que le consommateur va demander le produit de substitution parce que celui-ci est moins cher ou plus efficace dans la satisfaction apportée. Les exemples sont nombreux : le blé ou le riz pour l'apport en glucides, le café et le thé pour la consommation de caféine, le train et l'avion pour le transport en commun, etc. La substitution est généralement imparfaite, dans le sens où le produit va posséder des différences ne pouvant pas être quantifiées.

L'effet de substitution se manifeste lorsque les conditions de marché changent de manière drastique. Le produit de base peut devenir plus cher, ou moins abondant ; il peut devenir moins cher, ou plus abondant ; ou bien le niveau de vie des gens peut augmenter ou baisser de telle sorte qu'ils se mettent à préférer un produit à l'autre. Dans tous les cas, il faut qu'un changement arrive pour que la substitution se produise.

Cet effet de substitution se retrouve également dans les monnaies, et peut s'exprimer par exemple lorsque la monnaie officielle s'effondre, dans les pays en hyperinflation par exemple, ou qu'elle est interdite, comme dans les prisons. On observe alors un phénomène de monétisation des biens qui n'étaient initialement pas utilisés en tant que tels comme les voitures ou les cigarettes.

Avec Bitcoin, cet effet de substitution s'exerce de manière particulière. D'un côté, toute mise en œuvre de Bitcoin est limitée par un plafond de capacité transactionnelle, qui est souvent explicité par une taille ou un poids maximal des blocs [16]. De l'autre, le nombre de bitcoins est aussi limité. De ce fait, lorsque la demande d'activité monétaire augmente, il ne se crée pas plus de bitcoins, mais le coût d'inclusion dans un bloc augmente.

Cette particularité a pour effet d'exclure économiquement les transactions qui déplacent des sommes trop faibles pour que leur inscription sur la chaîne soit jugée rentable. Toutefois, la demande pour réaliser ces transferts ne disparaît pas. C'est pourquoi elle se retrouve partiellement sur des chaînes alternatives à bas frais, comme Litecoin ou Bitcoin Cash, dont la sécurité est moindre que celle de BTC [17].

De même, ce qu'on caractérise souvent par un manque de fonctionnalités dans Bitcoin-BTC correspond à une question de coût. Il est possible de simuler toutes les fonctionnalités présentes sur les autres chaînes d'une manière ingénieuse et détournée, mais il est bien moins coûteux et plus facile d'utiliser des protocoles qui les intègrent directement. C'est le cas de la confidentialité avec Monero, ou de la programmabilité générale avec Ethereum-ETH et Ethereum Classic.

Ainsi, l'effet de substitution joue un rôle important dans Bitcoin et dans les systèmes cryptoéconomiques en général, ce qui explique l'existence de nombreuses « cryptomonnaies alternatives ». En l'absence de cet effet, l'activité économique aurait convergé naturellement vers un seul protocole (BTC), mais on peut voir que ce n'est pas le cas, notamment lors des congestions du réseau.

La présence de l'effet de substitution explique la tendance vers un pluralisme cryptomonétaire extrême, dont les partisans prétendent que n'importe quelle technique légèrement supérieure pourrait détrôner le premier protocole du marché. Mais en cela, ils négligent lourdement l'effet de réseau et commettent ainsi l'erreur opposée à celle des maximalistes.

Pouvoir et influence

Pour comprendre plus finement comment le protocole en arrive à être ce qu'il est, il faut différencier le *pouvoir* de l'*influence* dans le cadre de Bitcoin. Dans le domaine politique, le pouvoir est la capacité de faire quelque chose sans un consentement tiers, ce qui se traduit en dernier lieu par l'intervention de la force physique. L'influence est quant à elle la capacité à influer sur le choix de ceux qui détiennent le pouvoir, typiquement les forces religieuses.

Dans Bitcoin, le pouvoir se transcrit par le pouvoir économique des commerçants sur le protocole. Par l'intermédiaire de leurs nœuds, ils vérifient les règles de consensus liées à l'unité qu'ils acceptent dans le commerce et apportent de ce fait une utilité économique à cette unité. Toutefois, ce pouvoir économique direct est bien souvent influencé par de nombreux acteurs.

Ces influences sont prises en compte dans le modèle de gouvernance classique de Bitcoin, qui fait généralement intervenir le triplet développeurs-mineurs-utilisateurs. Ces derniers acteurs forment des forces intérieures du système, car ils y participent plus ou moins directement.

En outre, l'influence sur le protocole provient également des entités extérieures qui interviennent de manière diffuse sur l'ensemble du système. Il est

impossible d'établir une liste exhaustive de ces influences extérieures, mais on peut en identifier les principales. Elles s'exercent en substance de trois manières – par le discours, par l'argent et par la force – et se rapportent à trois catégories d'acteurs : les relais d'opinion, les puissances financières et les forces étatiques.

Ainsi, les commerçants subissent un ensemble d'influences de la part de participants internes au système, comme les développeurs, les mineurs et les autres utilisateurs, mais également de la part d'acteurs externes, comme les relais idéologiques, les financiers et les régulateurs. Par ailleurs, ces groupes interagissent mutuellement, de sorte que le tout forme un ensemble sociologique complexe, qui influe sur le choix final du protocole. Même si expliquer comment cet ensemble complexe se comporte ne rentre pas dans nos compétences, essayons d'en esquisser un modèle général en nous attardant sur les pressions intérieures avant d'examiner les forces extérieures, plus diffuses.

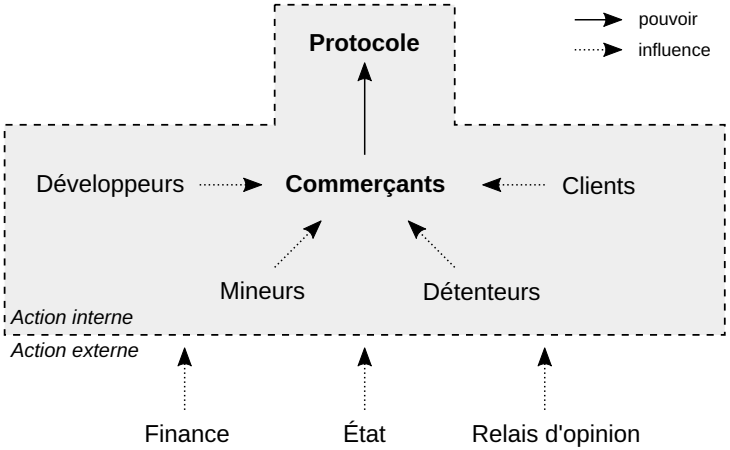

FIGURE 11.1 – Un modèle de gouvernance de Bitcoin : interactions des principaux groupes d'acteurs dans la détermination du protocole.

L'influence des développeurs

La première catégorie d'acteurs internes est formée des développeurs. Les développeurs sont les personnes qui travaillent directement au maintien et aux mises à niveau des implémentations complètes ou partielles du protocole. Ils œuvrent en particulier à la bonne santé de la chaîne par le biais des implémentations utilisées par les commerçants et par les mineurs. L'implé-

mentation de référence, qui est la plus utilisée et qui sert de modèle aux autres implémentations, est la plus importante.

Ce rôle d'intermédiaire leur confère une influence non négligeable sur les commerçants et les autres acteurs, qui ont rarement les capacités d'observer et de comprendre le code directement. De plus, le maintien d'un logiciel performant demande un travail coûteux qui ne peut pas être réalisé par n'importe qui. Cette situation leur donne une position de force dans la prise de décision sur le protocole.

Les développeurs sont nombreux et possèdent diverses opinions. Pour remédier à ce problème, ils fondent souvent leur décision sur le concept de consensus approximatif (*rough consensus*) qui n'est pas un consensus à proprement parler, mais l'estimation d'un sentiment de groupe ou d'une volonté générale. Ce recours au consensus approximatif permet en pratique d'obtenir une quasi unanimité sans qu'un élément individuel puisse perturber le processus [18]. Cette façon d'exclure les éléments récalcitrants peut être critiquée (une personne peut avoir raison contre le groupe), mais elle a l'intérêt de préserver l'effet de réseau du protocole, en offrant une proposition unique aux commerçants.

Pour BTC, l'implémentation de référence est Bitcoin Core, dirigée par des mainteneurs. Ces mainteneurs, et plus généralement les développeurs, sont vus comme les gardiens du protocole. L'utilisation d'une autre implémentation (*fork*) est toujours possible mais est à la fois coûteuse et mal vue, de sorte qu'il existe une inertie jouant en faveur de Bitcoin Core.

Cette dominance s'est manifestée au cours de l'histoire de Bitcoin par le rejet d'un certain nombre de dissidences, qui ont parfois donné lieu à la création d'une implémentation alternative. On peut citer :

— Mike Hearn, qui, en 2014, voulait ajouter une requête de réseau `getutxos` à Bitcoin Core mais qui a été refusée pour cause de non-unanimité, ce qui a mené à la création de Bitcoin XT ;

— Les partisans de l'augmentation de la limite de capacité transactionnelle du réseau durant la guerre des blocs, qui ont mis en place de multiples implémentations pour tenter, en vain, de faire adopter ce changement : Bitcoin XT mi-2015, Bitcoin Classic début 2016, Bitcoin Unlimited mi-2016 et btc1 mi-2017 ;

— Les opposants à la mise à niveau SegWit, soutenue largement par Bitcoin Core, qui n'ont eu d'autre choix que de développer Bitcoin ABC, qui augmentait dans le même temps la taille limite des blocs, menant à la création de Bitcoin Cash ;

— Jeremy Rubin, qui a menacé de faire activer le BIP-119 (soft fork) par les mineurs en 2022, en raison du refus de Bitcoin Core d'intégrer sa modification au logiciel, mais qui a fini par se raviser, ayant probablement obtenu l'attention qu'il désirait.

Les développeurs, et notamment ceux de Bitcoin Core, exercent ainsi une influence importante sur le protocole. Cependant cette influence reste limitée : dans le cas où ils s'opposeraient à l'économie de façon trop tranchée, ces derniers seraient remplacés par d'autres développeurs.

Le premier exemple d'une dissidence réussie se trouve dans l'histoire des débuts de Monero [19]. Monero a été créé sous le nom de Bitmonero en avril 2014 par un développeur utilisant le pseudonyme thankful_for_today, dans le but de relancer le projet Bytecoin qui avait fait l'objet d'un préminage massif. Cependant, il s'est rapidement avéré que thankful_for_today, « dictateur bienveillant » autoproclamé, procédait à des changements sans consulter les autres personnes impliquées et il s'est donc vu être évincé du projet après quelques jours. Une équipe de six développeurs a alors décidé de forker le projet et de le renommer en Monero.

Le second exemple d'une dissidence réussie est l'opposition à Bitcoin ABC en 2020 dans le cadre du protocole Bitcoin Cash. Bitcoin ABC, l'implémentation de référence de Bitcoin Cash depuis 2017, avait pour développeur en chef, Amaury Séchet. En 2020, ce dernier a approuvé la suggestion des mineurs de procéder à un soft fork pour rediriger une partie de la récompense de bloc vers les équipes de développement et a fini en novembre par tenter d'imposer ce changement via une intégration dans Bitcoin ABC. Une implémentation alternative, Bitcoin Cash Node, a alors été créée pour faire face à ce changement, et a recueilli une large majorité économique, devenant ainsi l'implémentation de référence de ce qu'on appelle toujours aujourd'hui Bitcoin Cash. L'application de la redirection de la subvention du protocole a mené à la création du protocole XEC.

Ainsi, l'influence des développeurs sur le protocole est réelle, mais elle est profondément limitée par l'intervention de l'économie si elle a lieu.

La pression des mineurs

La deuxième catégorie d'acteurs impliqués dans l'influence sur le protocole est constituée des mineurs. Les mineurs sont les personnes ou les groupes de personnes qui s'occupent de la confirmation des transactions grâce à la dépense énergétique liée à la preuve de travail. Comme montré dans le chapitre 9,

ils disposent d'un pouvoir de sélection sur les transactions, leur conférant par là, en cas de regroupement majoritaire, la possibilité de procéder à une double dépense ou d'appliquer une censure active.

Contrairement à ce qu'on peut parfois s'imaginer, les mineurs n'ont de pouvoir direct sur le protocole que dans le sens où ils forment une catégorie particulière de commerçants. Ils interviennent dans l'économie en acceptant de confirmer des transactions en échange de frais. Mais ce pouvoir direct est extrêmement limité du fait de la petitesse de leur activité économique par rapport à l'activité totale.

Il n'en reste pas moins que les mineurs possèdent une influence non négligeable dans la prise de décision, qui procède de leur pouvoir d'attaque sur le consensus. D'une part, les mineurs peuvent influer dans le choix de l'économie lors d'une scission en attaquant la branche concurrente dans le but de la discréditer. C'est ce qu'ont menacé de faire les mineurs pro-BSV en novembre 2018 suite à la séparation avec BCH [20]. C'est également ce qu'a fait le mineur pro-BCHN face à Bitcoin ABC en novembre 2020 en censurant la chaîne de Bitcoin ABC.

D'autre part, les mineurs peuvent influencer le choix de l'économie en imposant un soft fork qui, dans son application, est indiscernable de la censure. L'ensemble des règles de consensus initial reste le même, mais ne peut plus s'exprimer pleinement, à tel point que cela peut induire les commerçants à adopter le soft fork en arrêtant d'accepter les transactions et les blocs qui ne s'y conforment pas. C'est ce que le développeur Peter Todd a décrit comme un « soft fork forcé [21] » ou que d'autres appellent un « fork maléfique » (*evil fork*). La situation peut être résolue de deux manières : ou bien les commerçants continuent d'appliquer les anciennes règles et créent par là un différentiel de frais encourageant les mineurs à revenir à la normale ; ou bien ils conviennent d'adopter un hard fork annulant ce soft fork, prenant alors le risque de la spirale de scissions liée à l'intervention humaine rapide.

Toutefois, cette influence des mineurs s'arrête là. Les commerçants continuent de déterminer les règles et les mineurs sont impuissants face à cette réalité. Il est donc faux de prétendre que les mineurs sont les maîtres du protocole (gouvernance par preuve de travail), comme le faisaient une bonne partie des *big blockers* durant la guerre des blocs [22]. En effet, si c'était réellement le cas, alors le système économique de Bitcoin serait voué à l'échec, les mineurs étant naturellement incités à augmenter leurs revenus par l'inflation, à l'instar des banques centrales.

L'importance des utilisateurs

La troisième catégorie d'acteurs internes ayant une influence sur le protocole est la catégorie des utilisateurs non commerçants. Les utilisateurs sont souvent mis en avant comme les personnes ayant le dernier mot sur le protocole [23]. Toutefois, le terme d'utilisateur est ambigu et peut prêter à confusion, car l'utilisation du bitcoin englobe généralement trois actions distinctes : l'acceptation dans le commerce, la détention durant une période donnée et la dépense auprès d'autres personnes. De là, on peut dégager trois sous-catégories théoriques d'utilisateurs : les commerçants, les clients et les détenteurs. La première possède le pouvoir effectif sur le protocole, tandis que les deux autres n'exercent qu'une simple influence.

Parlons d'abord des clients, qui sont les personnes qui échangent leurs bitcoins contre des biens et services dans le commerce, y compris d'autres monnaies. Ils sont le pendant des commerçants, l'échange étant par définition symétrique : sans client (acheteur), il n'y a pas de commerçant (vendeur), et vice versa. Il y a donc une interdépendance entre les commerçants et les clients.

Dans la détermination du protocole, les clients exercent par conséquent une très grande influence. Un commerçant, s'il veut continuer à prospérer dans les affaires, devra choisir d'accepter (au moins) la monnaie liée au protocole soutenu majoritairement par ses clients. L'histoire du refus de SegWit2X en 2017 est l'exemple parfait de l'influence des clients, où les utilisateurs ont réussi à influencer les plus gros commerçants (les plateformes de change) et à les pousser à renoncer au doublement de la taille limite des blocs en novembre.

Toutefois, l'idée que ces clients partagent la maîtrise du protocole avec les commerçants est erronée. Si la dissension est équilibrée parmi les utilisateurs, alors c'est le commerçant qui tranche en optant pour un protocole plutôt que l'autre pour offrir ses biens et services à des prix acceptables. Au bout du compte, le client (qui se débarrasse de ses bitcoins) n'apporte aucune utilité à la monnaie ; le commerçant, si.

Considérons ensuite les détenteurs, c'est-à-dire les personnes qui conservent des bitcoins en réserve durant une période significative. Ces détenteurs sont parfois appelés thésauriseurs ou HODLers (par déformation du verbe *to hold*, « garder », « conserver » [24]) pour insister sur le fait qu'ils ne veulent pas se séparer de leurs bitcoins de sitôt. Par cette action, ils restreignent l'offre de monnaie à proprement parler ce qui, conjugué à une demande plus forte, a un effet haussier sur le pouvoir d'achat de l'unité et sur son taux de change avec le dollar, communément appelé « le prix ».

Les détenteurs ont une influence sur les commerçants. Premièrement, par leur épargne, ils augmentent la taille de la subvention du protocole, et donc le budget du minage pour la protection contre la double dépense, assurant une plus grande sécurité aux commerçants. Deuxièmement, la détention offre au marché plus de liquidité potentielle, ce qui permet à des utilisateurs plus importants d'entrer. Troisièmement, un prix plus haut a un effet de communication non négligeable, notamment par l'attention qu'un engouement spéculatif entraîne dans les médias. Ainsi, si une scission a lieu, les détenteurs peuvent vendre la monnaie d'une branche contre celle de l'autre et créer un différentiel favorable au protocole privilégié (c'est ce qui s'est passé durant la scission entre BTC et BCH).

La conception selon laquelle le pouvoir d'achat de la monnaie serait primordial a poussé certains protocoles cryptoéconomiques comme Dash et Tezos à innover en créant des systèmes de gouvernance internes permettant de résoudre les disputes à propos de la modification du protocole par un vote proportionnel à la possession d'unités (gouvernance par preuve d'enjeu). Les détenteurs seraient assimilés aux parties prenantes d'une société, possédant des parts dans cette dernière, qui serait essentiellement une organisation autonome décentralisée (DAO).

Toutefois, cette conception ne tient que dans la phase précoce de Bitcoin, où la création monétaire forme l'essentiel du revenu minier, où l'activité est encore hautement spéculative (l'achat et la vente de monnaie fiat dans le but d'en tirer un profit) et où les principaux commerçants sont les plateformes de change et leurs utilisateurs. À long terme, la diminution de la subvention minière et la stabilisation réduit cet effet et donne un rôle beaucoup plus important aux transactions non spéculatives, car s'il existe une relation entre l'utilité et le prix de l'unité, c'est la première qui prime sur le second.

Ainsi, l'influence générale des acteurs internes sur les commerçants – développeurs, mineurs, clients et détenteurs – est non négligeable et joue un rôle dans la détermination du protocole. Mais ce n'est pas la seule pression qui s'exerce, et il faut aussi compter les acteurs externes au système, qui participent aussi à leur niveau dans le mécanisme de gouvernance.

Le poids des relais d'opinion

La première catégorie des influences extérieures est celle des relais d'opinion, qui orientent l'avis des personnes actives dans Bitcoin. Ces relais peuvent être individuels (influenceurs) ou collectifs (médias). La raison de leur existence est qu'il est impossible de saisir par soi-même toutes les subtilités de

Bitcoin, de sorte que la plupart des utilisateurs se contentent souvent d'une explication rudimentaire proposée par autrui, et font reposer un partie de leur jugement sur la confiance accordée à autrui.

Cette situation conduit à l'émergence d'acteurs plus influents que les autres, par leur prestige individuel ou par les médias qu'ils dirigent. On dit parfois que Bitcoin n'a pas de chef, de meneur, qu'il est acéphale [25]. Cependant, force est de constater que ce n'est pas le cas *stricto sensu* et que certaines personnes ont un poids plus important que d'autres dans la prise de décision, indépendamment de leur activité économique.

D'abord, les experts techniques, qui sont censés mieux connaître les méandres du protocole que les autres, rentrent dans cette catégorie. Ils peuvent être développeurs eux-mêmes, avoir une activité proche, ou bien être éducateurs ou rédacteurs. Nous pouvons par exemple citer Adam Back, ancien cypherpunk et PDG de Blockstream, Andreas Antonopoulos, éducateur de longue date, ou encore Aaron van Wirdum, rédacteur expérimenté pour le Bitcoin Magazine et coanimateur du podcast Bitcoin Explained.

Ensuite, viennent les acteurs impliqués politiquement qui saisissent les intérêts profonds de Bitcoin. On peut mentionner ici l'activiste Alex Gladstein, directeur de la stratégie à la Human Rights Foundation. Puis viennent les économistes, qui comprennent mieux que les autres les mécanismes économiques à l'œuvre dans Bitcoin, comme l'économiste et auteur Saifedean Ammous, l'experte en macroéconomie Lyn Alden, ou encore le magistrat financier Yorick de Mombynes en France.

Enfin, nous avons les financiers, qui ont fait fortune avant de découvrir Bitcoin ou bien grâce à lui. Ces personnes sont considérées comme des modèles du fait de leur réussite financière, qui est l'objectif principal de la majorité des gens qui s'intéressent à Bitcoin en premier lieu. Roger Ver, les frères Winklevoss et Michael Saylor en font partie. On peut aussi citer le milliardaire Elon Musk, qui est l'archétype de ce type d'influence, et qui a notamment donné une seconde vie à Dogecoin en le citant à de multiples reprises dans ses interventions publiques.

Toutes ces personnalités sont souvent relayées par les médias, qui jouent eux-même un rôle de relai d'opinion. Ces derniers exercent en effet une certaine influence en choisissant quels contenus sont publiés ou diffusés et lesquels ne le sont pas. Ils permettent au grand public qui n'a pas le temps ou l'envie de lire sur le sujet de se forger un avis.

Il peut s'agir des vidéastes individuels qui produisent du contenu sur les cryptomonnaies, notamment sur la plateforme Youtube. Il y a aussi les autres

médias spécialisés comme les sites d'information (Bitcoin.org, Bitcoin.fr), les médias d'actualité (Bitcoin Magazine, Cointelegraph, Coindesk, Bitcoin.com à l'international ; Cryptoast et le Journal du Coin en France), les chaînes vidéo (Grand Angle Crypto), les podcasts, les lettres d'information payantes (The Big Whale). On peut également mentionner les plateformes de discussion spécialisées, dont le forum de discussion historique bitcointalk.org, les subreddits consacrés à Bitcoin (r/bitcoin, r/btc), et aujourd'hui les groupes Telegram dédiés.

Les médias généralistes exercent aussi une influence, bien qu'elle soit encore plus diffuse. C'est par exemple le cas des chaînes d'informations financières (CNBC, BFM Business) qui consacrent parfois des émissions au sujet des crypto-actifs. On peut aussi citer tous les médias sociaux qui peuvent modeler l'opinion publique à propos de Bitcoin, comme c'est le cas de Twitter, lieu privilégié pour la communication sur Bitcoin.

La puissance suggestive de la finance

Le discours n'est cependant pas la seule manière d'influencer les acteurs du système : il existe également le « pouvoir » de l'argent. Les puissances financières jouent un rôle dans la détermination du protocole en choisissant de financer l'écosystème et les influenceurs de la variante de Bitcoin qui leur plaît. Elles peuvent par exemple fournir des fonds pour la croissance commerciale (listage sur plateforme de change), le développement logiciel, la création d'applications innovantes, le marketing, le lobbying auprès des instances régulatrices, etc.

Le financement de l'implémentation de référence est particulièrement crucial. L'infrastructure logicielle n'est pas maintenue gratuitement, mais elle n'apporte aucun revenu, du fait de l'absence nécessaire de contrainte légale sur son utilisation. C'est pourquoi les développeurs doivent trouver de l'argent quelque part [26]. C'est ainsi que diverses organisations financent le développement : en 2023, le salaire versé aux personnes chargées de l'écriture et de la révision du code dans Bitcoin Core provient principalement (par ordre d'importance) de l'organisation caritative Brink (elle-même financée par les principales plateformes de change), la *Digital Currency Initiative* du MIT Media Lab, le groupe de développement et de recherche Chaincode Labs, l'entreprise Block de Jack Dorsey et la plateforme de trading sur marge BitMEX.

Cela donne aux puissances financières une influence particulière, chose qui a été dénoncée au sujet de Blockstream depuis ses débuts, l'entreprise

ayant notamment reçu un investissement de la part d'AXA. On peut aussi citer le cas de la *Digital Currency Initiative* dont le rôle est plus qu'ambigu. Cette entité a en effet été l'organisation en charge du développement du prototype de monnaie numérique de banque centrale des États-Unis tout en continuant de payer le mainteneur principal de Bitcoin Core, Wladimir van der Laan.

La guerre de l'État contre le protocole

Pour finir, la troisième et dernière méthode utilisée pour influencer les acteurs du système et donc le protocole, c'est la force, ou plus précisément la menace d'utiliser la force, une spécialité largement monopolisée par une grande institution appelée l'État.

L'existence de l'État est profondément liée au contrôle sur la monnaie, qui facilite grandement la collecte de son revenu. En particulier, il prélève un seigneuriage grâce à la domination qu'il exerce sur la détermination du support monétaire. De ce fait, il existe un rapport antagoniste entre l'État et Bitcoin, ce dernier redonnant aux individus la maîtrise totale de leur monnaie.

Il est donc logique que l'État cherche à influencer l'évolution du protocole, voire qu'il finisse par tenter de le décréter. Par la définition du cadre légal, il peut en effet influer sur le choix des commerçants. Son pouvoir politique n'est cependant pas illimité. S'il s'y prend mal ou si le changement est trop brutal, ces commerçants risquent de désobéir en masse et de rejoindre le marché noir, où aucune autorisation n'est requise.

C'est le pouvoir économique qui détermine le protocole en dernier lieu. Mais avec le temps l'État peut s'immiscer dans ses décisions pour altérer doucement les propriétés de Bitcoin. Par des lois intelligentes, il peut faire en sorte que son action reste largement acceptée et qu'une bonne partie de l'économie continue d'avoir lieu sur le marché réglementé. Il peut aussi influencer les différents acteurs qui jouent un rôle dans le modèle de gouvernance de Bitcoin, comme les développeurs, les mineurs ou les médias, sans que ceux-ci ne réagissent.

Les réglementations financières constituent des étapes préparatoires dans le déploiement d'une telle influence. Il s'agit des contraintes imposées aux plateformes de change (commerçants principaux) qui se chargent d'effectuer la jonction entre le bitcoin et les monnaies officielles. Initiées en 2013, ces réglementations imposent aujourd'hui une procédure de connaissance du client (KYC) et de connaissance des transactions (KYT) assez drastique, de sorte que l'anonymat dans ce type d'échange devient de plus en plus difficile à préserver. Elles ont le double avantage d'habituer les acteurs économiques à se

conformer et de restreindre leur nombre en requérant des contraintes de plus en plus insurmontables pour les plus petites plateformes. Ces réglementations peuvent également s'appliquer aux commerçants en général. De plus, la loi les contraint déjà dans la plupart des juridictions à déclarer leurs plus-values par rapport à la monnaie nationale, ce qui complique leur activité.

Voyons maintenant comment le protocole pourrait être attaqué. Tout d'abord, l'acceptation du bitcoin pourrait être rendue illégale, sans alternative. Toute l'économie portée par les commerçants du marché réglementé serait détruite d'un simple trait de plume. L'utilité du système serait alors grandement réduite sur le moment, ainsi que la valeur d'échange de l'unité de compte.

Ce type d'interdiction totale a déjà eu lieu dans certains pays, comme le Maroc, l'Algérie, la Bolivie ou le Népal. D'autres pays ont choisi d'interdire uniquement une section de l'économie, que ce soit le change avec la monnaie nationale (Chine), la vente de biens et services sur le territoire (Turquie, Équateur, Thaïlande) ou l'acquisition par des acteurs financiers (Iran, Nigéria). Toutefois, sauf dans le cas de la Chine, ces interdictions n'ont pas été réalisées par des puissances majeures, de sorte que l'utilisation du bitcoin reste légale sur la majorité de la planète. Une réelle interdiction, si elle avait lieu, aurait besoin de se faire de manière internationale pour avoir une influence réelle et amoindrir l'utilité de Bitcoin.

L'impact de cette interdiction pure et simple est difficile à mesurer. En effet, on peut douter de la capacité d'application de ces lois. Une interdiction sans soutien populaire aurait pour conséquence d'accroître la taille du marché noir. De ce fait, il semble évident qu'une telle attaque s'accompagnerait de la proposition d'une alternative contrôlée de Bitcoin ayant pour but de contenter la partie la plus « pragmatique » de l'économie.

Dans le but de s'opposer à Bitcoin, l'État pourrait ainsi déployer sa propre version du protocole dans le but de ronger progressivement les propriétés fondamentales de Bitcoin. Cette version altérée de Bitcoin serait rendue légale et bénéficierait d'un régime accommodant, tandis que la version originelle serait rendue illégale. Les acteurs conformistes seraient récompensés à court terme par une augmentation du prix, alors que les commerçants dissidents seraient punis par des amendes et des peines de prison.

En premier lieu, des soft forks de censure pourraient être appliqués en se basant sur les normes générales de LCB-FT. Ceux-ci pourraient s'accompagner d'une attaque de censure active par les mineurs. Les acteurs conformistes pourraient justifier leur choix en disant que ces transactions n'ont rien à faire sur la chaîne de Bitcoin.

En deuxième lieu, un soft fork pourrait aller jusqu'à concerner toutes les transactions, en requérant une autorisation étatique pour chacune d'entre elles. À ce stade, les plus conformistes pourraient toujours s'imaginer que la politique monétaire aurait été préservée.

En troisième lieu, un soft fork taxatoire pourrait être mis en place. Celui-ci consisterait à prélever une taxe fixe sur toutes les transactions, dans l'idée de la TVA, ou bien à extraire un demeurage, en soustrayant un montant dépendant du temps de détention des fonds dépensés. Ces impôts pourraient être réalisés dans l'objectif de réguler la nature trop déflationniste du bitcoin et la répartition inique de la richesse.

En quatrième lieu, un hard fork d'inflation pourrait être appliqué. À ce stade, les acteurs restants n'auraient plus rien à voir avec les acteurs originaux. Ce qui faisait la renommée de « Bitcoin » serait alors totalement anéanti, et le système correspondant ressemblerait trait pour trait à une monnaie numérique de banque centrale.

Ce scénario, bien qu'hypothétique, forme la conséquence logique de l'influence de l'État sur la monnaie et est donc inévitable jusqu'à un certain point. Toutefois, il suppose dans le même temps le développement d'une économie parallèle dans laquelle l'acceptation du bitcoin se ferait de manière clandestine. Face à la censure de plus en plus forte, il se formerait ainsi une opposition, une résistance. Les altérations progressives rendraient la chaîne officielle de moins en moins utile, en faisant fuir les commerçants ne souhaitant pas se conformer.

À un certain moment, une scission aurait lieu. La version étatique pourrait être minoritaire, auquel cas elle se séparerait naturellement de l'autre chaîne (scénario optimiste). Mais elle pourrait aussi être majoritaire, auquel cas la version clandestine serait contrainte de procéder à un hard fork pour subsister (scénario pessimiste). Dans les deux cas, la reconstruction de Bitcoin se produirait alors à partir de la chaîne libre, au sujet de laquelle il n'y aurait aucune ambiguïté au niveau du protocole. Cette chaîne pourrait cependant être attaquée du point de vue minier, ce que nous avons décrit en détail dans le chapitre 9.

Deux niveaux de sécurité

Bitcoin est un concept de monnaie numérique résistante à la censure et à l'inflation. Ces deux propriétés fondamentales sont complémentaires, mais elles nécessitent des sécurités différentes. La résistance à la censure repose sur la sécurité minière ; la résistance à l'inflation sur la sécurité commerciale.

La détermination du protocole – ou plutôt des protocoles puisqu'il peut y en avoir plusieurs – est réalisée par les commerçants au sens large, c'est-à-dire les personnes qui acceptent le bitcoin dans l'échange contre des biens, des services ou d'autres monnaies. Les commerçants vérifient les règles de consensus par l'intermédiaire de leurs nœuds. Ce pouvoir sur le protocole est proportionnel à l'activité économique potentielle du commerçant, qui peut être estimée par ses recettes effectives. Il dépend aussi de l'effet de réseau qui fait que l'utilité combinée apportée par les commerçants va évoluer de manière superlinéaire.

Un certain nombre d'influences s'exercent sur les commerçants pour qu'ils acceptent tel ou tel protocole. S'il est dur de comprendre comment cet ensemble complexe interagit, il est possible d'en dessiner les contours comme nous l'avons fait ici. En particulier, l'influence majeure à ne pas négliger est celle de l'État, qui pourrait attaquer le protocole en bonne et due forme par la coercition des commerçants et des autres acteurs.

Pour que le protocole de Bitcoin soit réellement robuste, il faut donc que l'activité économique soit décentralisée, à l'instar du minage : que les commerçants (ou petits groupes de commerçants) fassent fonctionner leurs propres nœuds pour que, dans l'hypothèse d'un changement des règles décrété par une autorité, les risques soient répartis dans l'économie et que Bitcoin puisse continuer à survivre clandestinement.

Il est nécessaire que l'accord sur le protocole s'exerce à long terme. La courte histoire de Bitcoin regorge de multiples perturbations qui montrent que le changement des règles de consensus ne se passe pas toujours dans les meilleures conditions. Seul le temps permet de faire le tri entre les bonnes modifications et les mauvaises.

12

Les rouages de la machine

Bitcoin est une étrange machine. Né dans un rapport antagoniste vis-à-vis de l'autorité, il possède des propriétés qui ne se retrouvent pas dans les systèmes informatiques communs. En particulier, il ne peut pas être modifié n'importe comment, ce qui explique sa conception originelle et son évolution ultérieure.

D'une part, la représentation des unités de base, les satoshis, ne se fait pas sous la forme de comptes où les soldes des utilisateurs seraient mis à jour, mais par le biais de pièces de cryptomonnaies pouvant être combinées et séparées dans les transactions. Ce fonctionnement favorise la confidentialité et la scalabilité de la chaîne, et s'adapte ainsi à l'utilisation monétaire.

D'autre part, Bitcoin intègre un système de programmation interne permettant d'intégrer des conditions de dépense dans les pièces, ce qu'on appelle parfois des contrats autonomes ou *smart contracts*. Il a été amélioré au cours des années, parfois au prix d'une plus grande complexité, notamment via l'ajout de SegWit et de Taproot.

Dans ce chapitre, nous examinerons les rouages de cette machine transactionnelle, avant de décrire comment elle peut être exploitée et améliorée à des fins de confidentialité. Le prochain chapitre sera consacré aux contrats en tant que tels.

Les transactions et les pièces

Dans Bitcoin, les transactions possèdent un rôle central. Le protocole est fait pour échanger de la valeur conformément à son rôle monétaire, donc de traiter les transferts de propriété. Tout le fonctionnement du système a été pensé pour faciliter la construction, la signature et la diffusion des transactions, leur conservation en mémoire dans la *mempool*, et leur ajout au registre par leur inclusion dans un bloc.

Chaque transaction est constituée d'une ou plusieurs entrées et d'une ou plusieurs sorties. Une sortie transactionnelle se compose simplement d'une indication de destination et d'un montant en unités (satoshis). Une entrée fait généralement référence à une sortie transactionnelle précédente, sauf dans le cas de la transaction de récompense où elle représente une « base de pièce » créant de nouvelles unités issues de l'émission monétaire et des frais de transaction.

L'identifiant d'une transaction (*transaction identifier* ou `txid`) est l'empreinte des données brutes qu'elle contient, obtenue via le hachage par double SHA-256. Chaque sortie transactionnelle est caractérisée par l'identifiant de la transaction dont elle est issue et par sa position dans cette transaction, qu'on appelle l'indice. Ce point de sortie (*outpoint*) sert d'indication de provenance. Un exemple de point de sortie est `f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16:0`.

Contrairement à ce que la description de la propriété dans le chapitre 7 suggère, la destination et la provenance des unités ne sont pas à proprement parler des adresses, mais des scripts de verrouillage, c'est-à-dire des petits programmes qui déterminent leurs conditions de dépense. Chaque sortie crée ainsi un script qui bloque les fonds d'une façon spécifique. Le plus souvent, ce script contient une clé publique ou une empreinte de clé publique, qui peut être interprétée comme une adresse par le portefeuille.

Pour être valide, une entrée doit contenir un script de déverrouillage dont l'exécution, combinée à celle du script de verrouillage, réussisse. En général, ce script de déblocage des fonds contient une signature numérique qui correspond à la clé publique liée au script de verrouillage précédent : la vérification de la signature permet de s'assurer que la personne qui dépense les unités en est le propriétaire.

Ce fonctionnement fait que le modèle de représentation des unités est contre-intuitif. Le protocole ne voit pas de comptes dont les soldes seraient actualisés par les transactions, comme c'est le cas dans Ethereum par exemple. Il voit simplement des sorties transactionnelles détenues par des propriétaires,

de manière similaire aux pièces de monnaies dans le monde physique.

Ainsi, Bitcoin met en œuvre le concept de pièce de monnaie numérique qui était discuté au sein de la communauté cypherpunk dans les années 1990. Dans le *Cyphernomicon* par exemple, Tim May estimait que la chose était impossible, en raison du problème de la double dépense. Satoshi Nakamoto, en découvrant une manière de résoudre ce problème, a pu rendre le concept viable et l'a intégré dans Bitcoin. Dans le livre blanc, il décrivait la notion de pièce numérique comme suit :

> « Nous définissons une pièce de monnaie électronique comme une chaîne de signatures numériques. Chaque propriétaire transfère la pièce au suivant en signant numériquement l'empreinte de la transaction précédente et la clé publique du propriétaire suivant, et en les ajoutant à la fin de la pièce. Un bénéficiaire peut vérifier les signatures pour vérifier la chaîne de propriété [1]. »

Dans Bitcoin, les pièces existantes sont donc les sorties transactionnelles non dépensées, nommées usuellement UTXO par abréviation de l'anglais *Unspent Transaction Outputs*, à savoir les sorties transactionnelles qui n'ont pas été utilisées comme entrée dans une autre transaction. L'ensemble de ces pièces, l'*UTXO set*, constitue le registre de propriété. C'est l'état du système, qui peut être récupéré à partir de son historique, la chaîne de blocs.

Chaque pièce est constituée d'un montant en unités (satoshis) et d'un script de verrouillage. Il peut ainsi exister des pièces d'un milliard de satoshis (10 bitcoins) tout comme on peut avoir des pièces de 546 satoshis (0,00000546 bitcoin).

Le script de verrouillage d'une pièce contient le plus souvent une clé publique ou une empreinte déterminée, de sorte que la pièce peut être vue comme étant détenue par l'adresse correspondante. De ce fait, deux pièces partageant le même script de verrouillage sont détenues par la même adresse. Un compte dans Bitcoin correspond à l'ensemble des adresses contrôlées par un utilisateur. Le solde est récupéré en balayant l'ensemble des UTXO de façon à retrouver les pièces détenues par ces adresses.

Ce modèle de représentation par des pièces fait qu'on peut voir le mécanisme de transaction comme une fonderie de pièces de monnaie. Chaque transaction consiste à fondre ensemble une ou plusieurs pièces de bitcoin en entrée et à frapper une ou plusieurs pièces en sortie. C'est en ceci que le serveur d'horodatage distribué de Bitcoin vient remplacer la monnaierie numérique centralisée permettant le remplacement systématique des pièces, qui est présente dans eCash et RPOW par exemple.

La construction d'une transaction implique de rassembler des pièces de

FIGURE 12.1 – Exemples de pièces détenues par un même compte.

valeur suffisante en entrée pour les fondre et en frapper de nouvelles. En général, deux pièces sont créées : la première est créée sur l'adresse fournie par le destinataire pour effectuer le paiement (sortie principale) et la seconde est créée sur l'une des adresses de l'expéditeur afin qu'il se « rende la monnaie » (sortie complémentaire). La différence entre le montant en entrée et le montant en sortie est prise en compte dans la récompense du mineur en tant que frais de transaction.

Considérons quelques exemples en ignorant ces frais et supposons qu'Alice veuille procéder à un paiement. Si Alice possède une pièce de 12 mBTC (0,012 BTC) et veut donner 7 mBTC à Bob, alors elle doit construire et signer une transaction ayant pour entrée cette pièce de 12 mBTC et pour sorties une pièce de 7 mBTC vers l'adresse de Bob et une pièce restante de 5 mBTC vers sa propre adresse. Cette transaction est représentée par la figure 12.2.

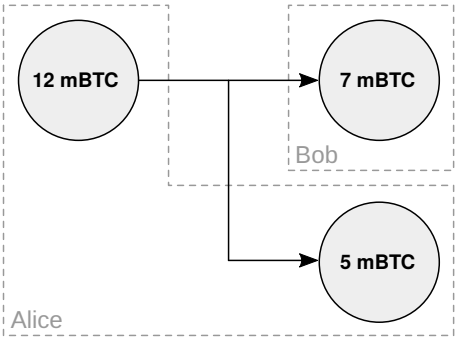

FIGURE 12.2 – Schéma d'une transaction à 1 entrée et 2 sorties.

Si Alice ne possède pas une pièce ayant une valeur faciale supérieure à 7 mBTC, alors elle doit regrouper des pièces pour réunir un montant suffisant en entrée, par exemple une pièce de 6 mBTC et une pièce de 2 mBTC. Comme précédemment, elle doit créer une sortie complémentaire vers elle-même dans le but de se rendre la monnaie. Dans ce cas, illustré sur la figure 12.3, on peut deviner en observant la transaction que la pièce de 7 mBTC est le résultat du paiement, car il serait économiquement irrationnel de fusionner plusieurs pièces pour envoyer 1 mBTC.

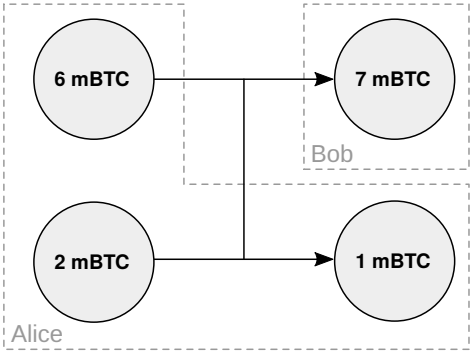

FIGURE 12.3 – Schéma d'une transaction à 2 entrées et 2 sorties.

Si Alice désire transférer l'intégralité des fonds vers un autre compte, alors elle rassemble l'ensemble de ses pièces (6 mBTC, 4 mBTC, 2 mBTC) pour les envoyer vers une adresse unique, comme montré sur la figure 12.4. C'est ce qu'on appelle une consolidation de portefeuille, qui peut être identifiée par un observateur extérieur en raison de l'unicité de la sortie.

Nous voyons ainsi que les transactions ne sont pas des transferts bruts d'une adresse vers une autre, mais des combinaisons-séparations de pièces de monnaies numériques. Ce fonctionnement est quelque peu contre-intuitif, mais se révèle utile pour la scalabilité du système, en permettant le traitement indépendant des pièces, et pour la confidentialité des utilisateurs, en n'incitant pas au rassemblement des fonds sur une même adresse et en facilitant l'implémentation de techniques d'anonymisation comme le mélange des pièces. Ce modèle est donc particulièrement adapté à l'utilisation monétaire.

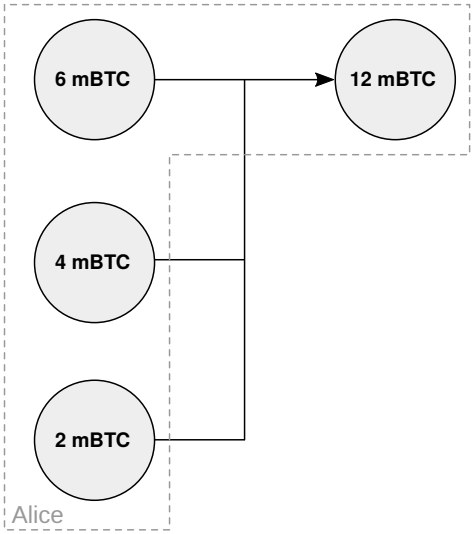

FIGURE 12.4 – Schéma d'une transaction à 3 entrées et 1 sortie.

La machine virtuelle

Les scripts présents au sein des transactions font de Bitcoin un système de monnaie programmable. Ces scripts permettent en effet la mise en place d'une variété de conditions de dépense, aussi appelées clauses, qui vont au-delà de l'exigence d'une signature simple, comme la connaissance d'un secret, l'attente d'une période de temps ou la production de signatures multiples.

La mise en œuvre de Bitcoin crée une machine abstraite dont le fonctionnement est répliqué sur tous les nœuds du réseau grâce à l'algorithme de consensus. Elle est simulée par l'intermédiaire de l'implémentation logicielle, de sorte qu'on parle de machine virtuelle. Plus précisément, il s'agit d'une machine à états, dont l'état courant est l'ensemble des pièces existantes, c'est-à-dire l'ensemble des sorties transactionnelles non dépensées (UTXO), et dont les transitions sont les transactions, qui détruisent des pièces pour en créer de nouvelles. Ces transactions sont assemblées dans des blocs qui sont validés à intervalles réguliers par les mineurs. La diffusion d'un bloc sur le réseau permet d'actualiser l'état de la machine virtuelle, qui est (sauf dans le cas d'un embranchement) partagé par tous les nœuds.

Au sein d'une transaction, le déverrouillage des pièces se fait par l'exécution de scripts. Les scripts sont des prédicats au sens mathématique, c'est-à-dire des expressions incomplètes qui deviennent des propositions pouvant

être évaluées si elles sont complétées par un ou plusieurs éléments. De ce fait, la dépense consiste à réunir le script de verrouillage de la sortie précédente et le script de déverrouillage, et à les exécuter l'un après l'autre : le script de déverrouillage d'abord, le script de verrouillage ensuite. L'utilisation de la pièce comme entrée de transaction n'est approuvée que si l'exécution réussit.

Les scripts sont écrits dans le langage de programmation interne de Bitcoin, conçu par Satoshi Nakamoto dès 2008 et baptisé de façon peu originale « Script ». Ce langage de programmation fonctionne de manière similaire à Forth, un langage utilisé dans les années 1970 et 1980. Il se base en particulier sur deux piles de données, qui sont des structures de données fondées sur le principe du « dernier arrivé, premier sorti » (*last in, first out*, ou LIFO). Le langage agit essentiellement sur la pile primaire, de sorte que celle-ci est la plus importante ; la pile secondaire permet seulement de mettre des données de côté pendant l'exécution d'un script.

Satoshi Nakamoto a inclus ce système de scripts dans Bitcoin pour lui permettre de gérer une grande variété de cas d'utilisation. En juin 2010, en réponse à Gavin Andresen, il écrivait la chose suivante sur le forum :

> « La nature de Bitcoin est telle que, dès la version 0.1 lancée, son fonctionnement de base était gravé dans le marbre pour le reste de son existence. C'est pour cette raison que je voulais concevoir Bitcoin pour qu'il supporte tous les types de transactions auxquels je pouvais penser. Le problème était que chaque élément requérait un code de prise en charge et des champs de données spéciaux, qu'il soit utilisé ou non, et ne pouvait couvrir qu'un cas particulier à la fois. Ç'aurait été une explosion de cas particuliers. La solution était script, qui généralisait le problème de façon à ce que les parties contractantes puissent décrire leurs transactions comme des prédicats que les nœuds du réseau évaluaient. Les nœuds ont seulement besoin de comprendre la transaction dans la mesure où ils évaluent si les conditions de l'expéditeur sont remplies ou non [2]. »

Le langage est constitué de plus d'une centaine d'opérateurs, aussi appelés codes opération (*opcodes*), qui agissent sur la pile primaire d'une manière ou d'une autre. Les opérateurs sont des nombres codés sur 1 octet (allant de 0 à 255), mais sont usuellement désignés par un nom décrivant leur fonction, dans le but de rendre la lecture plus compréhensible par l'être humain. Ils sont notés en majuscules et sont souvent précédés du préfixe `OP_` même s'il peut être omis en l'absence d'ambiguïté. Par exemple, l'opérateur permettant de vérifier une signature (`0xac`) est noté `OP_CHECKSIG` ou `CHECKSIG`.

Les opérateurs allant de 1 à 75, parfois notés `OP_PUSHBYTES_X`, ont pour action d'empiler des données ayant une taille allant de 1 à 75 octets.

L'utilisation d'opérateurs supplémentaires spécifiques (notés `OP_PUSHDATA_Y`) permet cependant de placer une information plus grande sur la pile. Bien qu'on puisse utiliser cette notation, il est généralement plus simple de placer un élément entre chevrons pour indiquer qu'il est placé au sommet de la pile. Par exemple, le fait d'écrire `<signature>` au sein d'un script signifie que la signature est empilée.

La valeur retournée à la fin de l'exécution des scripts est un booléen, de sorte que le script peut être valide, auquel cas la dépense de la pièce est approuvée, ou bien invalide, auquel cas la transaction est rejetée dans son ensemble. Le script est valide si et seulement si la valeur `TRUE` (« vrai ») est présente en haut de la pile à la fin de l'exécution. Il est invalide si ce n'est pas le cas ou si son exécution s'est arrêtée avant la fin.

Le langage Script est cependant limité. Rien dans sa conception de base ne permet de faire de boucles, ni d'accéder à des données extérieures à celles de la transaction, contrairement au langage d'Ethereum qui est quasi Turing-complet. Cette particularité fait qu'il est moins flexible, mais qu'il a l'avantage d'être plus simple à appréhender et donc plus sûr.

L'exemple typique de script, présenté par Andreas Antonopoulos[3], est celui qui consiste à résoudre une équation simple impliquant une addition. Si on considère l'équation $17 + x = 38$, alors le script de verrouillage qui correspond est :

```
<17> ADD <38> EQUAL
```

Toute personne disposant de la réponse peut dépenser la pièce, ce qui on en convient n'est pas très sécurisé. La dépense requiert ici de fournir le script de déverrouillage composé uniquement de la solution de l'équation, à savoir 21 :

```
<21>
```

L'exécution successive de ces deux scripts (voir figure 12.5) a lieu comme suit : 1) la valeur 21 est placée sur la pile ; 2) la valeur 17 est placée au-dessus ; 3) l'opérateur `OP_ADD` additionne les deux valeurs en haut de la pile et les remplace par leur somme, ici 38 ; 4) la valeur 38 est placée au sommet de la pile ; 5) l'opérateur `OP_EQUAL` compare les deux valeurs en haut de la pile et les remplace par le booléen d'égalité, ici `TRUE`. L'exécution du script est donc un succès.

Si la valeur avait été différente, de 22 par exemple, alors la dernière opération aurait retourné le booléen `FALSE` (« faux ») et la transaction de dépense aurait été invalidée.

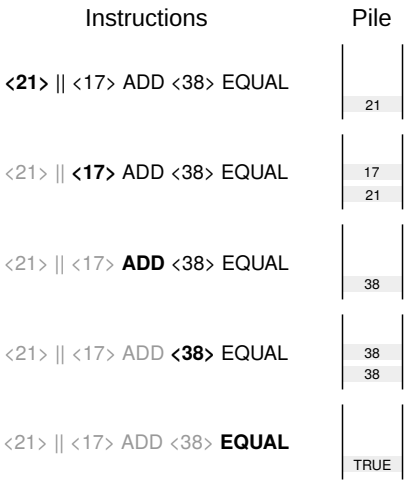

FIGURE 12.5 – Exécution d'un script d'addition sur la pile de données.

Beaucoup de conditions de dépense différentes peuvent être implémentées par ce système. Certaines de ces conditions sont simples comme la connaissance d'un secret spécifique ou la production d'une signature valide correspondant à une clé publique particulière. La connaissance d'un secret (dont l'empreinte est spécifiée dans l'UTXO) est vérifiée par les scripts suivants qui placent le secret au sommet de la pile, le hachent par SHA-256 et comparent le résultat à l'empreinte :

```
<secret> || SHA256 <empreinte> EQUAL
```

De même, la vérification de la validité d'une signature est réalisée par les scripts suivants qui empilent d'abord la signature, puis la clé publique avant de contrôler leur correspondance :

```
<signature> || <clé publique> CHECKSIG
```

En outre, il existe des conditions plus avancées comme les verrous temporels. Ceux-ci permettent de bloquer les fonds de la pièce pour un temps précis, que ce soit jusqu'à une date donnée, auquel cas on parle de temps de verrouillage absolu, ou bien pendant une période donnée, auquel cas on parle de temps de verrouillage relatif. Le premier est le fait de l'opérateur `OP_CHECKLOCKTIMEVERIFY` dont les spécificités techniques sont décrites dans le BIP-65. Le second est appliqué par le code opération `OP_CHECKSEQUENCEVERIFY` décrit dans le BIP-112.

Les schémas classiques

Le langage Script permet de faire des choses diverses et variées. Pendant les premiers temps de Bitcoin, le système était relativement libre et autorisait les gens à écrire ce qu'ils voulaient dans les scripts sans discrimination. Toutefois, cette situation était considérablement risquée. La raison principale était que le fonctionnement des codes opération n'était pas encore vérifié et testé, comme l'avait montré la découverte en juillet 2010 d'une vulnérabilité rendue possible par certains opérateurs binaires (CVE-2010-5137). C'est pourquoi il a été décidé à la fin de l'année 2010, sous l'impulsion de Gavin Andresen, de restreindre la facilité de programmation du système [4].

Cette restriction a été appliquée en imposant des schémas standards de scripts, qui faisaient que les nœuds configurés par défaut ne relayaient plus les transactions contenant des scripts qui ne respectaient pas ce standard. Il ne s'agissait pas ainsi d'une restriction des règles globales de consensus, mais des règles locales de mempool qui s'appliquent à la transmission des transactions. Des schémas standards rendant les choses plus simples et plus sûres ont ainsi été développés au cours des années. Les schémas standards de sortie transactionnelle étaient en 2023 au nombre de huit : P2PK, P2PKH, P2MS, P2SH, NULLDATA, P2WPKH, P2WSH et P2TR.

P2PK : Pay to Public Key

Le premier schéma s'appelle Pay to Public Key (P2PK), qu'on peut traduire littéralement en français par « payer à la clé publique ». Il s'agit de créer une pièce liée à la clé publique d'un destinataire, que lui seul peut dépenser en signant avec sa clé privée. Le script de verrouillage permettant ce type d'envoi est :

```
<clé publique> CHECKSIG
```

La présence de la clé publique explique qu'on parle parfois de « scriptPubKey » pour désigner le script de verrouillage en général, indépendamment de ce qu'il contient.

Au moment de la dépense, le destinataire doit utiliser un script de déverrouillage contenant simplement sa signature :

```
<signature>
```

La présence de la signature dans ce script explique qu'on parle parfois de « scriptSig » pour désigner le script de déverrouillage en général, indépendamment de ce qu'il contient. L'exécution successive de ces deux scripts

permet, comme on l'a vu, de vérifier que la signature fournie par l'utilisateur correspond à sa clé publique, auquel cas elle est valide.

Le schéma P2PK était utilisé dans les débuts de Bitcoin pour recevoir les paiements par IP (P2IP) et pour récupérer la récompense de minage. Il est aujourd'hui tombé en désuétude au profit d'un schéma rival : P2PKH.

P2PKH : Pay to Public Key Hash

Le schéma Pay to Public Key Hash (P2PKH), qui est traduit littéralement par « payer à l'empreinte de la clé publique », est le deuxième type de format de réception apparu dans Bitcoin dès le début du fait de la conception de Satoshi Nakamoto. Ce schéma permet non pas de réaliser un paiement vers une clé publique, mais vers l'empreinte d'une clé publique, tout en faisant en sorte que l'interpréteur vérifie quand même la validité de la signature vis-à-vis de la clé publique lors de la dépense des fonds. L'empreinte de la clé publique est alors considérée comme la donnée essentielle (« charge utile ») de l'adresse, qui dans ce cas commence toujours par un 1, comme par exemple `1FjBKPQ7MTiPSDkJ2ZwPgAXUKQ8yoGbVJX`. Le script de verrouillage ici est :

```
DUP HASH160 <empreinte de la clé publique> EQUALVERIFY CHECKSIG
```

Et le script de déverrouillage est :

```
<signature> <clé publique>
```

L'exécution des deux scripts permet de : 1) vérifier que le passage de la clé publique par la fonction de hachage HASH-160 est égale à l'empreinte qui est spécifiée dans le script ; 2) vérifier que la signature correspond à la clé publique.

L'avantage de ce schéma est qu'il permet d'avoir des adresses plus courtes (l'information à encoder n'est que de 20 octets au lieu de 33 ou 65 octets pour une clé publique), raison pour laquelle Satoshi Nakamoto l'a implémenté. De plus, en ne révélant la clé publique qu'au moment de la dépense, ce schéma accroît aussi la sécurité contre la menace (très hypothétique) de l'ordinateur quantique.

P2MS : Pay To MultiSig

Le schéma Pay To MultiSig (P2SH), qui signifie littéralement « payer à la multisignature », est un schéma de signature multipartite exigeant la signature de M personnes parmi N participants prédéterminés (« M-parmi-N », ou

« M-of-N » en anglais). Il a été rendu standard sous une forme limitée à 3 participants en mars 2012 avec la sortie de la version 0.6.0 du logiciel. Le script de verrouillage est le suivant :

```
M <clé publique 1> ... <clé publique N> N CHECKMULTISIG
```

Le script de déverrouillage correspondant est :

```
<leurre (0)> <signature 1> ... <signature M>
```

La présence du leurre (généralement 0) est dû à un défaut dans l'implémentation de l'exécution de l'opérateur `OP_CHECKMULTISIG` par Satoshi, qui requiert un élément de trop. Les développeurs n'ont pas jugé opportun de corriger ce défaut, car cette correction constituait un hard fork.

C'est ce schéma, particulièrement exigeant au niveau de la mise en place, qui a motivé la création du schéma P2SH.

P2SH : Pay to Script Hash

Le schéma Pay to Script Hash (P2SH), pouvant être traduit littéralement par « payer à l'empreinte du script », reprend l'idée derrière P2PKH, à la seule différence que la donnée hachée n'est pas une clé publique, mais le script lui-même ! Le script en question est alors appelé script de récupération (*redeem script*) pour le différencier du script de déverrouillage. Son empreinte est la donnée constitutive de l'adresse, cette dernière commençant toujours par un 3 à l'instar de `3K8Ps6Ayw5ZaKDaLZjfGo3mTgDsc1VXZ8d`.

Ce schéma donne à l'utilisateur la possibilité d'y inclure n'importe quel script, sans discrimination sur son format, à condition qu'il respecte bien sûr certaines limites. Il permet aussi de recevoir des fonds depuis la quasi-totalité des portefeuilles existants, le fardeau de la construction et du déverrouillage du script revenant uniquement au destinataire, et n'est pas partagé à l'expéditeur comme dans le cas de l'utilisation de scripts bruts.

Le script de verrouillage pour le schéma P2SH est :

```
HASH160 <empreinte du script de récupération> EQUAL
```

Et le script de déverrouillage est un script de la forme :

```
[éléments de déverrouillage] <script de récupération>
```

L'exécution de P2SH est plus complexe que pour les précédents schémas, ce qui peut s'expliquer par le contexte dans lequel il a été développé. L'idée

d'implémenter un schéma de script qui utilise l'empreinte d'un autre script comme l'empreinte de clé publique dans le schéma P2PKH est née en 2011 par l'intermédiaire de plusieurs propositions. Elle a été rendue plus concrète avec la proposition de l'opérateur `OP_EVAL` par Nicolas van Saberhagen le 2 octobre, un code opération qui permettait l'exécution récursive d'un script à l'intérieur d'un autre script [5]. Gavin Andresen a expliqué comment en faire un soft fork par le remplacement de l'instruction sans effet `OP_NOP1` [6].

L'opérateur `OP_EVAL` devait permettre de former un nouveau schéma standard. Le script de verrouillage aurait été :

```
DUP HASH160 <empreinte du script de récupération> EQUALVERIFY EVAL
```

tandis que le script de déverrouillage aurait été le même que pour P2SH. L'exécution successive de ces deux scripts aurait permis dans un premier temps de vérifier la conformité du hachage du script de récupération avec l'empreinte ; puis dans un second temps d'exécuter le script de récupération et de lui combiner les éléments de déverrouillage. Néanmoins cette solution n'a pas été acceptée, celle-ci ayant été jugée trop dangereuse à cause de son pouvoir de récursion. Il lui a été préféré le modèle, plus restrictif, de P2SH.

L'exécution de P2SH fonctionne exactement comme le schéma lié à `OP_EVAL`, à l'exception qu'une partie du script n'est pas explicitement indiquée. D'un côté, la vérification de la correspondance entre l'empreinte indiquée et le script de récupération est bien réalisée par le script de verrouillage. De l'autre côté, l'évaluation du script de récupération est effectuée implicitement grâce à une exception ajoutée au code source qui fait que les nœuds du réseau qui reconnaissent le schéma l'interprètent différemment. Dans Bitcoin Core, on peut observer cette condition au sein de la fonction `VerifyScript` de l'interpréteur.

La proposition a été codifiée dans le BIP-16. Si cette solution est pratique, elle crée de la complexité et n'est pas très élégante. Comme le disait Gavin Andresen dans l'explication introductive de ce BIP :

> « Reconnaître une forme "spéciale" de scriptPubKey et réaliser une validation supplémentaire quand elle est détectée, c'est laid. Cependant, l'avis général est que les alternatives sont soit encore plus laides, soit plus complexes à implémenter, et / ou étendent le pouvoir du langage d'expression de manière dangereuse [7]. »

Le schéma P2SH a fini par être activé le 1er avril 2012 sous la forme d'un soft fork, en dépit de l'opposition notable de Luke-Jr qui proposait un opérateur alternatif, `OP_CHECKHASHVERIFY`, décrit dans le BIP-17.

NULLDATA

Le schéma NULLDATA, signifiant littéralement « données insignifiantes », est un schéma d'inscription de données arbitraires sur la chaîne. Il est le quatrième schéma classique et a été rendu standard avec l'arrivée de la version 0.9.0 de Bitcoin Core en mars 2014. Il se base sur l'instruction `OP_RETURN` dont l'effet est de mettre fin à l'exécution du script et de rendre indépensable la pièce correspondante [8]. Le script de verrouillage du schéma commence toujours par `OP_RETURN` et est suivi des données empilées :

```
RETURN [données arbitraires]
```

La sortie contenant ce script est exempte de la limite standarde de poussière, qui est actuellement de 546 satoshis pour les sorties P2PKH, de sorte qu'elle peut être de 0 satoshi. La taille maximale des données pouvant être inscrites est de 80 octets par transaction sur BTC. De plus, en raison de leur caractère assurément indépensable, les sorties peuvent être retranchées de l'ensemble des UTXO des nœuds. Tout ceci fait de ce schéma le moyen normal d'inscrire des informations sur le registre.

Les types de signatures

La programmabilité de Bitcoin n'est pas seulement issue de son langage de programmation mais aussi du système de signature qui permet de sélectionner quelle partie de la transaction est signée. Ce facteur de programmabilité est mis en œuvre par l'existence d'un indicateur, appelé type de hachage de la signature ou *signature hash type*, qui est ajouté à la transaction non signée, puis à la signature elle-même. Celui-ci indique quelle partie de la transaction doit être hachée avant d'être soumise à l'algorithme de signature, d'où son nom.

Le type de signature est construit à partir de plusieurs signaux de signature qui peuvent être combinés. Les quatre signaux de signature qui existent sont :

— `SIGHASH_ALL` (`0x01`) qui indique que toutes les sorties sont signées ;
— `SIGHASH_SINGLE` (`0x03`) qui permet de ne signer qu'une seule sortie ;
— `SIGHASH_NONE` (`0x02`) qui indique qu'aucune sortie n'est signée ;
— `SIGHASH_ANYONECANPAY` (`0x80`) qui permet de ne signer qu'une seule entrée.

Les trois signaux concernant les sorties peuvent être associés à `SIGHASH_ANYONECANPAY`, ce qui permet de former finalement six types de signatures différents, représentés sur la figure 12.6. Le type de signature le plus fréquent

est évidemment `SIGHASH_ALL` même si certains autres types peuvent parfois trouver une utilité. C'est notamment le cas de `SIGHASH_ALL | SIGHASH_ANYONECANPAY` qui permet de construire des transactions de type *anyone-can-pay*, dont les sorties sont déterminées, mais où chacun peut signer sa propre entrée sans connaître les autres.

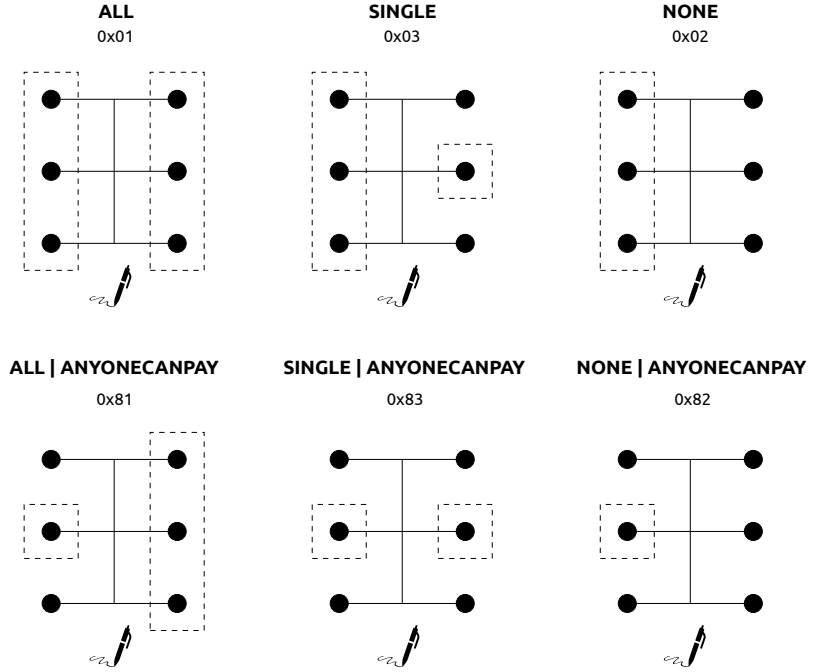

FIGURE 12.6 – Les différents types de signatures dans Bitcoin.

Ces signaux ont été implémentés dès le début par Satoshi Nakamoto au sein du prototype. Il en manquait logiquement un, que Satoshi Nakamoto a probablement jugé inutile : celui qui ne signait aucune entrée. Toutefois, avec le développement des canaux de paiements pour le réseau Lightning, les développeurs se sont rendu compte qu'il pouvait avoir une utilité. C'est dans cet esprit que le signal de signature `SIGHASH_NOINPUT` a été proposé en février 2016 par Joseph Poon [9].

Ce type de signal pourrait être implémenté de manière partielle dans BTC par l'intermédiaire du BIP-118, qui prévoit l'intégration de deux nouveaux signaux au sein des scripts de Taproot : `SIGHASH_ANYPREVOUT` et `SIGHASH_ANYPREVOUTANYSCRIPT`. Il permettrait d'améliorer le fonctionnement du

réseau Lightning par la mise en œuvre du protocole Eltoo reposant sur la construction de transactions flottantes.

SegWit : le témoin séparé

SegWit, abréviation de *Segregated Witness*, qu'on peut traduire littéralement par « témoin séparé », est une mise à niveau du protocole ayant lieu sur Litecoin-LTC et sur Bitcoin-BTC en 2017. Elle a consisté à faire en sorte que les données de déverrouillage des entrées transactionnelles, telles que les signatures, se retrouvent dans une structure de données séparée (*segregated*) appelée le témoin (*witness*) afin de supprimer la malléabilité des transactions. SegWit constituait ainsi une restructuration profonde des transactions.

Outre la correction de la malléabilité, SegWit a apporté une augmentation de capacité transactionnelle et un versionnage des scripts pour faciliter les mises à niveau ultérieures. Elle a également amélioré l'algorithme de signature pour éviter les hachages redondants durant la vérification et pour rendre plus sûre la signature hors-ligne.

La malléabilité

SegWit tire son origine du problème de la malléabilité des transactions, un problème identifié depuis janvier 2012. Dans Bitcoin, les transactions sont malléables dans le sens où elles peuvent être modifiées légèrement après leur diffusion sans devenir invalides aux yeux du réseau. Cette propriété vient du fait qu'une signature ne peut pas se prendre en compte elle-même et que, par conséquent, le script de déverrouillage n'est pas signé avec le reste de la transaction. La malléabilité peut ainsi prendre deux formes : la malléabilité intrinsèque à l'algorithme ECDSA, qui se base sur un nombre aléatoire pour produire une signature (malléabilité par le signataire) ; la malléabilité provenant de la forme des signatures et des scripts de déverrouillage des entrées (malléabilité par un tiers).

La malléabilité n'est pas rédhibitoire pour la sécurité des fonds, mais elle permet de modifier l'identifiant de la transaction après sa publication, ce qui peut se révéler problématique dans certaines situations. Ainsi, entre le 9 et le 11 février 2014, Mt. Gox et d'autres plateformes de change ont subi des attaques exploitant cette malléabilité des transactions. Les transactions de retrait ont été modifiées par les attaquants, faisant croire aux plateformes, dont l'infrastructure logicielle était mal configurée, que ces transactions n'avaient pas été confirmées. Les pirates ont vu leurs comptes être recrédités tout en

conservant dans le même temps les bitcoins retirés. Ces attaques ont mené à une perte totale de 64 564 bitcoins [10].

Des propositions ont tenté de corriger la malléabilité par un tiers en contraignant au maximum la forme des transactions. C'est dans cet esprit qu'a été créé le BIP-62 en mars 2014, dont l'une des exigences (l'encodage standard des signatures décrit dans le BIP-66) a été incluse dans les règles de consensus le 4 juillet 2015. Toutefois, ces changements ne s'appliquaient pas à la malléabilité par le signataire, ce qui créait une demande pour une correction généralisée.

Cette malléabilité signifiait que tout acteur participant à un contrat de signature multipartite pouvait modifier la transaction et donc son identifiant à tout moment. Cela altérait significativement la possibilité d'implémentation du réseau Lightning, dont les canaux de paiements, comme on le verra plus bas, se basent sur des transactions non publiées auxquelles il faut faire référence et font intervenir des signatures multiples.

La solution était de mettre de côté les scripts de déverrouillage dans le processus de hachage de la transaction, pour qu'un changement de ces scripts n'influence pas l'identifiant. Cette idée a été proposée initialement par Gregory Maxwell en août 2013 sur IRC, avant d'être mise en œuvre au sein de la version alpha du modèle de sidechain Elements, annoncée le 8 juin 2015 par Blockstream. Le même jour, Gregory Maxwell présentait cette version d'Elements incluant *Segregated Witness* dans un séminaire de développeurs à San Francisco : il décrivait alors le témoin comme « une valeur spécifique qui constitue une preuve concrète d'affirmation existentielle [11] ».

Cette solution a été adaptée pour Bitcoin au cours de l'automne 2015, pour être appliquée comme un soft fork. La mise à niveau SegWit a été officiellement introduite à la communauté par le développeur Pieter Wuille le 7 décembre 2015, lors de la conférence Scaling Bitcoin II à Hong Kong. En substance, elle consistait à déplacer les scripts de déverrouillage dans le témoin de la transaction. Deux identifiants étaient alors calculés : l'identifiant classique (`txid`), qui ne prend pas en compte ce témoin, et l'identifiant complet (noté `wtxid` pour *witness transaction identifier*), qui recouvre l'intégralité de la transaction. Les identifiants complets étaient regroupés dans un second arbre de Merkle, l'arbre témoin, dont la racine était placée dans la transaction de récompense du bloc, ce qui faisait que toutes les données étaient engagées dans le calcul de la preuve de travail. De l'autre côté, les transactions et les blocs restaient valides pour les nœuds n'ayant pas été mis à niveau.

SegWit est active depuis le 24 août 2017. L'absence de script de déver-

rouillage dans le calcul de l'identifiant classique permet de ne plus avoir de malléabilité du tout, ni des signataires, ni d'un tiers extérieur.

L'augmentation de la capacité transactionnelle

SegWit a aussi eu pour effet indirect de créer un bloc d'extension et d'augmenter la capacité transactionnelle. En effet, les nœuds suivant les anciennes règles ne voyaient pas le témoin, de sorte qu'ils ne le comptabilisaient pas dans la taille du bloc. La question était alors de savoir quelle limite mettre sur le témoin.

La réponse a été d'inventer une nouvelle métrique pour mesurer l'impact des transactions et des blocs sur le réseau : le poids (*weight*), qui est une moyenne pondérée de la taille de base et de la taille du témoin. Exprimé en unités de poids (*weight unit*), il est défini comme la somme du quadruple de la taille de base (s_b) et de la taille du témoin (s_w) :

$$w = 4\, s_b + s_w$$

Il en découle une taille virtuelle (s_v) qui est définie comme la somme de la taille de base et du quart de la taille du témoin, c'est-à-dire : $s_v = s_b + \frac{s_w}{4}$. La taille limite des blocs est devenue un poids limite des blocs, qui était de 4 millions d'unités au moment de la mise à niveau et qui était toujours le même en novembre 2023.

De ce fait, les frais qui étaient initialement calculés en satoshis par octet (sat/o), sont, depuis SegWit, mesurés en satoshis par octet virtuel (sat/ov). Les mineurs sélectionnent les transactions en fonction de ce taux afin d'être les plus rentables possibles par rapport à cette limite. Cet effet n'est valable que si la limite est atteinte.

Avec SegWit, il s'agit donc de pondérer l'impact des entrées par rapport à celui des sorties sur le calcul des frais. Si l'activité rejoint le plafond de capacité, alors les sorties sont quatre fois plus chères à inscrire sur la chaîne que les scripts de déverrouillage contenus dans les entrées. La mise à niveau, en plus d'installer une remise qui incite à son usage, a créé une dissuasion à alourdir l'ensemble des UTXO. Le facteur 4 se rapproche de la pondération matérielle [12].

Cette limite de 4 millions d'unités de poids est indicative. La taille réelle des blocs n'atteint généralement pas 4 Mo en raison de la forme des transactions. Les données contenues dans les transactions normales ne sont en effet pas regroupées dans le témoin, de sorte qu'elles ne remplissent pas entièrement l'espace de bloc autorisé. Par exemple, si nous prenons un bloc constitué

uniquement de transactions à 2 entrées et 2 sorties utilisant SegWit, alors sa taille réelle sera de 1,784 Mo [13].

Les transactions dont les données de déverrouillage sont plus grandes profitent mieux de cet espace de bloc supplémentaire. C'est le cas des transactions qui utilisent la multisignature telles que les fermetures de canaux de paiement. Il est ainsi possible d'approcher la taille des 4 Mo en maximisant la taille des données contenues dans le témoin. C'est ce qui a été fait le 1er février 2023 avec la création d'un bloc de 3,955 Mo dont le témoin a servi à l'inscription d'une image [14].

Le versionnage des scripts

Enfin, la mise à niveau SegWit a apporté un versionnage des scripts, qui permettait le déploiement de futures mises à niveau. La version permettait ainsi d'indiquer quelles règles étaient appliquées. La première version de SegWit en 2017 utilisait la version 0, et le déploiement de Taproot en 2021 a été fait au moyen de la version 1.

Trois types de sorties natifs liés à SegWit existent pour l'instant : le schéma P2WPKH, le schéma P2WSH et le schéma P2TR.

P2WPKH : Pay to Witness Public Key Hash

Le schéma *Pay to Witness Public Key Hash* (P2WPKH), qui signifie littéralement « payer à l'empreinte de la clé publique témoin », est le premier schéma mis en place par SegWit. L'empreinte de la clé publique est obtenue par le hachage standard (SHA-256 suivi de RIPEMD-160). Le script de verrouillage apparent est alors :

```
<version (0)> <empreinte (hash160) de la clé publique>
```

Ce script est semblable à un script *anyone-can-spend*, que tout le monde pourrait dépenser, mais l'interpréteur ajoute une condition supplémentaire pour que ce ne soit pas le cas. Le type de la sortie est détecté grâce à sa forme : la version de SegWit (ici 0) et la taille de l'empreinte (ici 20 octets). La version et l'empreinte forment l'information essentielle de l'adresse, qui est encodée grâce au format Bech32 et qui commence toujours par `bc1q`, à l'instar de `bc1q5x9a0aqmgtrucm4l5n0y8e4kxfy9xm4udhygr2`.

Le script de déverrouillage est vide. Les données de déverrouillage sont contenues dans le témoin de la transaction. La partie du témoin correspondant à l'entrée est :

```
<2> <signature> <clé publique>
```

P2WSH : Pay to Witness Script Hash

Le schéma *Pay to Witness Script Hash* (P2WSH), dont la traduction littérale est « payer à l'empreinte du script témoin », est la retranscription de P2SH pour SegWit. L'empreinte du script de récupération est obtenue par SHA-256, par peur d'une collision de RIPEMD-160 dans le cas d'une adresse générée par plusieurs personnes [15]. Le script de verrouillage est le suivant :

```
<version (0)> <empreinte (sha256) du script de récupération>
```

Ce script est encore une fois *anyone-can-spend* de manière apparente. Le type de la sortie est détecté par l'interpréteur grâce à sa forme : la version de SegWit (ici 0) et la taille de l'empreinte (ici 32 octets). L'adresse est à nouveau constituée de ces deux informations et encodée grâce au format Bech32.

Le script de déverrouillage est vide. Les données de déverrouillage sont contenues dans le témoin de la transaction. La partie du témoin correspondant à l'entrée est :

```
<nombre d'éléments + 1> [éléments de déverrouillage] <script de
récupération>
```

Dans les deux cas, l'empreinte est aussi appelée « programme du témoin ».

Les types imbriqués (P2SH-P2WPKH, P2SH-P2WSH)

SegWit a aussi modifié le format P2SH pour inclure de nouvelles exceptions. Ces exceptions correspondent aux types imbriqués (*nested*) P2SH-P2WPKH et P2SH-P2WSH. Leur fonctionnement consiste à inclure les scripts de verrouillages précédents (version + empreinte) dans une sortie P2SH en tant que scripts de récupération. Le script de récupération est alors exécuté différemment pour faire appel aux données contenues dans le témoin.

Ces types imbriqués ont permis de faciliter la transition vers SegWit en rendant les portefeuilles non mis à jour capables d'envoyer des fonds vers ces adresses. L'utilisation d'adresses SegWit natives reste néanmoins plus avantageuse.

P2TR : Pay to Taproot

Le dernier schéma à entrer en vigueur est le schéma *Pay to Taproot* (P2TR), dont le nom peut être traduit par « payer à Taproot ». Ce schéma permet de

recevoir un paiement sur une clé publique externe qui cache une clé privée servant à signer les transferts de fonds, ou bien la racine pivot d'un arbre de Merkle contenant les clauses d'un contrat autonome (MAST). Puisque la destination du paiement est une clé publique, il s'agit en quelque sorte d'un retour au P2PK. Le script de verrouillage présent dans la sortie transactionnelle est :

```
<version (1)> <clé publique Taproot>
```

La clé publique en question mesure 32 octets. La version et la clé publique constituent les éléments constitutifs de l'adresse. Cette dernière est encodée grâce au format Bech32m, qui est une variante de l'encodage Bech32 ayant corrigé un petit bug dans le calcul de la somme de contrôle. L'adresse résultante commence toujours par `bc1p` comme par exemple `bc1pqlqqhzrg60v5h87r8lugusrddgz0j306shcupthy0tdqaqurwn8qr8qsej`. Le déverrouillage de la sortie se fait avec une signature simple, ou bien avec l'exécution du MAST.

Toutes ces modifications majeures font de SegWit une mise à niveau profonde du protocole, qui a amené beaucoup de choses dans Bitcoin. L'exigence de passer par un soft fork explique la forme qu'elle a prise et elle ne peut par conséquent être comprise que dans le contexte dans lequel elle a été activée. Toutefois, cette mise à niveau a aussi apporté des inconvénients majeurs, dont les deux principaux sont la dette technique alourdissant le coût de maintien et d'amélioration du code, et l'affaiblissement de la confidentialité générale due à l'apparition de nouveaux types d'adresses partiellement adoptés. SegWit était donc loin d'être une mise à niveau parfaite.

Le mélange de pièces

Le fait que les transactions soient publiées sur la chaîne entraîne une surveillance. Comme nous l'avons fait remarquer précédemment, il est possible de faire des suppositions pour deviner ce qui se passe réellement sur la chaîne, en admettant que l'utilisateur cherche à minimiser les frais payés au sein de ses transactions. Ces heuristiques (telles que l'heuristique de codépense, l'heuristique de la sortie complémentaire ou encore l'heuristique de l'empreinte du portefeuille) forment la base d'une discipline appelée l'analyse de chaîne qui consiste à recouper ces observations avec l'identification d'acteurs réels afin de tirer des conclusions sur leur activité économique effective. C'est pourquoi on parle parfois de « transparence » de la chaîne.

Cependant, cette transparence est toute relative, car les données de la chaîne ne révèlent pas l'identité des personnes : le système est pseudonyme,

dans le sens où il recense les mouvements entre les adresses, et pas entre les personnes. Le modèle de confidentialité de Bitcoin, décrit par Satoshi Nakamoto dans le livre blanc en 2008, consiste ainsi à garder secret le lien qui existe entre l'identité d'une personne et ses adresses [16].

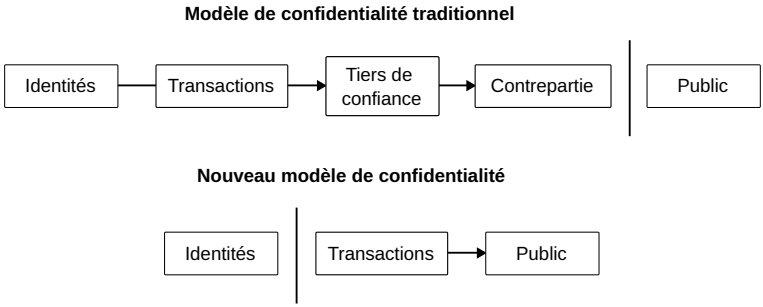

FIGURE 12.7 – Modèle de confidentialité présenté dans le livre blanc de Bitcoin.

Ce modèle de confidentialité possède des faiblesses évidentes : les fuites d'information accidentelles, qui ont toujours lieu en ce qui concerne le numérique, et la divulgation volontaire de l'identité de l'utilisateur par son interlocuteur dans l'échange. Par conséquent, nul ne peut prétendre exercer une activité complètement secrète qui échapperait absolument à la surveillance. C'est pour cette raison qu'il existe des méthodes permettant de limiter l'effet de ces révélations afin de restaurer sa confidentialité en toute sérénité.

La première mesure est l'usage unique des adresses. Elle consiste à générer une nouvelle clé privée et une nouvelle adresse lors de chaque paiement entrant ou sortant. L'apport de cette pratique est de réduire l'impact de la divulgation du lien avec l'identité sur la confidentialité générale : tant que l'adresse n'est pas liée à d'autres par l'observation d'une action sur la chaîne (codépense par exemple), la fuite d'information se limite à cette seule adresse. Cette bonne pratique, citée dans le livre blanc [17], est aujourd'hui implémentée dans tous les bons portefeuilles.

Au-delà de la prévention, il existe également des méthodes pour corriger ses erreurs. La plus connue d'entre elles est le mélange de pièces, qui consiste à combiner ses UTXO avec les UTXO d'autres utilisateurs afin de briser les liens déterministes qui existent entre les pièces et l'identité de leurs propriétaires.

Le mélange de bitcoins était originellement pris en charge par des services de mixage centralisés, appelés *mixers* ou *tumblers*, qui recevaient les bitcoins des utilisateurs, les fusionnaient et leur renvoyaient des bitcoins communs au

bout d'un certain temps, préférablement sous la forme de plusieurs transactions. Le premier mélangeur de ce type était BitLaundry, une plateforme qui a été lancée en septembre 2010 par Peter Vessenes. Ces services permettaient d'obscurcir la provenance des bitcoins pour un observateur extérieur, mais pas pour leurs gestionnaires, qui pouvaient aussi s'emparer des bitcoins au passage, ce qui constituait un risque double.

Une technique pour procéder à ce type de mélange sans devoir passer par un intermédiaire a été développée par la suite : c'était CoinJoin, dont la description formelle a été faite en août 2013 par Gregory Maxwell [18]. Cette méthode consiste à impliquer les pièces dans une transaction jointe collaborative qui brise la correspondance entre les entrées et une partie des sorties. La transaction classique que l'on se représente est celle de plusieurs utilisateurs qui signent chacun une entrée, dont le même nombre de sorties possèdent un montant égal, et dont le reste des sorties forment les sorties complémentaires. Dans ce cas, les sorties complémentaires sont toujours liées aux entrées, contrairement aux sorties principales qui sont indiscernables les unes des autres.

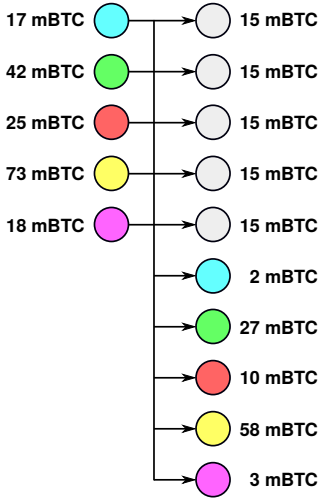

FIGURE 12.8 – Exemple d'une transaction CoinJoin à 5 utilisateurs.

Ces mélanges reposent sur la notion d'« ensemble d'anonymat » (*anonymity set*) qui permet de mesurer la difficulté à faire le lien entre l'entrée et la sortie à un moment donné. On peut ainsi obtenir un score prospectif qui est le nombre de possibilités de pièces en sorties auxquelles peuvent correspondre

une pièce en entrée. Dans notre exemple illustré par la figure 12.8, le score prospectif de la sortie au moment de la transaction est de 5. Si la pièce avait subi un nouveau mélange (comme c'est fait dans Whirlpool), alors elle aurait eu un score prospectif de 9. De même, si l'une des autres pièces avait été incluse dans un nouveau mélange, alors le score de la pièce observée aurait augmenté d'autant. On peut aussi calculer un score rétrospectif qui correspond au nombre de potentielles pièces en entrée auxquelles peut être liée une sortie particulière, qu'on suppose être de 5 dans le cas de notre transaction simple, mais qui peut être largement supérieur si une ou plusieurs pièces ont déjà fait l'objet de mélanges successifs [19].

Pour gérer le tout, le système utilise généralement un protocole qui permet aux participants d'être mis en relation anonymement par le biais d'un coordinateur sans risque de fuite d'information ou de vol des fonds. Le plus connu est ZeroLink, développé par Adam Ficsor et William Hill en août 2017, qui est un protocole qui utilise le procédé de signature aveugle de David Chaum [20]. C'est en ce sens qu'on parle parfois de CoinJoin chaumien (*Chaumian CoinJoin*). Une implémentation classique de cette idée a été réalisée par Whirlpool (Samourai Wallet [21]) et par Wasabi 1.0. De plus, des variantes (CoinShuffle, CoinShuffle++, CashShuffle, CashFusion) ont été implémentées sur des variantes de Bitcoin comme Decred ou Bitcoin Cash. Plus récemment le portefeuille Wasabi a intégré Wabisabi qui permet de réaliser des mélanges avec des valeurs arbitraires en sortie, ce qui complique l'estimation de la confidentialité apportée mais évite d'avoir à gérer les sorties complémentaires d'une manière séparée.

Pour autant, les transactions collaboratives ne se limitent pas à CoinJoin. Il existe par exemple une autre méthode, appelée PayJoin, qui permet au commerçant de réaliser un mélange avec le client au moment du paiement, en impliquant une pièce en entrée. Cette opération a pour effet de fausser l'analyse de chaîne en faisant croire à l'observateur extérieur qu'un seul utilisateur a réuni ses pièces en entrée et en cachant le montant réel du paiement.

Reprenons notre exemple d'Alice qui paie 7 mBTC à Bob en réunissant deux pièces de 6 et 2 mBTC afin d'atteindre un montant suffisant en entrée. Dans ce cas, les deux entrées sont supposément liées entre elles (heuristique de codépense) et liées à la sortie de 1 mBTC (heuristique de la sortie complémentaire). Ici, comme représenté sur la figure 12.9, l'application de PayJoin consiste pour le commerçant à inclure une ou plusieurs pièces en entrée et à augmenter d'autant le montant de la sortie qui lui est destinée, de 7 mBTC par exemple.

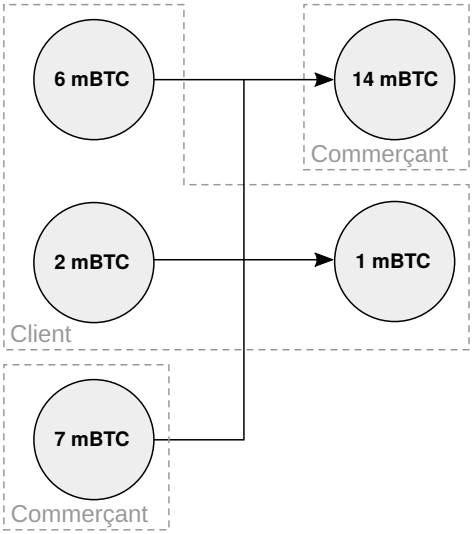

FIGURE 12.9 – Exemple d'une transaction PayJoin.

Cette technique a été conceptualisée en 2018 de plusieurs manières indépendantes, notamment par le biais du protocole de paiement Pay-to-EndPoint (P2EP) et par les transactions Stowaway de Samourai Wallet. Leur implémentation s'est faite respectivement en 2019 pour les transactions Stowaway et en 2020 pour P2EP.

Enfin, une dernière méthode qui s'inscrit dans la logique du mélange de pièces est Coinswap, qui est un procédé développé par Chris Belcher, permettant à deux utilisateurs ou plus d'échanger leurs pièces sans qu'ils aient besoin de se faire confiance et sans que cette opération laisse une trace particulière sur la chaîne [22]. Cette technique comporte cependant un inconvénient supplémentaire dans le sens où l'une des parties récupère l'historique entier de la pièce de l'autre, et doit en assumer l'éventuelle responsabilité.

D'autres techniques de confidentialité

Outre le mélange de pièces simple consistant à brouiller les pistes qu'un observateur externe pourrait suivre, il existe un certain nombre de techniques qui permettent d'améliorer la confidentialité de Bitcoin. Celles-ci requièrent souvent la modification du protocole de base et représentent des compromis, raison pour laquelle elles ne sont pas forcément mises en œuvre.

Ces techniques ont été développées dans les années qui ont suivi l'apparition de Bitcoin, notamment sur le forum Bitcointalk. N'étant probablement pas un cryptographe universitaire, Satoshi Nakamoto s'est surtout focalisé sur la robustesse du système lorsqu'il l'a conçu et n'a pas cherché à y inclure des techniques avancées. Cependant, il était ouvert à toutes les propositions qui permettraient de créer une « mise en œuvre de Bitcoin bien meilleure, plus facile et plus pratique [23] ».

La première technique de cet ordre est le procédé de signature de cercle (*ring signature*), qui a été formalisé en 2001 par Ronald Rivest, Adi Shamir et Yael Tauman. Celui-ci se base sur le procédé de signature de groupe, introduit par David Chaum et Eugène van Heyst en 1991, qui permettait à chaque membre d'un groupe de signer un message au nom du groupe sans que ce membre puisse être identifié par un vérificateur externe, mais qui reposait sur un administrateur central. La signature de cercle innovait par le fait qu'elle ne requérait pas d'administrateur, pas de procédure d'installation, pas de coordination, et qu'elle ne permettait pas à un membre de révoquer son anonymat.

En ce qui concerne la cryptomonnaie, le principe est le suivant : pour chaque pièce en entrée de la transaction, le signataire rassemble plusieurs autres pièces disponibles sur la chaîne (appelées sorties leurres ou *decoy outputs*), utilise leurs clés publiques et signe avec sa clé privée. Il fournit également une image de clé (*key image*) correspondant à la pièce, qui est écrite sur la chaîne et qui permet de garantir que la même pièce n'est pas dépensée deux fois. Plus le cercle implique de sorties, plus l'ensemble d'anonymat est grand. Le compromis est que l'utilisation des sorties transactionnelles en tant que leurres oblige les nœuds à conserver l'ensemble de ces sorties, puisqu'on ne peut pas savoir laquelle a été réellement dépensée.

La deuxième technique est le procédé des adresses furtives, qui a été décrit en 2011 par Nicolas van Saberhagen et qui a été formalisé en 2014 par Peter Todd dans le cadre de Bitcoin [24]. Il utilise essentiellement le schéma d'échange de clés Diffie-Hellman basé sur les courbes elliptiques, abrégé en ECDH, afin de permettre de générer des adresses à usage unique.

Le fonctionnement de base est le suivant. Le destinataire génère une clé privée et en déduit une clé publique qu'il transmet sous la forme d'une méta-adresse. L'expéditeur génère une clé privée éphémère, appelée clé privée de la transaction, et calcule la clé publique correspondante. Ils peuvent calculer un secret partagé à partir de leur clé privée et de la clé publique de l'autre (ECDH). L'expéditeur utilise ce secret et la clé publique du destinataire pour construire

une adresse à usage unique et y envoie les fonds, que seul le destinataire peut dépenser sous condition de connaître la clé publique de transaction (qui peut être stockée dans une sortie NULLDATA). Au lieu d'utiliser une seule paire de clés, le destinataire peut également en utiliser deux pour qu'elles aient des rôles séparés : les clés d'inspection (*view keys*) et les clés de dépense (*spend key*). La clé privée d'inspection est le seul élément non public qui intervient dans la construction de l'adresse côté destinataire et sert donc à identifier les sorties correspondant à l'adresse en question. La clé privée de dépense est celle qui sert, comme son nom l'indique clairement, à dépenser les fonds [25].

Si elle est implémentée de manière externe au protocole, cette méthode a l'inconvénient d'exiger de balayer l'entièreté de la chaîne de blocs pour savoir si on a reçu un paiement. C'est dans l'idée d'éviter cette charge que le BIP-47 a été proposé.

Le BIP-47 formalise ainsi une autre méthode apparentée aux adresses furtives, plus complexe, qui est celle des codes de paiement réutilisables (*reusable payment codes*) et qui a été implémentée sous la forme des PayNyms dans les portefeuilles Samourai et Sparrow. Une autre méthode apparentée et plus complexe est celle des codes de paiement réutilisables (*reusable payment codes*) formalisés par Justus Ranvier dans le BIP-47, qui a été implémentée sous la forme des PayNyms dans les portefeuilles Samourai et Sparrow. Dans ce procédé, les codes de paiement de deux participants permettent de dériver les adresses de réception grâce à la dérivation de clés. Cela implique qu'il faut qu'ils connaissent leurs codes de paiement respectifs, et qu'au moins l'un de ces deux codes reste secret. Le code de paiement du destinataire est généralement public, de sorte que c'est celui de l'expéditeur qui doit être caché. Ce dernier est transmis de manière chiffrée sous la forme d'une transaction de notification envoyée à l'adresse du destinataire. Ce schéma a donc pour gros défaut d'exiger la réalisation d'une transaction (et le paiement des frais lié) pour ajouter un destinataire possible.

Une dernière variante est le procédé des paiements silencieux (*silent payments*), proposé en 2022 par Ruben Somsen [26], qui évite la charge de la notification en utilisant la clé publique de l'une des entrées de la transaction, et réduit la charge du balayage de la chaîne, en se limitant à l'ensemble des UTXO ou à un sous-ensemble comme les sorties P2TR par exemple.

La technique des signatures de cercle et le procédé des adresses furtives ont été combinés en 2013 dans le concept de cryptomonnaie CryptoNote par Nicolas van Saberhagen [27]. Dans celui-ci, les nœuds ont besoin de conserver l'ensemble des sorties transactionnelles (car le procédé des signatures de

cercle dissimule le fait qu'une sortie a été dépensée) et chaque portefeuille a besoin de balayer l'ensemble de ces sorties pour voir s'il a reçu un paiement. L'intégration des *stealth addresses* au protocole permet de publier la clé publique éphémère directement dans la transaction (ce qui en fait une clé de transaction) et d'éviter la nécessité de notification. Le concept a été implémenté initialement dans le très douteux Bytecoin en mars 2014, avant de se retrouver dans Monero en avril de la même année, qui en est aujourd'hui le représentant principal, mettant notamment en œuvre des signatures de cercle à 16 membres.

La troisième technique d'amélioration de la confidentialité est le procédé des *Confidential Transactions*, qui permet de dissimuler les montants impliqués dans les échanges des utilisateurs, et qui en toute logique devrait plutôt s'appeler *Confidential Amounts*. Le procédé a été décrit par Adam Back en 2013 et a été formalisé par Gregory Maxwell en 2015 [28]. Il impose à chaque sortie transactionnelle de contenir un engagement de Perdersen (*Pedersen commitment*) qui lie la pièce à la clé publique du destinataire sans la dévoiler, et une preuve de portée (*range proof*) qui est une preuve à divulgation nulle de connaissance (ZKP) démontrant la validité du montant sans le révéler.

Les Confidential Transactions ont été ajoutées en 2017 à Monero grâce au travail de Shen Noether. RingCT, qui permet de cacher les montants échangés, a ainsi été ajouté au protocole en janvier 2017 et a été rendu obligatoire en septembre de la même année. Il alourdissait les transactions par rapport aux transactions classiques. Néanmoins, depuis octobre 2018, ce compromis a été atténué grâce à l'implémentation des bulletproofs, qui a allégé le fardeau des preuves de portée et qui a permis de réduire de 80 % la taille des transactions [29].

Un autre concept faisant usage des Confidential Transactions est Mimblewimble. Celui-ci a été proposé le 1er août 2016 par un inconnu se faisant appeler Tom Elvis Jedusor au sein du canal IRC `#bitcoin-wizards` où il partageait un lien vers un texte descriptif hébergé sur Tor [30]. Mimblewimble a attiré l'attention de certains développeurs de Bitcoin, dont le mathématicien Andrew Poelstra qui en a fait une description plus avancée dans un papier daté du 6 octobre 2016 [31].

L'apport de Mimblewimble est de condenser l'historique des transactions en chamboulant la structure des transactions. Il repose sur trois primitives cryptographiques : les Confidential Transactions, qui cachent les montants, les signatures agrégées à sens unique (OWAS), qui permettent de combiner les transactions au sein d'un bloc, et le sectionnage des transactions (*transaction cut-through*), qui permet de supprimer les sorties transactionnelles intermé-

diaires. Cette réduction, qui améliore la confidentialité du système de manière relativement légère, se fait au prix de la programmabilité, rendue directement impossible.

Mimblewimble a été mis en œuvre de manière native au sein du système Grin développé par Ignotus Peverell à partir d'octobre 2016 et lancé le 15 janvier 2019. Une autre implémentation, également lancée en janvier 2019, était le réseau Beam. Mimblewimble a également été intégré à Litecoin le 20 mai 2022 sous la forme d'un soft fork de bloc auxiliaire, appelé MWEB pour *MimbleWimble via Extension Blocks*.

Enfin, il existe d'autres techniques d'anonymisation basées sur des preuves à divulgation nulle de connaissance. Les plus connues ont été popularisées au moyen de deux protocoles rendus publics en 2013 et en 2014 par Matthew Green et ses étudiants : Zerocoin et Zerocash [32]. Le premier protocole, Zerocoin, permet de cacher la provenance des fonds. Le second protocole permet de cacher la provenance, la destination et les montants, au moyen de zk-SNARK (*Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge*).

Zerocoin a été implémenté dans Zcoin en septembre 2016. À partir de 2019, Zcoin s'est progressivement éloigné du Zerocoin en adoptant les protocoles Sigma et Lelantus, et est devenu Firo en 2020. Zerocash a lui été implémenté au sein du système Zcash en octobre 2016. L'utilisation de preuves à divulgation nulle de connaissance demandait une configuration de confiance des paramètres publics. Tandis que les développeurs de Zcoin qui ont fait le choix d'utiliser des paramètres connus, ceux de Zcash ont décidé d'organiser un évènement, appelée « *The Ceremony* », dans le but de générer ces paramètres. Cette cérémonie a eu lieu du 21 au 23 octobre 2016 et a réuni six participants : Andrew Miller, Peter Van Valkenburgh, Zooko Wilcox-O'Hearn, Derek Hinch, Peter Todd et surtout Edward Snowden sous le pseudonyme de John Dobbertin [33]. Cette configuration de confiance a été rendue inutile en 2022 avec l'intégration du protocole Halo.

De manière générale, tous ces procédés supposent des compromis au niveau de la scalabilité (les preuves sont plus lourdes qu'une simple signature), au niveau de l'auditabilité (ne pas voir les montants implique de devoir faire entièrement confiance aux procédés et à leur implémentation) et au niveau de la programmabilité (programmer des pièces s'oppose au fait de les rendre indistinctes). C'est pourquoi ils ont tous été mis en œuvre dans des versions alternatives de Bitcoin et pas dans sa version principale (BTC), la communauté de cette dernière étant plus conservatrice par nature.

Une machine complexe

Bitcoin forme ainsi une machine qui peut sembler, à première vue, assez complexe. Cet enchevêtrement s'explique par ses objectifs et par les évènements qui ont jalonné son histoire technique. Son but premier – être une monnaie – est à l'origine de la représentation des bitcoins en circulation par des sorties transactionnelles non dépensées, une représentation qui rend la parallélisation plus facile et favorise la confidentialité des échanges (pouvant elle-même être accrue par le mélange des pièces et les techniques cryptographiques dédiées).

De plus, la volonté de Satoshi d'automatiser divers mécanismes lui a fait intégrer un véritable système de programmation au sein du protocole. Celui-ci permet de mettre en place des contrats autonomes qui exécutent des interactions financières complexes entre plusieurs participants. Il facilite aussi, indirectement, l'inscription de données arbitraires sur la chaîne. Ces deux utilisations (contractuelle et notariale) forment les deux cas d'usage secondaires de Bitcoin, dont nous parlerons dans le prochain chapitre.

13

Les contrats autonomes

Un contrat autonome, de l'anglais *smart contract*, est un programme informatique dont l'exécution ne nécessite pas l'intervention d'un tiers de confiance. On parle aussi de contrat auto-exécutable ou de contrat intelligent (traduction littérale). Chaque contrat est constitué de clauses qui sont des conditions de dépense spécifiques.

Bitcoin constitue la première implémentation concrète d'un système hébergeant des contrats autonomes, par le biais de son système de programmation interne qui met en œuvre des scripts au sein des transactions. Il permet d'exécuter une variété de contrats allant du compte multisignatures au canal de paiement, en passant par le dépôt fiduciaire. L'ouverture apportée par cette possibilité facilite l'inscription de données arbitraires sur la chaîne, un cas d'utilisation strictement non monétaire du protocole.

Les contrats simples

La notion de contrat autonome [1] a germé au sein du mouvement cypherpunk dans les années 1990. Elle a été exposée par Nick Szabo en 1994, qui la définissait comme suit :

> « Un contrat autonome est un protocole de transaction informatisé qui exécute les termes d'un contrat. Les objectifs généraux de la conception de contrats autonomes sont de satisfaire les conditions contractuelles courantes (telles que les

> conditions de paiement, les privilèges, la confidentialité et même l'exécution), de limiter au mieux les interruptions tant malveillantes qu'accidentelles, et de minimiser le besoin de recourir à des intermédiaires de confiance [2]. »

Le transfert de valeur constitue le cas le plus simple de contrat autonome, ne contenant qu'une seule clause : la fourniture d'une signature numérique correspondant à une clé publique donnée. Mais une multitude d'autres contrats peuvent être implémentés sur Bitcoin, à tel point qu'il est impossible d'en dresser une liste exhaustive. Nous nous contenterons ici d'en décrire quelques exemples pour expliquer comment ils peuvent être mis en place. Voyons d'abord les cas spécifiques du compte multisignatures, du dépôt fiduciaire, du financement participatif et de l'échange atomique.

Le compte multisignatures

Le compte multisignatures est un compte partagé entre plusieurs entités. Il se base sur le schéma de signature multipartite décrit dans le chapitre 12, dans lequel la dépense des fonds demande M signatures parmi N participants (ce qu'on appelle « M-parmi-N » ou « M-of-N » en anglais). Par exemple, la dépense depuis un compte 2-parmi-3 exige que 2 personnes parmi 3 participants prédéterminés produisent une signature valide, peu importe l'identité précise de ces personnes.

Ce type de contrat est utile pour avoir un compte joint entre époux (2 parmi 2), pour faciliter la détention par une entreprise (3 associés parmi 7 par exemple) ou pour améliorer la conservation de bitcoins en général. Les plateformes d'échange utilisent notamment ce type de contrat pour conserver leurs avoirs. En novembre 2023, la deuxième adresse la plus riche du monde en 2023 était ainsi l'adresse multisignatures 3-parmi-5 de Bitfinex contenant plus de 178 000 BTC [3].

Le dépôt fiduciaire

Le dépôt fiduciaire, appelé *escrow* en anglais, est une méthode basée sur le recours à un tiers de confiance, comme un notaire, pour sécuriser une transaction entre deux parties qui se méfient l'une de l'autre. L'utilisation de la programmabilité de Bitcoin permet de diminuer le pouvoir du tiers en incluant une limite dans la clause qui le concerne. Ce type de contrat repose sur deux briques techniques de base : la signature multipartite et les verrous temporels.

Prenons l'exemple de deux personnes qui ne se connaissent pas, Alice et Bob, et qui veulent réaliser une transaction en ligne : Alice est l'acheteuse, Bob le vendeur. Les deux parties font appel à un intermédiaire de confiance, Lenny, avec qui elles créent le contrat de dépôt fiduciaire. Alice y envoie les fonds et attend de recevoir le bien. Deux clauses peuvent alors être activées :

— Le règlement à l'amiable : le contrat est déverrouillé par les signatures des deux parties, qui peuvent choisir d'envoyer les fonds vers Bob (réussite de l'échange) ou bien de rembourser Alice (échec de l'échange) ;

— Le litige : après une période prédéterminée (par exemple 30 jours), le contrat est déverrouillé par la signature de Lenny et celle de l'une des deux parties ; dans ce cas, Lenny se charge de déterminer qui est la partie honnête et de lui envoyer les fonds.

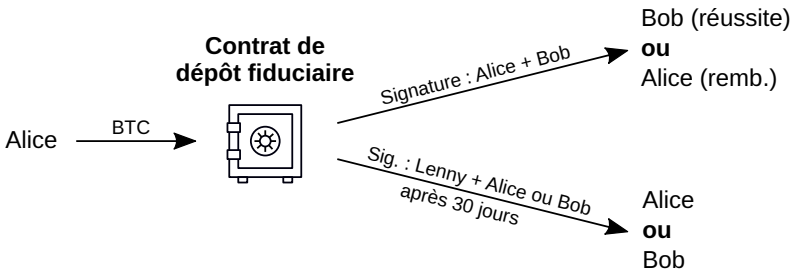

FIGURE 13.1 – Contrat de dépôt fiduciaire.

Ce fonctionnement, décrit sur la figure 13.1, incite d'une part les deux parties à coopérer pour ne pas perdre de temps, et empêche d'autre part la collusion de la tierce partie (Lenny) avec l'une des deux autres avant le délai prévu (30 jours ici). Le recours à la confiance est ainsi minimisé autant que possible.

Ce type de contrat était soutenu par Satoshi Nakamoto dans le livre blanc [4]. En effet, l'irréversibilité des transferts dans Bitcoin offrait peu de garantie pour les commerçants, et le dépôt fiduciaire permettait d'atténuer le problème. C'est typiquement ce genre de mécanisme qui intervient aujourd'hui dans les plateformes de change de pair à pair comme Bisq ou Hodl Hodl, même si l'implémentation diffère de ce qui est présenté ici.

Le financement participatif

Le financement participatif consiste à faire appel au grand public pour contribuer au soutien d'un projet, par opposition au financement par prêt

bancaire ou par levée de fonds auprès des professionnels du capital-risque. Il s'agit le plus souvent d'un accord informel entre le promoteur du projet et le public ayant pour but de soutenir la création d'un bien commun, qui profite à tous. Dans Bitcoin, il est possible d'exécuter cet accord par le biais de promesses de paiement résiliables qui ne sont pas soumises à l'arbitraire d'un tiers de confiance.

D'un point de vue technique, il s'agit de créer une transaction dite *anyone-can-pay* (« tout le monde peut payer ») où la signature de chaque contributeur ne prend en compte que la sortie transactionnelle de la levée de fonds et l'entrée du contributeur en question, donnant la possibilité d'ajouter des entrées (voir figure 13.2). La transaction résultante n'est valide que si le montant en entrée atteint le montant indiqué en sortie, de sorte que les contributeurs conservent le contrôle de leurs fonds jusqu'à la réalisation du paiement total et peuvent se retirer à tout moment.

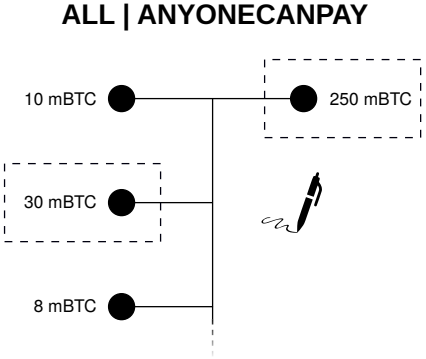

FIGURE 13.2 – Transaction de financement participatif.

Dans le monde du logiciel libre, ce type de financement participatif est particulièrement important, car il n'y a pas de privilège lié à l'écriture du code qui permette de gagner sa vie par la vente de licences. C'est encore plus vrai dans le monde de la cryptomonnaie qui dépend fortement du bon maintien des implémentations logicielles. C'est pourquoi Mike Hearn, qui s'intéressait de près aux capacités de programmation de Bitcoin, s'est vite approprié cette possibilité pour déployer de tels « contrats de garantie » (*assurance contracts*) permettant de financer les biens publics. Il a mis le concept en œuvre au sein de son application Lighthouse, dont une version fonctionnelle est sortie en 2015, qui avait pour but de faciliter le soutien communautaire des projets de l'écosystème. Avec le déclenchement de la guerre des blocs, ce projet a été

mis de côté par Hearn et a fini par être abandonné. Le procédé a été néanmoins repris sur Bitcoin Cash en 2020 par l'intermédiaire de Flipstarter, qui a permis de lever d'importantes sommes pour le financement de l'infrastructure logicielle du protocole.

L'échange atomique

L'échange atomique (*atomic swap*) est une manière sûre d'échanger deux cryptomonnaies fonctionnant sur des chaînes de blocs différentes, sans passer par un intermédiaire de confiance. L'adjectif « atomique » se rapporte à la nature insécable (en grec ancien ἄτομος, átomos) de l'échange : soit les deux parties transfèrent leur dû, soit il ne se passe rien. Le concept a été décrit par Sergio Lerner et Gregory Maxwell en juillet 2012 sur le forum Bitcointalk [5].

L'échange atomique repose sur le concept de contrat verrouillé par une empreinte et par un temps, appelé HTLC par abréviation du terme anglais *Hash Time Locked Contract*. Celui-ci est un contrat à deux clauses, c'est-à-dire que les fonds peuvent être déverrouillés à deux conditions [6] :

— L'accord mutuel : la révélation d'un secret qui est haché par une fonction de hachage et comparé à l'empreinte (*hash*) inscrite dans le contrat ;
— Le litige : l'attente d'un certain temps (*time*) de verrouillage déterminé dans le contrat.

Considérons l'exemple d'un échange atomique entre Alice, qui possède du BTC, et Bob, qui possède du LTC. Alice (*maker*) propose d'échanger 0,03 BTC pour 10 LTC, à un taux de change de 0,003 LTC par BTC, et Bob (*taker*) accepte cet échange. Cette négociation peut avoir lieu par le biais d'un carnet d'ordres public ou privé. Alice choisit au hasard un secret (noté s), qui est un nombre de 32 octets, dont elle fournit l'empreinte cryptographique $H(s)$ à Bob. Ils peuvent ainsi construire un contrat chacun de leur côté pour effectuer l'échange atomique. Son déroulé est décrit au sein de la figure 13.3.

La première phase est la phase d'engagement. D'abord, Alice construit, signe et diffuse une transaction d'engagement envoyant 0,03 BTC vers le contrat d'échange atomique sur la chaîne de Bitcoin. Elle fournit son contenu et son adresse à Bob pour qu'il en vérifie la validité. Puis, elle construit et signe une transaction de remboursement dépensant les fonds de ce contrat qu'elle pourra diffuser après un délai prédéfini (ici 16 heures). Ensuite, une fois que la transaction d'engagement d'Alice a été confirmée, Bob fait de même de son côté : il crée un contrat équivalent sur la chaîne de Litecoin, où il envoie 10 LTC, et en donne le contenu et l'adresse à Alice pour qu'elle s'assure que

tout est en ordre. Enfin, il construit et signe une transaction qui le remboursera au bout d'un délai strictement inférieur à celui de la transaction d'Alice : ici 8 heures. Cette différence résulte du rapport déséquilibré qui existe entre Alice (qui connaît le secret de déverrouillage) et Bob (qui ne le connaît pas).

Lorsque les transactions d'engagement ont toutes deux été confirmées sur leurs chaînes respectives, la seconde phase de l'échange atomique, la phase de collecte, peut commencer. Alice construit, signe et diffuse une transaction de collecte qui lui permet de récupérer les 10 LTC de Bob. Pour cela, elle fournit le secret au sein de la transaction et, ce faisant, le révèle nécessairement à Bob. Finalement, Bob peut lui aussi construire, signer et diffuser une transaction qui lui octroie les 0,03 BTC sur son compte. De cette manière, l'échange est clos !

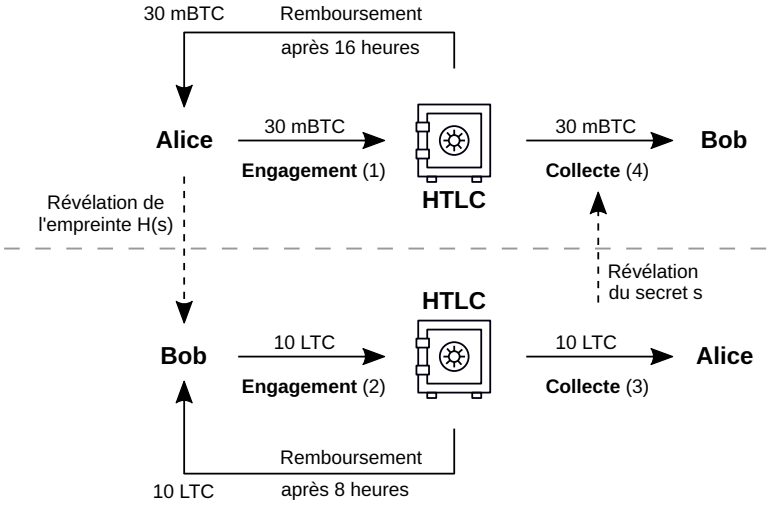

FIGURE 13.3 – Contrats et transactions dans un échange atomique.

Ce modèle garantit qu'aucun des deux participants ne peut se rembourser avant la fin du temps de verrouillage de Bob (8 heures) ; qu'Alice ne peut pas faire valoir sa transaction de remboursement au moment de la diffusion de sa transaction de collecte ; et que Bob ne peut pas s'approprier des fonds d'Alice tant qu'elle n'a pas diffusé sa transaction de collecte. Ces garanties rendent le procédé logiquement sécurisé, même si certains évènements perturbateurs peuvent survenir comme une augmentation des temps de confirmation liée à la volatilité du marché des frais.

Le premier *atomic swap* réel a été réalisé entre Litecoin et Decred le 19 sep-

tembre 2017 par Charlie Lee et Alex Yocom-Piatt [7]. Aujourd'hui, les échanges atomiques sont rares, les carnets d'ordres de plateformes spécialisées comme AtomicDEX étant très peu fournis. Toutefois, avec le durcissement réglementaire sévissant dans l'écosystème et rendant les plateformes centralisées moins fiables, il n'est pas exclu qu'ils jouent un rôle majeur à l'avenir.

Les canaux de paiement

Un cas particulier de l'application des contrats autonomes dans Bitcoin est le déploiement de canaux de paiement. Un canal de paiement est une manière pour deux utilisateurs d'effectuer des paiements répétés en bitcoins de manière sûre et instantanée sans publier de transactions sur la chaîne de blocs à partir de liquidités préalablement bloquées. Ces canaux sont notamment à la base du réseau Lightning, construit en surcouche de la chaîne.

Les canaux de paiement de Poon-Dryja

Même si l'idée d'un canal de paiement était envisagée dès les origines, elle ne s'est concrétisée qu'avec le concept élaboré par Joseph Poon et Thaddeus Dryja dans le cadre de leur projet du réseau Lightning [8]. Il s'agit d'un concept de canal bidirectionnel dont la sécurité repose sur un mécanisme de punition. Les deux participants bloquent des fonds dans un contrat et peuvent procéder à des paiements l'un vers l'autre dans la limite des liquidités disponibles. La somme des deux soldes des participants est appelée la capacité du canal.

Un canal traverse trois phases au cours de son existence :

— La phase d'ouverture ou d'installation, lors de laquelle les fonds sont bloqués par les participants sur un contrat autonome de multisignature 2-parmi-2 ;
— La phase de négociation ou de mise à jour, durant laquelle la répartition des fonds au sein du canal est ajustée ;
— La phase de fermeture ou de règlement, au cours de laquelle les fonds sont distribués aux participants sur la chaîne, généralement de manière coopérative selon le dernier état du canal.

La répartition initiale et la mise à jour du canal se font par l'intermédiaire de transactions d'engagement qui sont échangées entre les participants et *qui ne sont pas diffusées* sur le réseau, sauf dans le cas d'un litige, c'est-à-dire d'une fermeture non coopérative. Ces transactions d'engagement sont asymétriques, dans le sens où les participants en possèdent chacun leur propre version.

Supposons qu'Alice et Bob possèdent un canal, tel qu'illustré sur la figure 13.4. Dans ce cas, la dernière transaction d'engagement d'Alice, qui peut uniquement être finalisée et diffusée par Bob, prend en compte l'état actualisé du canal et répartit les fonds entre l'adresse d'Alice et un contrat de réclamation. Ce contrat de réclamation contient deux clauses :

— La récupération des fonds par Bob au terme d'un temps de verrouillage, ce qui répartit les fonds selon les soldes indiqués dans le canal ;
— La récupération des fonds par Alice à l'aide d'une clé de révocation qui est révélée plus tard lorsque le canal est de nouveau mis à jour.

Si un paiement a lieu d'Alice vers Bob, la mise à jour du canal se fait de la manière suivante. Alice construit et signe sa transaction d'engagement en utilisant la clé publique de révocation de Bob que ce dernier lui a transmise au préalable. Seul Bob peut finaliser la signature de cette transaction et la diffuser sur le réseau. Bob lui répond en lui envoyant sa clé privée de révocation, ce qui rend la dernière transaction d'engagement d'Alice inopérante. La même chose se produit ensuite de manière symétrique : Bob construit et signe sa transaction d'engagement qu'il transmet à Alice, et cette dernière lui révèle en échange sa clé privée de révocation, ce qui rend la transaction d'engagement de Bob impuissante [9].

La révélation de la clé de révocation à chaque étape de mise à jour rend possible l'activation d'un mécanisme de punition à tout moment. Si l'une des deux parties diffuse une transaction d'engagement correspondant à un état antérieur du canal, alors l'autre peut récupérer *l'intégralité* des fonds du canal. Par exemple, Alice pourrait récupérer les fonds de Bob si ce dernier était amené à diffuser le précédent état du canal dans le but d'« annuler » le dernier paiement réalisé.

Le défaut principal de ce mécanisme de punition est qu'il faut surveiller le réseau en permanence pour éviter un vol, ce qui se fait avec un nœud complet ou bien avec un tiers de confiance bien choisi (« tour de garde » ou « *watchtower* »).

Ce fonctionnement des canaux de Poon-Dryja fait aussi que toute erreur est très pénalisante : la diffusion accidentelle d'une transaction d'engagement antérieure mène à la récupération des fonds par l'autre partie. Il a également d'autres défauts : il impose de conserver l'ensemble des états antérieurs du canal, il oblige les participants à choisir les frais des transactions à l'avance et il alourdit considérablement les innovations au sein du réseau Lightning. C'est par volonté d'améliorer cette situation qu'ont été conceptualisés les canaux dits « de Decker-Russell-Osuntokun ».

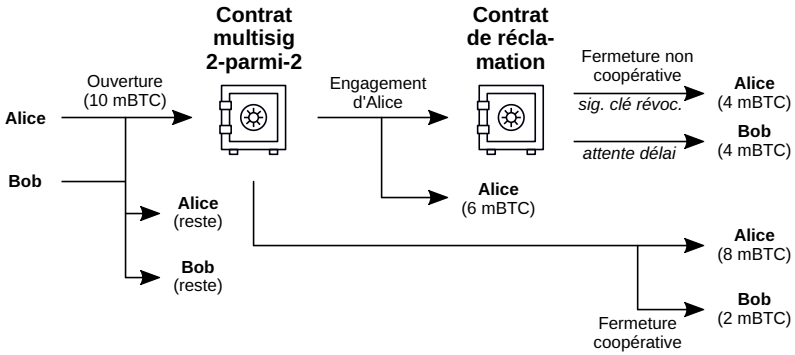

FIGURE 13.4 – Contrats et transactions dans un canal de paiement de Poon-Dryja : cas d'un paiement de Bob de 2 mBTC à Alice.

Les canaux de paiement de Decker-Russell-Osuntokun

Les canaux de paiement de Decker-Russell-Osuntokun ont été décrits par Christian Decker, Rusty Russell et Olaoluwa Osuntokun dans un livre blanc publié en avril 2018 [10]. Le protocole sous-jacent est appelé Eltoo, qui est une déformation de l'anglais « *L2* » (signifiant *layer two*).

Le fonctionnement des canaux de Decker-Russel-Osuntokun se base sur une chaîne de transactions, qui ne sont pas censées être diffusées sur la chaîne, sauf celles d'ouverture et de fermeture (cf. figure 13.5). Le principe est le suivant :

— Le canal est ouvert par une transaction d'ouverture ($T_{u,0}$), préalablement garantie par une transaction de règlement ($T_{s,0}$) qui rembourse les participants en cas de litige ;
— Le canal est mis à jour par des transactions de mise à jour ($T_{u,i}$) qui invalident les transactions de règlement précédentes ($T_{s,i-1}$) ;
— La fermeture du canal peut se faire après un certain délai d'expiration par la diffusion de la dernière transaction de règlement ($T_{s,i}$).

Ici il n'y a plus besoin de recourir à des clés de révocation pour rendre les anciens états du canal inexploitables : ce sont les transactions elles-mêmes qui ont ce rôle. Eltoo fait intervenir ce qu'on appelle des transactions flottantes, qui peuvent dépenser les fonds issus de n'importe quelle transaction de mise à jour précédente. De cette manière, chaque transaction de mise à jour est flottante, ainsi que chaque transaction de règlement, ce qui permet d'omettre toutes les mises à jour précédentes. De plus, un numéro d'état est inscrit dans chaque transaction pour ordonner les transactions et ainsi éviter la diffusion

d'un état antérieur.

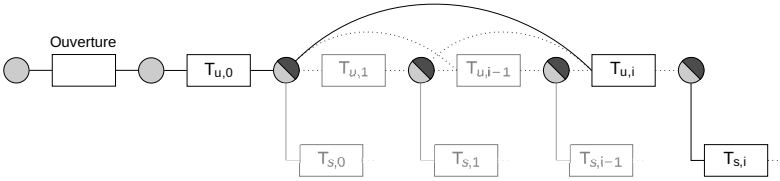

FIGURE 13.5 – Aperçu du protocole Eltoo.

Une transaction supplémentaire est ajoutée à la chaîne de transactions pour éviter que le délai d'expiration des transactions de règlement $T_{s,i}$ soit atteint et qu'elles soient diffusées sur la chaîne. Cette transaction envoie simplement les fonds vers un compte multisignatures classique, et est signée et diffusée après la signature des premières transactions de mise à jour et de règlement ($T_{u,0}$ et $T_{s,0}$). Le délai d'expiration ne commence que lorsque la transaction $T_{u,0}$ est diffusée.

Ce fonctionnement permet d'obtenir un protocole simple de mise à jour du canal, peu contraignant pour les nœuds, sans mécanisme de punition, et permettant de ne pas à avoir à décider les frais à l'avance. Cette facilité d'implémentation pourrait rendre plus aisée la création de contrats plus complexes sur Lightning, comme les canaux de paiement à 3 participants ou plus. En outre, leur implémentation ne doit en aucun cas remplacer celle des canaux de Poon-Dryja : les deux modèles peuvent coexister au sein d'un seul et même réseau de canaux de paiement.

Les transactions flottantes sont implémentées à l'aide de `SIGHASH_ANYPREVOUT`. La mise en œuvre de Eltoo repose donc sur l'intégration du BIP-118 dans Bitcoin.

L'inscription de données arbitraires

Bitcoin permet d'inscrire des données non financières sur la chaîne, c'est-à-dire des données qui ne sont pas nécessaires dans le blocage et le déblocage des fonds et qui sont interprétées de manière extérieure au protocole. Même en imposant toutes les restrictions possibles, on ne peut pas empêcher l'inscription de ces données, même s'il est possible de la rendre plus coûteuse.

La chaîne de blocs de la version principale de Bitcoin est largement partagée autour du monde, et sera conservée par l'humanité, au moins comme un reliquat historique, laissant supposer que ce qui y est stocké sera conservé

très longtemps. Cette caractéristique pousse les gens à y inclure des choses qui leur tiennent à cœur. Il est dans la nature de l'homme de chercher à laisser des traces de son passage sur Terre et écrire sur un registre réputé immuable est une manière de le faire.

Il existe diverses méthodes d'inscription, qui ont chacune leurs qualités et leurs défauts. Celles-ci ont évolué au fur et à mesure des années, alors que cette utilisation se libéralisait.

D'une part, l'écriture de données arbitraires peut être réalisée par les mineurs au sein de l'entrée de transaction de récompense, et plus précisément dans le script de déverrouillage. Ce champ est en effet superflu conceptuellement, la base de pièce ne faisant référence à aucune sortie existante, et peut donc être exploité de manière discrétionnaire. C'est cette méthode dont Satoshi Nakamoto a fait usage pour inscrire le désormais célèbre titre de une du Times du 3 janvier 2009 dans le bloc de genèse :

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

D'autres blocs contiennent des messages emblématiques. Le bloc d'exode de BCH (de hauteur 478 559) contenait un message de bienvenue pour Shuya Yang, la fille du PDG de la coopérative ViaBTC. Le bloc précédant le troisième halving sur BTC en 2020 (de hauteur 629 999) incluait le titre d'un article du New York Times du 9 avril annonçant l'injection de liquidité record de la Réserve Fédérale (2 300 milliards de dollars) en réaction à la crise du Covid-19 : « *NYTimes 09/Apr/2020 With $2.3T Injection, Fed's Plan Far Exceeds 2008 Rescue* ».

Le script de déverrouillage de la base de pièce peut être utilisé pour écrire d'autres données. C'est le cas du nonce supplémentaire (le critère qui a permis d'identifier les bitcoins de Satoshi). C'est aussi le cas du signalement des coopératives minières qui est réalisé via ce champ : par exemple, la base de pièce du bloc 751 005 contient la chaîne de caractères `poolin.com`, ce qui indique que sa validation a probablement été réalisée par la coopérative chinoise Poolin.

D'autre part, l'inscription des données arbitraires peut aussi être le fait des utilisateurs, qui peuvent les inclure dans leurs transactions et payer les frais correspondants. Plusieurs méthodes ont été exploitées pour ce faire.

Avant 2014, on procédait la plupart du temps à ces inscriptions en stockant les données dans les scripts de verrouillage, par exemple par l'utilisation de l'instruction de dépilement `OP_DROP` [11]. Une autre pratique courante était d'inscrire les données dans les sorties de type P2PKH, qui étaient rendues indépensables au passage. Cette méthode était extrêmement coûteuse en raison

de la forme de la transaction (imposant l'inscription dans les sorties transactionnelles) et le fait de devoir envoyer des montants non nuls en sortie. Elle était également dommageable pour le système dans son ensemble, car elle encombrait l'ensemble des UTXO.

Après 2014, une manière plus efficace de stocker des données a été autorisée par le biais de la standardisation du schéma NULLDATA qui se basait sur l'instruction `OP_RETURN`. Ce changement permettait de créer « une sortie assurément élagable, pour éviter les schémas de stockage d'informations [...] qui enregistraient des données arbitraires, telles que des images, en tant que sorties transactionnelles éternellement indépensables, gonflant ainsi la base de données des UTXO de bitcoin [12] ». Il limitait aussi le gaspillage de fonds en autorisant la création d'une sortie de 0 satoshi. Ce schéma s'est rapidement imposé comme la manière la plus populaire pour publier des informations sur la chaîne.

En outre, il est aussi possible de stocker des données au sein des entrées transactionnelles ou des témoins liés, lors de la dépense de sorties P2SH, P2WSH ou P2TR. Cette écriture peut se faire dans les scripts de récupération ou bien dans les éléments de déverrouillage. Cette méthode a l'avantage de ne pas surcharger l'ensemble des UTXO. Côté utilisateur, pour les entrées où SegWit s'applique, elle a pour bénéfice de diviser le coût des données arbitraires inscrites dans la transaction par quatre.

Ces différentes méthodes ont été utilisées pour inscrire toutes sortes de choses sur la chaîne, dont notamment des empreintes cryptographiques, du texte et des images [13].

D'abord, on peut inscrire une empreinte, l'inscription servant alors à l'horodatage. Il s'agit d'inscrire l'empreinte d'un fichier sur la chaîne en tant que preuve d'existence. Cette idée a été mise en avant en février 2009 par Hal Finney dans un de ses courriels adressés à la liste de diffusion dédiée à Bitcoin. Il suggérait alors que « la pile de blocs de bitcoin serait parfaite » pour « prouver qu'un certain document a existé à un certain moment dans le passé [14] », un point de vue approuvé par Satoshi. En somme, cette pratique permet de démontrer la connaissance d'une information avant sa publication, et donc indirectement qu'on en est l'auteur probable. Ce type d'usage a notamment été mis en œuvre par l'entreprise française Woleet.

Cette possibilité peut aussi être exploitée par les systèmes décentralisés d'hébergement de fichiers, comme le système IPFS (InterPlanetary File System) qui utilise les empreintes des fichiers pour les identifier et permettre leur stockage par un réseau pair à pair d'utilisateurs. Il est donc possible d'associer

le texte écrit sur la chaîne de blocs et des images ou des vidéos, hébergées de manière décentralisée.

Ensuite, on peut inscrire un texte, qui est généralement encodé en ASCII/UTF-8. Par exemple, la phrase « La beauté sauvera le monde. » a été inscrite sur la chaîne de BTC le 10 août 2022 dans la transaction d'identifiant `08e5ce0783ab6d5534e234136df02e0e240f76108eb6af04b8b624646b66f5eb`. L'inscription de textes permet aussi de dessiner des images en art ASCII. C'est le cas de l'hommage à Len Sassaman (voir figure 13.6), décédé en juillet 2011, qui a été inscrit sur la chaîne par les développeurs Dan Kaminsky et Travis Goodspeed dans des sorties P2PKH, et qui contient notamment une représentation de l'ancien président de la Fed, Ben Bernanke.

```
---BEGIN TRIBUTE---  =-=-=-=-=-=-=-=-=-=     ASCII BERNANKE
#./BitLen            LEN "rabbi" SASSAMA  :'::.:::::.:::.::.:
::::::::::::::::::       1980-2011       : :.: ' ' ' ' : :':
:::::::.::.::.:::  Len was our friend.  :.:     _.__    '.:
:.: :.' ' ' ' : :  A brilliant mind,    :   _,^"   "^x,   :
:.:'' ,,xiW,"4x, ''  a kind soul, and   '  x7'       '4,
:  ,dWWWXXXXi,4WX,   a devious schemer;   XX7           4XX
' dWWWXXX7"     'X,  husband to Meredith  XX             XX
 lWWWXX7   __   _ X  brother to Calvin,   Xl ,xxx,   ,xxx,XX
:WWWXX7 ,xXX7' "^^X  son to Jim and      ( ' _,+o, | ,o+,"
lWWWX7, _.+,, _.+.,  Dana Hartshorn,      4   "-^' X "^-'" 7
:WWW7,. '^"-" ,^-'   coauthor and         l,     ( ))     ,X
 WW",X:        X,    cofounder and        :Xx,_ ,xXXXxx,_,XX
 "7^^Xl.    _(_x7'   Shmoo and so much     4XXiX'-___-'XXXX'
 l ( :X:       __ _  more.  We dedicate     4XXi,_   _iXX7'
 '. " XX  ,xxWWWWX7  this silly hack to     , '4XXXXXXXXX^ _,
  )X- "" 4X" .___.   Len, who would have    Xx,  ""^^^XX7,xX
,W X     :Xi  _,,_   found it absolutely  W,"4WWx,_ _,XxWWX7'
WW X      4XiyXWWXd  hilarious.           Xwi, "4WW7""4WW7',W
"" ,,      4XWWWWXX  --Dan Kaminsky,      TXXWw, ^7 Xk 47 ,WH
, R7X,       "^447^  Travis Goodspeed     :TXXXWw,_ "), ,wWT:
R, "4RXk,      _, ,  P.S.  My apologies,  ::TTXXWWW lXl WWT:
TWk  "4RXXi,   X',x  BitCoin people.  He  ----END TRIBUTE----
lTWk,  "4RRR7' 4 XH  also would have
:lWWWk,  ^"     '4   LOL'd at BitCoin's
::TTXWWi,_  Xll :..  new dependency upon
```

FIGURE 13.6 – Hommage à Len Sassaman (art ASCII).

Enfin, on peut inclure une image, qui peut être encodée dans de multiples formats, dont notamment en JPEG ou en PNG. Un logo Bitcoin inscrit le 13 mai 2011 peut par exemple être retrouvé. Un hommage à Nelson Mandela accompagné d'une photo a été publié le 7 décembre 2013, quelques jours après sa mort. En 2022, l'absence de restriction standarde sur la taille des scripts

de Taproot a permis de réaliser des inscriptions volumineuses d'une manière bien plus transparente et directe. C'est ce qui a notamment permis d'inscrire l'image des Taproot Wizards qui pesait quasiment 4 Mo (voir figure 13.7).

FIGURE 13.7 – Image (réduite) des Taproot Wizards.

De manière générale, tout format de fichier peut être stocké sur la chaîne au moyen de transactions multiples : un document, un livre, une vidéo, un jeu, etc. Cependant, cette utilisation n'est pas forcément toujours pertinente. L'inscription demande le paiement de frais, parfois élevés, et la chaîne de blocs de BTC n'est pas franchement faite pour conserver des données volumineuses. La publication de ces fichiers sur IPFS et sur serveur local est généralement bien plus opportune.

Notons que la communauté de Bitcoin SV s'est focalisée sur le stockage de données, considérant que son registre était une « source universelle de vérité [15] ». On peut ainsi retrouver un volume assez important de données météorologiques sur sa chaîne, qui y sont inscrites depuis 2019. Cela fait que le réseau BSV est extrêmement centralisé tant du point de vue minier que commercial, ce qui remet en cause l'utilité première de l'inscription d'informations sur une chaîne de blocs : l'immuabilité.

Les métaprotocoles

Les métaprotocoles sont des protocoles qui se servent du protocole de base pour fonctionner. Ils font usage de l'inscription de données arbitraires sur la chaîne pour inclure des instructions qui sont interprétées par des implémentations logicielles spécifiques. Ils ont pour particularité d'être plus extensifs que le protocole de base.

Il ne s'agit pas d'une idée nouvelle. Dès les premières années d'existence de Bitcoin, certaines personnes ont souhaité l'exploiter plus en profondeur, en se servant de lui d'une autre manière que comme un instrument de transfert de valeur. Ce mouvement initial, visant à ajouter des fonctionnalités à Bitcoin de cette façon, était appelé « Bitcoin 2.0 ». Il a finalement mené à l'élaboration d'Ethereum à partir de 2013.

Le premier type de métaprotocole qui a été élaboré est le procédé des *colored coins*, ou pièces colorées en français, qui consiste à marquer des pièces (UTXO) par l'inscription annexe de données, comme montré sur la figure 13.8. Chaque type de jeton créé est lié à un identifiant, que l'on peut assimiler à une couleur, d'où le nom de ce procédé. L'idée a été présentée en 2012 par Yoni Assia et Meni Rosenfeld [16].

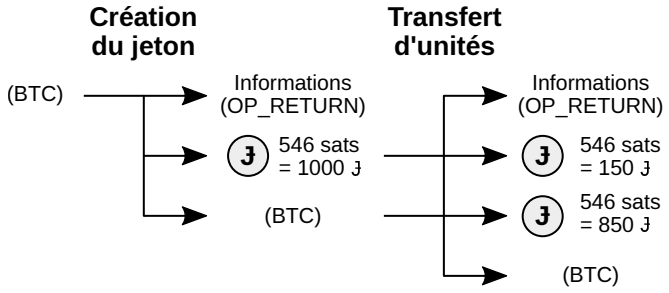

FIGURE 13.8 – Création et transfert d'un jeton émis sous la forme d'un colored coin.

L'implémentation de ce concept a été réalisée dès la fin de l'année 2012 par l'intermédiaire du ChromaWallet. Cependant, elle n'a vraiment pris de l'ampleur qu'à partir de 2014, avec l'apparition des Open Assets de Coinprism, des *CoinSpark assets* de Coin Sciences, et des Colored Coins de Colu. Ces usages sont depuis tombés en désuétude, même si le procédé a pu servir de manière sporadique au fil des années, comme dans le cas du jeton BSQ de Bisq créé en 2018 comme base de sa DAO. Une tentative de restauration a également été faite sur Bitcoin Cash avec les jetons SLP, sans grand succès.

Au-delà des pièces colorées, il existait des protocoles plus évolués qui avaient la particularité de gérer une unité de compte propre. Il s'agissait

essentiellement de Mastercoin, qui a été rebaptisé Omni en mars 2015, et de Counterparty.

Le premier métaprotocole avancé a été Mastercoin, dont le livre blanc, intitulé « *The Second Bitcoin Whitepaper* », a été publié le 6 janvier 2012 par J.R. Willett [17]. Il s'agissait d'un protocole permettant à ses utilisateurs de créer leurs propres devises, appelées « *user currencies* ». Mastercoin reposait sur une unité de compte notée le MSC, qui a fait l'objet d'une prévente d'un mois en juillet-août 2013 [18]. C'était la première *Initial Coin Offering* de l'histoire, et elle a recueilli 5 120 BTC, soit plus de 500 000 $ à ce moment-là.

Le plus grand succès de ce protocole a probablement été la création du premier stablecoin, le Tether USD, qui a été émis sous le nom de Realcoin en octobre 2014. Mastercoin / Omni a longtemps été l'unique manière de posséder et de transférer de l'USDT avant que le jeton ne soit émis massivement sur d'autres chaînes comme Ethereum et Tron.

Le second métaprotocole avancé a été Counterparty, lancé en janvier 2014. Cette plateforme reposait également sur un jeton natif, le XCP, qui lui servait de carburant, et qui a été créé par brûlage de bitcoins durant son premier mois d'existence [19]. Ce sont 2 140 bitcoins qui ont ainsi été rendus inutilisables pour donner vie à plus de 2,6 millions de XCP, encore en circulation aujourd'hui. Counterparty se voulait plus flexible que Mastercoin en rendant possible l'implémentation de contrats autonomes, notamment dans le but de créer des jetons et d'héberger des plateformes d'échange décentralisées, appelées des « distributeurs ».

En particulier, Counterparty a été la première plateforme à proposer la gestion de jetons non fongibles (NFT). Il s'agissait là de mettre en œuvre une vieille idée, qui avait notamment été mise en valeur par Hal Finney en 1993 sur la liste de diffusion cypherpunk sous la forme de « cartes à collectionner cryptographiques [20] ». Counterparty a ainsi hébergé une multitude de collections de tels objets, comme les cartes à jouer de *Spells of Genesis* et de SaruTobi créées en 2015, ou les Rare Pepes émis entre 2016 et 2018.

En 2018, l'apparition de Bitcoin Cash a motivé la création d'un média social dont les données seraient entièrement stockées sur la chaîne, les développeurs de BCH étant plus libéraux à ce sujet. Le protocole s'appelait Memo et consistait à publier de courts messages visibles publiquement sous un profil défini et à pouvoir suivre les autres utilisateurs, à aimer et répondre à leurs messages. L'idée était d'obtenir une sorte de réseau social résistant à la censure, mais souffrait néanmoins de la nécessité de payer des frais à chaque action.

Tous ces protocoles ont perdu leur attrait jusqu'à l'apparition du protocole Ordinals, lancé en janvier 2023. Ce métaprotocole permettait de créer et de gérer des « artéfacts numériques », c'est-à-dire des NFT dont l'intégralité des données est stockée de manière immuable sur une chaîne résistante à la censure. Le protocole Ordinals reposait sur une « théorie des ordinaux » permettant de suivre et de transférer des satoshis liés à une inscription, comme un texte, une image ou autre chose. En particulier, Ordinals a été utilisé pour émuler la propriété et le transfert de jetons fongibles, baptisés « BRC-20 », dont le succès spéculatif a provoqué une congestion du réseau menant à une hausse des frais de transaction historique. Le succès d'Ordinals a également inspiré la création du protocole STAMPS, qui se basait sur Counterparty pour le suivi des artéfacts et stockait leurs données dans des sorties P2MS.

Toutes ces pratiques ont créé des débats. En effet, Bitcoin était présenté comme un modèle de monnaie numérique et il semblait contreproductif d'en faire un protocole de conservation de données qui ne seraient pas relatives au transfert de bitcoins. Ainsi, dès décembre 2010, Jeff Garzik s'opposait au fait d'utiliser la chaîne pour le stockage généralisé [21]. Plus tard, en 2014, des disputes similaires ont éclaté au sujet de Counterparty [22]. En 2023, c'est également la même discorde qui a eu lieu suite au succès d'Ordinals [23].

Ces métaprotocoles présentent deux défauts majeurs. Le premier est que la vérification de leurs règles dépend d'un petit sous-ensemble de nœuds du réseau. En effet, la gestion d'un tel protocole construit en surcouche demande des ressources supplémentaires, notamment en ce qui concerne l'indexation pour les pièces colorées. De ce fait, peu de personnes déploient une implémentation complète, ce qui centralise considérablement le protocole et le rend sensible à l'altération par un adversaire qui aurait pour but de le censurer.

Le second défaut concerne leurs frais d'utilisation parfois très élevés, surtout si la limite de capacité transactionnelle du réseau est atteinte. Les transactions qui mettent en place ces solutions sont nécessairement plus volumineuses que les transactions normales et entraînent par conséquent des frais plus élevés. Elles sont donc plus facilement exclues par l'augmentation des frais issue de la congestion du réseau.

C'est pour ces raisons que les personnes qui ont travaillé sur ces solutions s'en sont vite détournées, préférant se réfugier vers des plateformes alternatives comme NXT et surtout Ethereum. Vitalik Buterin lui-même s'intéressait aux pièces colorées et à Mastercoin en 2013 avant de commencer à bâtir ce qui allait devenir Ethereum [24]. C'est aussi pour ces raisons que des solutions moins coûteuses (des surcouches utilisant la chaîne comme un procédé de

règlement et non pas comme un lieu où inscrire toutes les opérations) sont aujourd'hui privilégiées pour faire ce genre de choses comme RGB ou Taproot Assets.

Les contrats hors chaîne

La cryptographie permet de déployer des contrats sans que ceux-ci ne doivent être inscrits sur la chaîne. Cette particularité a été facilitée grâce à la mise à niveau Schnorr-Taproot, souvent simplement appelée « Taproot », qui est survenue sur BTC le 14 novembre 2021 et qui incluait deux éléments majeurs : le schéma de signature de Schnorr et le procédé de programmation de contrats Taproot. Ces fonctionnalités ont été intégrées sous forme d'un soft fork au sein du schéma standard P2TR correspondant à la version 1 de SegWit.

Le schéma de Schnorr implémenté est une dérivation du protocole d'authentification du même nom décrit en 1989 par Claus-Peter Schnorr. Il s'agit d'une alternative à ECDSA qui se base sur la même courbe elliptique (secp256-k1) et qui permet de signer des transactions grâce aux mêmes paires de clés.

Comparé à ECDSA, le schéma de signature de Schnorr possède quelques avantages. Premièrement, il produit des signatures moins grandes. Deuxièmement, les signatures produites ne sont pas malléables, le procédé ne faisant pas intervenir de nombre aléatoire. Troisièmement, et c'est le plus important, il présente une propriété de linéarité, ce qui permet notamment de faire des choses comme la vérification par lots et l'agrégation des clés.

Le schéma de Schnorr est supérieur à ECDSA et existait en 2008, mais Satoshi Nakamoto n'a pas daigné s'en servir. Ce choix s'explique par le fait que l'algorithme était breveté aux États-Unis jusqu'en février 2008 et que par conséquent il n'existait pas d'implémentation standardisée. Le logiciel de Bitcoin utilisait en effet OpenSSL, qui n'intégrait pas ce type d'algorithme.

Le schéma de Schnorr autorise le déploiement de *Scriptless Scripts*, de contrats « sans script » qui sont exécutés en dehors de la chaîne et appliqués au sein des signatures. Le concept a été théorisé en 2017 par Andrew Poelstra [25]. Il se retrouve dans des exemples comme le schéma de signature multipartite MuSig2, les *Adaptor Signatures* ou encore les *Discreet Log Contracts*.

Outre cela, le schéma de Schnorr facilite grandement l'implémentation de Taproot (BIP-341), qui a été intégré au protocole au même moment. Taproot (dont le nom signifie littéralement « racine pivot » en français) est un procédé de programmation de contrats autonomes qui ancre les clauses d'un contrat au sein d'un arbre de Merkle et qui cache cet arbre sous une clé publique agrégée

appartenant à ses participants. Il permet de ne publier le contrat qu'en cas de litige, et même dans ce cas, de ne publier que les conditions exécutées. Les scripts utilisés dans Taproot utilisent un langage de programmation nommé Tapscript (BIP-342), basé sur le langage de script classique de Bitcoin.

Taproot repose sur un arbre de hachage, appelé un MAST [26], dont les feuilles sont les clauses du contrat, c'est-à-dire les conditions de dépense. Lors de l'exécution du MAST, les participants concernés ont seulement besoin de révéler la clause appliquée et de fournir les empreintes liées aux autres clauses (chemin de Merkle), comme montré sur la figure 13.9. Les autres conditions de dépense ne sont ainsi pas révélées.

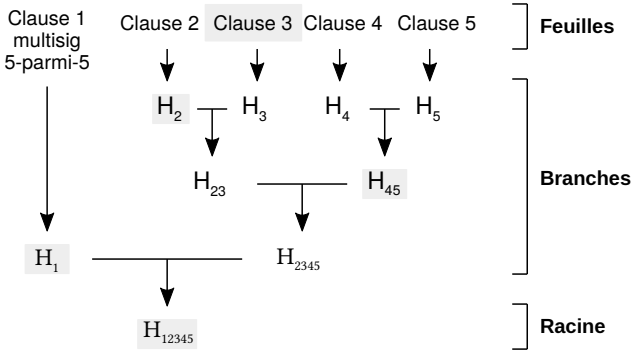

FIGURE 13.9 – MAST impliquant les clauses d'un contrat.

L'implémentation de tels MAST au sein de Bitcoin avait déjà été proposée par le passé, que ce soit sous la forme d'une nouvelle version de SegWit (BIP-114), ou bien d'un nouveau code opération appelé `OP_MERKLEBRANCHVERIFY` (BIP-116, BIP-117). Mais Taproot a constitué une proposition supérieure en permettant de ne pas révéler l'existence du MAST lui-même.

Taproot inclut en effet une condition de dépense coopérative intégrée. La clé publique agrégée interne est modifiée légèrement (*tweaked*) à l'aide de la racine du MAST, afin de prendre ce dernier en compte. La clé obtenue est celle inscrite dans le script de verrouillage de la pièce, de sorte qu'elle est indiscernable des autres sorties P2TR. De même, la signature agrégée ne peut pas être distinguée d'une signature classique. De ce fait, les participants peuvent dépenser les fonds à l'amiable, tout en étant sûrs qu'un litige mènera au règlement sur la chaîne.

Une alternative à Taproot est RGB, qui est un système de contrats autonomes hors chaîne, construit à la fois en surcouche de Bitcoin et de Lightning. Le nom est issu du standard RGB (*Red Green Blue*) qui permet de définir une

couleur et constitue par conséquent une référence directe aux *colored coins*, RGB ayant été originellement conçu comme « une meilleure version des pièces colorées [27] ». Cependant, même si RGB permet effectivement d'émettre et de gérer des jetons, cette fonctionnalité est loin d'être la seule.

RGB se base sur deux primitives techniques conceptualisées en 2016 par le développeur Peter Todd : la validation côté client (*client-side validation*) et les scellés à usage unique (*single-use seals*). Cela permet la gestion d'un état indépendant, où la double dépense est empêchée par ces scellés. Après avoir fait l'objet de recherches par Giacomo Zucco et le BHB Network, RGB est actuellement développé par la LNP/BP Standards Association.

L'implémentation de contrats en dehors de la chaîne est donc possible sur Bitcoin, et ils apportent deux choses. D'une part, ils réduisent le paiement de frais en ayant une empreinte minimale sur la chaîne. D'autre part, ils améliorent la confidentialité de leurs participants. C'est pourquoi ils ont le potentiel de jouer un grand rôle à long terme.

Une monnaie programmable

L'aspect programmable de Bitcoin est souvent négligé. Il n'est en effet pas directement présenté dans le livre blanc, même si Satoshi Nakamoto l'avait déjà élaboré à ce moment-là. Il est toutefois très utile et constitue l'une des facettes essentielles de Bitcoin.

La programmabilité de la monnaie peut servir à contrôler, comme l'illustrent les projets de MNBC qui fleurissent autour du monde. Mais elle peut également rendre un fier service à la liberté individuelle. En effet, cet aspect modulable donne l'occasion à des personnes qui ne se connaissent pas d'échanger de la valeur de la façon la plus sûre possible ou, comme l'exprimait Tim May dans son *Manifeste crypto anarchiste* de 1988, de « faire des affaires et négocier des contrats électroniques sans jamais connaître le Vrai Nom, ou l'identité légale, de l'autre [28] ».

Les contrats autonomes forment la pierre angulaire des relations financières dans le cyberespace. Même la communauté de Monero, qui avait particulièrement restreint cet aspect à des fins de confidentialité, est revenue sur ses pas en intégrant au protocole la fonctionnalité de signature multipartite, notamment dans le but de permettre les échanges atomiques. Une monnaie réellement libre se doit de pouvoir être programmée librement.

14

Le passage à l'échelle

La scalabilité, calque de l'anglais *scalability*, aussi appelée extensibilité, désigne la capacité d'un système à passer à l'échelle, c'est-à-dire à continuer de fonctionner de manière équivalente à mesure que le nombre d'utilisateurs augmente. Dans un système géré de manière centralisée, cette capacité est assurée par l'apport de matériel informatique, soit en ajoutant de la puissance de calcul à l'infrastructure existante (passage à l'échelle vertical), soit en multipliant les instances de l'infrastructure pour partager le traitement des requêtes (passage à l'échelle horizontal). La scalabilité dépend par conséquent du niveau de prévision de l'entité qui s'occupe du système.

Dans le cas d'un système distribué, qui a un comportement différent, la scalabilité se rapporte à quelque chose de plus compliqué. L'ajout de matériel ne suffit pas : il faut également que les propriétés dudit système se conservent avec la hausse de l'activité. Dans le cas de Bitcoin, ce problème est particulièrement ardu, car toute montée en charge affecte durablement les nœuds du réseau, en raison de la nécessité de partage de la chaîne de blocs intégrale. En substance, le système ne passe pas à l'échelle, ou très peu.

Ce problème de scalabilité de Bitcoin a été une préoccupation majeure de la communauté, à tel point qu'il a provoqué un véritable conflit ouvert entre 2015 et 2017 : la fameuse guerre des blocs que nous avons décrite dans le chapitre 2. Certains pensaient qu'augmenter la taille des blocs suffiraient à gérer la demande sans altérer l'offre, tandis que d'autres imaginaient que les

solutions de surcouche comme le réseau Lightning seraient assez efficaces pour traiter tous les transferts. Ce chapitre a pour objectif de faire un tour d'horizon de la situation et de proposer une troisième voie.

L'absence de scalabilité du système

La conception originelle de Bitcoin repose sur un principe simple : obtenir et vérifier l'intégralité des transactions dans le but de s'assurer qu'il n'y a pas de double dépense. Comme l'écrivait Satoshi Nakamoto dans le livre blanc, « la seule façon de confirmer l'absence d'une transaction est d'être au courant de toutes les transactions [1] ». De ce fait, pour disposer d'une sécurité maximale, chaque nœud doit, en principe, entretenir une version complète de la chaîne de blocs.

Dès les origines, ce fonctionnement particulier a naturellement amené la question de la montée en charge du système. Lorsque Satoshi Nakamoto a présenté sa découverte sur la liste de diffusion dédiée à la cryptographie de Metzdowd.com le 31 octobre 2008, la première réponse qu'il a reçue concernait ainsi ce problème. Cette réponse était celle de l'ancien cypherpunk James A. Donald le 2 novembre, qui écrivait :

> « Nous avons vraiment, vraiment besoin d'un tel système, mais d'après ce que je comprends de votre proposition, il ne semble pas pouvoir s'adapter à la taille requise.
>
> Pour que des jetons de preuve de travail transférables aient de la valeur, ils doivent avoir une valeur monétaire. Pour avoir une valeur monétaire, ils doivent être transférés au sein d'un très grand réseau — par exemple un réseau d'échange de fichiers semblable à bittorrent.
>
> Pour détecter et rejeter un événement de double dépense dans un délai convenable, il faut disposer de la plupart des transactions passées des pièces impliquées dans la transaction, ce qui, mis en œuvre naïvement, exige que chaque pair dispose de la plupart des transactions passées, ou de la plupart des transactions passées qui ont eu lieu récemment. Si des centaines de millions de personnes effectuent des transactions, cela représente beaucoup de bande passante — chacun doit avoir connaissance de toutes les transactions ou d'une partie substantielle de celles-ci [2]. »

James A. Donald mettait par là en valeur le manque de scalabilité de Bitcoin. Pour tout système donné, une augmentation de volume transactionnel accroît le nombre de transactions à obtenir et à traiter. Cet accroissement rend plus difficile de faire fonctionner un nœud, ce qui peut affecter la décentralisa-

tion du réseau et donc la sécurité. De ce fait, il existe toujours un compromis entre l'utilité et la sécurité du système, ou pour mieux le dire, entre la facilité de transaction et la facilité de vérification.

Ce compromis se manifeste généralement par une limite de capacité transactionnelle, décrite par les règles de consensus (limite explicite) ou, plus rarement, par les règles de réseau (limite implicite). La limite de capacité transactionnelle était originellement décrite comme une taille limite des blocs, qui interdisait aux mineurs de créer des blocs plus grands qu'une certaine taille. Dans le prototype, cette taille était définie implicitement par la taille maximale des messages du protocole de transmission, c'est-à-dire 32 Mio. Puis, une limite explicite de 1 mégaoctet (1 Mo) a été ajoutée par Satoshi Nakamoto en septembre 2010 par le biais de la constante `MAX_BLOCK_SIZE`, sans annonce publique de sa part, dans le but d'éviter les attaques par déni de service. Cette taille correspondait, pour un réseau tournant à plein régime, à un volume théorique de 4,5 transactions classiques par seconde, ce qui se ramenait plutôt à 3 transactions par seconde en pratique.

Avec l'intégration de SegWit dans la version principale de Bitcoin en août 2017, cette limitation est devenue un poids limite des blocs. Cette nouvelle métrique donnait une importance plus grande de la taille de base par rapport à la taille du témoin dans le calcul de la mesure du bloc, modifiant également la façon dont comptaient les mineurs pour ajouter les transactions au bloc. Cette modification était une augmentation effective de la capacité transactionnelle du protocole, portant le volume autorisé de transactions à 8 transactions par seconde en théorie, et à 4,5 transactions par seconde en pratique.

L'existence d'une limite de capacité transactionnelle engendre nécessairement une rareté de l'espace de bloc. Si elle est fixe, elle rend l'offre par essence inélastique. Ainsi, une forte demande pour l'espace de bloc fait, par effet d'enchère, augmenter le prix pour l'inclusion, c'est-à-dire les frais de transaction. Le marché des frais est stimulé par cette limite rigide au lieu de rester à son niveau naturel, à savoir celui du coût d'inclusion par défaut des mineurs.

Par son effet sur le niveau des frais, la limite crée un plancher d'utilité, c'est-à-dire un niveau de valeur en deçà duquel le transfert et la détention ne sont pas considérés comme rentables par les utilisateurs. En effet, les mineurs sont amenés à rejeter les transactions qui ne paient pas un taux de frais suffisant par rapport à leur taille. De ce fait, l'utilité d'une transaction peut être estimée insuffisante par son auteur au regard du niveau de frais moyen de la chaîne, auquel cas elle n'a pas lieu. Si une personne désire acheter un

café pour 2 $ en BTC, mais que les frais usuels sont de 1 $, cette personne passera vite son chemin. De manière générale, les cas d'utilisation requérant des frais « faibles » sont chassés de la chaîne, à l'instar du service de jeu d'argent SatoshiDICE, qui a dû cesser ses activités sur BTC en 2017 suite à l'augmentation des frais.

La limite de capacité transactionnelle a pour vertu de garantir que le coût d'utilisation d'un nœud reste bas. Elle agit ainsi sur la décentralisation *potentielle* du réseau. En effet, contrairement au matériel minier, le coût lié à la vérification n'est pas compensé par un revenu proportionnel, de sorte qu'il atteint tout le monde de la même manière. Les opérateurs de nœud les moins bien équipés ne peuvent pas matériellement suivre le rythme, ce qui affecte la facilité du réseau à se décentraliser *effectivement*.

L'influence sur la décentralisation potentielle concerne à la fois le minage et le commerce en empêchant les plus petits acteurs de pouvoir réaliser ces activités à leur échelle. La centralisation du minage augmente le risque de censure, tandis que la centralisation du commerce augmente le risque d'altération du protocole, et donc le risque d'inflation. C'est pourquoi la limite de capacité transactionnelle joue un rôle majeur dans le modèle de sécurité : moins cette limite est élevée, plus la sécurité *potentielle* du système est grande.

La limite de capacité transactionnelle est déterminée de manière subjective par les commerçants, en fonction de leur *perception de la menace* et de leur *utilisation personnelle* de la chaîne. Il n'existe pas de limite de taille des blocs idéale : il n'y a que des êtres humains qui calculent un risque par rapport à une éventuelle récompense. On peut tenter d'établir une moyenne pour estimer une limite qui correspond à une utilisation donnée, mais cette estimation serait au mieux imparfaite.

Par son effet sur la décentralisation, la limite crée un plafond d'utilité, c'est-à-dire un niveau de valeur au-delà duquel le transfert et la détention sont considérés trop risqués pour la sécurité effective du système. En effet, aucune sécurité n'étant absolue, le transfert et la détention d'une certaine valeur peut ne plus bénéficier suffisamment de la protection apportée par le réseau. Par exemple, recevoir ou conserver l'équivalent de plusieurs millions de dollars sur la chaîne de Bitcoin SV est, c'est le moins qu'on puisse dire, imprudent.

Le plancher d'utilité (induit par l'action négative de la limite sur l'espace de bloc) et le plafond d'utilité (induit par l'action positive de la limite sur la sécurité) ont pour effet de borner une plage de valeurs en dehors de laquelle le transfert et la détention ne sont plus pertinents [3]. C'est l'existence de cette plage de valeurs qui entraîne l'apparition de substituts à un système donné.

L'arrivée de nouveaux utilisateurs et l'augmentation subséquente de la demande pour l'espace de blocs rehaussent le plancher d'utilité. Toute montée en charge du système en modifie les caractéristiques. Par conséquent, tout système Bitcoin est en substance non scalable, au sens premier du terme. Il existe cependant des méthodes pour contourner cette absence de scalabilité.

L'amélioration de l'efficacité de base

La première proposition vis-à-vis du passage à l'échelle a été d'augmenter progressivement la limite de taille des blocs dans le but d'accompagner l'accroissement de l'activité [4]. C'était la solution soutenue par Satoshi Nakamoto, comme en témoigne sa première réaction à la réponse de James A. Donald le 3 novembre 2008 :

> « La bande passante n'est peut-être pas aussi prohibitive que vous le pensez. Une transaction typique est d'environ 400 octets (la cryptographie sur les courbes elliptiques est agréablement compacte). Chaque transaction doit être diffusée deux fois, soit 1 Ko par transaction. Visa a traité 37 milliards de transactions au cours de l'année 2008, soit une moyenne de 100 millions de transactions par jour. Un tel nombre de transactions nécessiterait 100 Go de bande passante, soit la taille de 12 DVD ou de 2 films en qualité HD, ou encore environ 18 $ de bande passante au prix actuel. Si le réseau devait atteindre cette taille, cela prendrait plusieurs années, et d'ici là, l'envoi de 2 films en HD sur Internet ne semblera probablement pas être un gros problème [5]. »

La vision de Satoshi était cependant bien trop optimiste. D'une part, il ne voyait pas la centralisation du minage comme un problème existentiel, prévoyant dès le début que la puissance de calcul du réseau reposerait sur des « fermes de serveurs composées de matériel spécialisé ». D'autre part, il pensait que la vérification de paiement simplifiée suffirait, ne tenant pas compte de ses défauts de fiabilité et de confidentialité, ni de son incapacité à exercer un pouvoir sur la détermination des règles de consensus. Le plan de Satoshi était donc faillible sans pour autant être entièrement mauvais.

Le fonctionnement d'un nœud dépend d'un certain nombre de charges. Les principales sont le stockage sur disque dur (HDD) pour l'historique (chaîne de blocs), le stockage en mémoire flash (SSD) pour l'état (ensemble des UTXO), le stockage en mémoire vive (barrette de RAM) pour la réserve des transactions non confirmées (mempool) et la réserve des blocs orphelins, le maintien d'une bande passante (ou débit binaire, usuellement exprimé en Mbit/s) permettant de recevoir et d'envoyer les blocs et les transactions, et le calcul du processeur

(CPU) pour la vérification des données et notamment des signatures. Faire diminuer le coût d'un nœud consiste ainsi à réduire l'une de ces charges.

Même si l'augmentation naïve de la taille limite des blocs ne constitue pas en soi une méthode de scalabilité, il s'avère qu'elle peut être compensée par le progrès technique provenant de l'optimisation logicielle, matérielle ou algorithmique. Premièrement, les performances du logiciel (pour un ensemble donné de règles de consensus) peuvent être améliorées, et il s'agit même de l'une des tâches de base de l'équipe de Bitcoin Core [6]. Deuxièmement, le matériel informatique peut être rendu plus efficace, certains composants devenant progressivement moins coûteux (loi de Moore [7]). Troisièmement, le protocole peut lui-même être perfectionné au niveau algorithmique, par la découverte et l'adoption de nouvelles techniques plus efficaces : c'est par exemple le cas de l'algorithme de signature de Schnorr qui produit des signatures plus compactes qu'ECDSA (40 octets au lieu de 72), ou bien des bulletproofs qui rendent les preuves de portée des Confidential Transactions beaucoup moins volumineuses.

Au-delà de ces optimisations, il n'existe pas de manière d'augmenter le volume transactionnel de la chaîne sans faire de compromis au niveau du modèle de Bitcoin. La solution consiste ainsi à modifier le comportement du système, de telle manière qu'il n'affecte pas trop le modèle de sécurité. Plusieurs facteurs peuvent ainsi être optimisés, dont la taille de la chaîne à conserver, l'*Initial Block Download* (IDB) et la taille de l'ensemble des UTXO.

D'abord, on peut choisir de supprimer les blocs les plus anciens une fois qu'on les a vérifiés. On conserve simplement la chaîne des entêtes, l'état du réseau, ainsi que les blocs les plus récents afin de pouvoir rejoindre le consensus dans le cas d'une recoordination profonde. Cette méthode est appelée l'élagage ou *pruning*.

Mais cette méthode n'enlève pas la charge de l'IBD, c'est-à-dire le processus de téléchargement et de vérification de la chaîne de blocs jusqu'à sa hauteur actuelle. Pour ce faire, on peut procéder à diverses techniques plus ou moins risquées. La première est la supposition de validité des signatures, basée sur le paramètre `assumevalid`, qui a été introduite dans Bitcoin Core en 2017 [8], et qui consiste à sauter la vérification des signatures jusqu'à un bloc d'empreinte donnée, faisant gagner beaucoup de temps dans la synchronisation initiale. Cette méthode n'est pas un point de contrôle (elle n'impose pas au bloc d'exister) et le risque qu'elle comporte est minime. La deuxième technique est AssumeUTXO, qui a été proposée en 2019 par James O'Beirne

et est toujours en développement [9], et qui implique de supposer valide un ensemble des UTXO donné (identifié par son empreinte) à une hauteur de bloc déterminée : l'opérateur de nœud télécharge la sauvegarde de l'ensemble des UTXO auprès d'un tiers et débute la synchronisation initiale à partir de celui-ci, remettant à plus tard (ou ignorant complètement) le téléchargement et la vérification des blocs précédents. Cette méthode présente un défaut de vérification (au moins temporaire) de sorte que l'opérateur est exposé à la tromperie, mais le risque est considéré comme acceptable. Il existe également une troisième technique plus radicale, l'engagement des UTXO (ou *UTXO commitments*), qui est un soft fork obligeant les mineurs à ajouter l'empreinte de l'ensemble des UTXO dans le bloc [10] : cet engagement permettrait de disposer d'une source bien plus fiable pour télécharger la sauvegarde à partir de laquelle commencer la synchronisation.

Ensuite, au-delà de l'IBD, reste le problème de la taille de l'ensemble des UTXO, qui est l'un des facteurs limitants les plus importants. La première idée pour réduire cette taille est une proposition de Cory Fields appelée UHS (pour *UTXO Hash Set*) qui consiste uniquement à stocker les empreintes (*hashes*) des UTXO individuelles [11]. La deuxième idée est de se servir d'accumulateurs cryptographiques, comme l'a fait Thaddeus Dryja avec sa proposition nommée Utreexo, qui implique de regrouper les UTXO dans des arbres de Merkle afin de condenser l'ensemble à conserver en mémoire, au prix d'un compromis sur la bande passante [12].

Enfin, on peut également choisir d'éclater le minage et la vérification des transactions en séparant l'historique et l'état du système en plusieurs fragments, qui sont chacun soutenus par une partie (variable) du réseau. C'est ce qu'on appelle le partitionnement ou *sharding*. C'était l'idée derrière l'utilisation d'un arbre préfixe de Merkle-Patricia (aussi appelé arbre Merklix) vaguement envisagée par les développeurs de Bitcoin Cash, ou le *dankSharding* qui pourrait être implémenté dans Ethereum. Cependant, il s'agit là d'une modification importante du protocole qui pourrait ne jamais être implémentée dans une version de Bitcoin.

Ces propositions sont des compromis se faisant au niveau de la chaîne qui affectent souvent le système dans son entièreté. Toutefois, il est également possible de faire un compromis différent, au niveau des pièces individuelles, par l'utilisation de banques et, surtout, de surcouches.

Les banques et les surcouches

Les autres propositions généralement citées comme alternatives à l'augmentation de la taille des blocs sont des solutions consistant à ne pas réaliser tous les transferts sur la chaîne, mais à en déporter les plus petits ailleurs, ceux-ci étant « regroupés » dans des transactions plus grosses. La chaîne est alors utilisée pour régler les dettes, contractées de manière analogique (contrat juridique) ou numérique (contrat autonome). Cela consiste à considérer le protocole comme un protocole de règlement.

La première manière de faire est de réintroduire de la confiance dans le système en contractant des obligations de manière traditionnelle, auprès de ce que nous appellerons ici des banques. Les banques en question peuvent émettre une monnaie représentative en gardant l'intégralité des fonds, ou bien offrir du crédit en ne conservant que des réserves fractionnaires. L'utilisation de la chaîne sert au règlement entre les banques, qui assure le transfert de fonds entre leurs clients. C'est en somme le modèle de la banque libre promu par George Selgin et Larry White dans les années 1990.

Cette première conception a été défendue par Hal Finney, qui avait connaissance des travaux de Selgin et de White, comme nous l'avons vu dans le chapitre 6. Le 30 décembre 2010, il faisait ainsi l'apologie d'un modèle de banque libre basé sur le bitcoin :

> « En fait, il existe une très bonne raison pour que les banques basées sur Bitcoin existent et émettent leur propre monnaie numérique, convertible en bitcoin. Bitcoin lui-même ne peut pas passer à l'échelle pour que chaque transaction financière dans le monde soit diffusée publiquement et incluse dans la chaîne de blocs. Il doit y avoir un niveau secondaire de systèmes de paiement, plus léger et plus efficace. [...] Les banques basées sur Bitcoin résoudront ces problèmes. Elles pourront fonctionner comme les banques le faisaient avant la nationalisation de la monnaie. Les différentes banques pourront avoir des politiques différentes, certaines plus agressives, d'autres plus conservatrices. [...] Je pense que tel sera le destin ultime du bitcoin, à savoir être la "monnaie de base" qui sert de monnaie de réserve aux banques qui émettent leur propre argent liquide. La plupart des transactions en bitcoin se feront entre banques, pour régler les transferts nets. Les transactions en bitcoin effectuées par des particuliers seront aussi rares que... eh bien, que les achats en bitcoin le sont aujourd'hui [13]. »

Cette vision a été reprise en 2018 par Saifedean Ammous dans son livre, *L'Étalon-Bitcoin*, dans lequel il soutenait que le rôle principal du bitcoin était d'être une monnaie de réserve [14]. Cette thèse a été par la suite développée par d'autres personnes comme Nik Bhatia.

Dans la réalité, cette manière de détourner l'activité de la chaîne s'est effectivement matérialisée avec les places de marché, qui permettaient de traiter les nombreux ordres d'achat et de vente liés à la spéculation. Elle s'est aussi manifestée par le biais des plateformes de casino qui regroupaient les opérations liées au jeu d'argent. Enfin, elle a été mise en œuvre par les services fiduciaires comme Grayscale qui offraient aux institutions financières la possibilité d'intégrer du bitcoin à leur bilan.

Toutefois, il ne s'agit nullement d'un passage à l'échelle de Bitcoin. Le traitement bancaire n'est pas résistant à la censure, ni résistant à l'inflation, et sa généralisation conduirait *in fine* à la destruction totale de la proposition de valeur de Bitcoin. Ainsi, on peut vraisemblablement supposer qu'une telle solution ne peut fonctionner qu'à petite échelle, pour des montants modestes, dans la mesure où l'État ne va pas intervenir, comme dans le cas de Bitcoin Beach au Salvador.

La deuxième variante de cette solution est de passer, non plus par des contrats juridiques reposant sur la confiance, mais par des contrats autonomes, dans le but de gérer les transferts en dehors de la chaîne. L'idée est ainsi de minimiser la confiance pour rendre le procédé viable. C'était par exemple la démarche derrière les *fidelity bonds*, proposés par Peter Todd en 2013, dont le but était de réduire l'influence du tiers en préservant de la confidentialité financière des clients et en permettant d'auditer efficacement les banques [15].

Cette démarche s'est popularisée au moyen de ce qu'on appelle généralement le passage en surcouche (*layering*) qui consiste à déporter l'activité financière vers des protocoles ouverts et décentralisés, préservant partiellement les propriétés de la chaîne. L'idée est de condenser une multitude de transferts en un petit nombre de transactions effectuées sur la couche de base, c'est-à-dire la chaîne de blocs. Cette terminologie est issue de la décomposition en couches de la suite des protocoles Internet, qui est organisée en couches multiples dépendant l'une de l'autre, comme TCP qui dépend de IP.

Dans le passage en surcouche, le compromis de sécurité est partiel (seuls certains bitcoins sont concernés) et limité dans le temps (ces bitcoins peuvent être récupérés sur la chaîne), par opposition au compromis de sécurité total et persistant imposé par l'augmentation de la taille limite des blocs. Il s'agit d'une méthode conforme au modèle à deux couches que Nick Szabo imaginait pour bit gold, avec une couche de base dont le rôle était de garantir la rareté infalsifiable de la monnaie, et une couche supérieure qui permettait de réaliser les paiements effectifs.

Il existe ainsi une diversité de propositions permettant d'effectuer ce pas-

sage en surcouche en réalisant un compromis plus ou moins important. Les principales sont les chaînes latérales, le réseau Lightning et Fedimint, dont nous parlerons en détail par la suite. Il existe également d'autres propositions comme l'échange d'objets physiques (OpenDime), le protocole Rumple, les statechains, les ZK-rollups ou encore le protocole Ark.

Les chaînes latérales

Les chaînes latérales, ou *sidechains* en anglais, sont des chaînes de blocs secondaires fonctionnant parallèlement à une autre chaîne de blocs dite « principale ». Elles ont été formalisées en octobre 2014 par les développeurs de Blockstream [16]. Cette solution technique apporte une capacité de traitement supplémentaire et une extensibilité supérieure, au prix d'une sécurité locale sensiblement amoindrie. En 2014, Blockstream envisageait de construire ainsi tout un écosystème de chaînes latérales permettant d'accomplir des tâches impossibles sur la chaîne principale comme l'émission d'actifs natifs, le déploiement de contrats autonomes avancés ou la gestion de noms de domaine.

Une chaîne latérale est une chaîne de blocs parallèle à une autre qui permet de transférer des fonds d'une chaîne à l'autre sans mettre en jeu l'intégrité des fonds déplacés. Il s'agit généralement de procéder à un ancrage bilatéral (*two-way peg*) permettant aux bitcoins d'être transférés d'une chaîne à l'autre sans perte de valeur, comme représenté sur la figure 14.1. Dans un sens, les bitcoins sont verrouillés sur la chaîne principale et leur équivalent est créé sur la chaîne latérale ; dans l'autre, les bitcoins sont détruits sur la chaîne latérale et leur équivalent est déverrouillé sur la chaîne principale.

Deux aspects différencient le modèle de sécurité d'une chaîne latérale de celui de la chaîne principale : le maintien de l'ancrage bilatéral et le mécanisme de consensus. Le premier consiste à décider qui peut déverrouiller les fonds lors d'un transfert de la chaîne latérale vers la chaîne principale. En effet, puisque la chaîne latérale est voulue comme un complément (et pas comme une extension), les nœuds de la chaîne principale n'ont pas connaissance de cette chaîne latérale. De ce fait, le retrait est soumis à une certaine confiance, placée usuellement dans une fédération de participants qui se méfient les uns des autres.

Le second aspect concerne la confirmation des transactions sur la chaîne latérale, et ici les options sont plus variées. Le consensus peut reposer sur le minage combiné, auquel cas c'est le travail de la chaîne principale qui est utilisé. Il peut se fonder sur la preuve d'enjeu, auquel cas c'est l'unité de

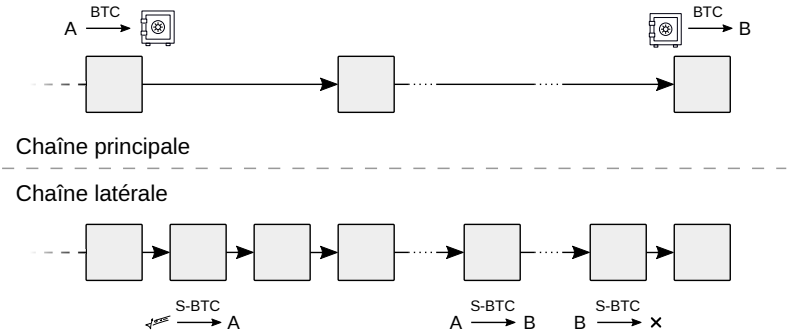

FIGURE 14.1 – Chaîne latérale : dépôt, transfert et retrait.

la chaîne principale qui est impliquée. Ou il peut recourir à une fédération se mettant d'accord grâce à un algorithme BFT classique, auquel cas c'est l'appartenance à cette fédération qui importe (preuve d'autorité).

Cette vision s'est concrétisée avec le lancement sur BTC de deux chaînes latérales distinctes en 2018. La première était RSK (aussi appelée Rootstock), qui a été lancée par Sergio Lerner en janvier de cette année-là et qui était focalisée sur l'exécution d'une machine virtuelle Turing-complète s'approchant de celle d'Ethereum. La seconde était Liquid, qui était la mise en œuvre du modèle Elements développé par Blockstream et dont le but primaire était de faciliter les transactions entre les différents acteurs financiers du secteur, dont notamment les plateformes d'échange. Dans Liquid, la sécurité repose sur une fédération de fonctionnaires qui assurent les deux rôles : ils maintiennent l'ancrage du L-BTC en tant que gardiens (*watchmen*) et participent au consensus de la chaîne en tant que signataires de blocs (*blocksigners*). RSK allie le minage combiné et une fédération de « notaires » pour assurer à la fois l'ancrage du RBTC et le traitement des transactions.

Les deux chaînes latérales n'ont cependant pas réussi à attirer une activité significative au fil des années, en raison des risques liés. En effet, utiliser ces chaînes requiert toujours une forme de confiance qui, bien que réduite au possible, reste bien présente. Un exemple malheureux d'une sidechain qui a mal tourné est celui de la chaîne latérale SmartBCH de Bitcoin Cash, où la société qui gérait le plus gros pont entre les deux chaînes, CoinFLEX, a fait faillite et n'a pas été en mesure de rembourser les utilisateurs.

Pour répondre à ces inconvénients et réduire la confiance impliquée, un protocole plus avancé a été élaboré par le chercheur Paul Sztorc depuis novembre 2015 : Drivechain [17]. Comme son nom l'indique (*drive chain* signifie

chaîne de transmission), il s'agit d'une véritable machine de création et de gestion de chaînes latérales.

La caractéristique principale de Drivechain est que l'ancrage bilatéral est confié aux mineurs, grâce au dépôt fiduciaire par taux de hachage (*hash-rate escrow*) défini dans le BIP-300. Durant chaque période de six mois (26 300 blocs), les mineurs votent pour la transaction de retrait de la chaîne latérale distribuant les fonds aux utilisateurs en ayant fait la requête. La transparence et la lenteur de ces transactions permettent à l'ensemble des commerçants de la chaîne principale de les auditer. Les transferts courants, plus rapides, se font par des échanges atomiques ou par des services centralisés.

La validation des transactions sur la chaîne latérale utilisant Drivechain peut être assurée par n'importe quel algorithme de consensus. Mais le plus naturel est d'utiliser le minage combiné. C'est pourquoi le projet Drivechain contient également la proposition du minage combiné « aveugle » (BIP-301), une technique permettant aux mineurs de la chaîne principale de déléguer automatiquement la validation d'une chaîne latérale à autrui contre une rémunération. Le validateur gagne la différence entre le revenu de la chaîne latérale et l'achat du « droit de trouver un bloc ». Ceci a pour effet de ne pas obliger les mineurs à gérer les chaînes latérales tout en touchant une partie de leur revenu.

Drivechain est un concept astucieux qui aurait pour avantage de pleinement réaliser la vision de Blockstream de 2014. Cependant, il présente un inconvénient majeur : le modèle de sécurité de son ancrage bilatéral. Celui-ci repose en effet sur le recours éventuel à un soft fork réalisé par les commerçants dans le but de corriger une transaction de retrait frauduleuse, qui serait par exemple le fait de mineurs malintentionnés cherchant à voler l'argent du dépôt fiduciaire. Il se fonde donc sur la propension des commerçants à suivre l'activité de la chaîne latérale en question d'une part, et à procéder à une modification du protocole pour geler la transaction incriminée d'autre part. C'est pourquoi cette proposition est, encore aujourd'hui en 2023, largement disputée.

Le réseau Lightning

Le réseau Lightning, ou *Lightning Network* en anglais, est un concept de réseau de canaux de paiements bidirectionnels. Celui-ci a été présenté pour la première fois le 23 février 2015 par Joseph Poon et Thaddeus Dryja lors d'un séminaire de développeurs Bitcoin à San Francisco [18]. À l'époque, des propo-

sitions concurrentes basées sur des idées similaires existaient comme Amiko Pay (conceptualisé par Corné Plooy), Impulse (développé par Jeff Garzik pour Bitpay) et Ström (imaginé par la start-up Strawpay), mais Lightning est rapidement devenu dominant. En 2023, il s'agissait de la solution favorisée par les utilisateurs de BTC pour effectuer davantage de transferts, si bien que le sigle LNP/BP a émergé pour désigner l'ensemble des protocoles intervenant dans le passage en surcouche (à l'instar de TCP/IP vis-à-vis d'Internet).

L'infrastructure du réseau Lighning repose sur des canaux de paiement qui sont ouverts et fermés entre des participants. Un canal de paiement est, comme décrit dans le chapitre 13, un ensemble de contrats autonomes qui permet à deux personnes d'effectuer des paiements répétés de manière sûre et instantanée à partir de liquidités préalablement bloquées. L'utilisation d'un canal est par conséquent limitée par sa capacité, c'est-à-dire la somme des deux soldes des acteurs concernés.

Le principe du réseau Lightning est de router les paiements au travers de ces canaux par l'intermédiaire de HTLC, qui sont des contrats d'engagement plus complexes permettant de mettre à jour les canaux concernés [19]. Un paiement transite sur le réseau moyennant des frais minimes qui vont aux nœuds le relayant. Le réseau Lightning est donc semblable à un boulier, dont les tiges sont des canaux et dont les boules sont les satoshis qui transitent d'un côté ou de l'autre des canaux, comme on peut le voir sur la figure 14.2.

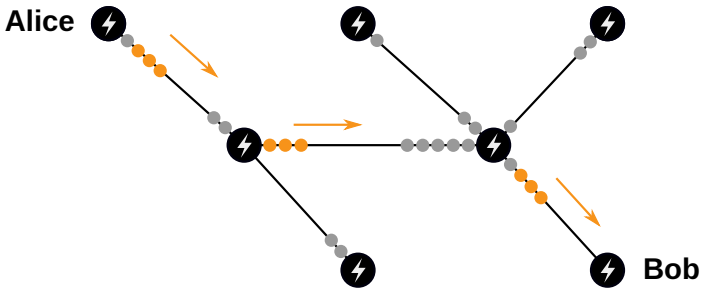

FIGURE 14.2 – Paiement de 3 mBTC sur le réseau Lightning.

Ce fonctionnement offre la possibilité de réaliser des paiements quasi instantanés et peu chers. Il permet de faire plus de transferts en bitcoins sans réaliser davantage de transactions sur la chaîne et sans déléguer explicitement la gestion des fonds à un tiers. De plus, le modèle conserve toute la programmabilité de Bitcoin et ouvre le champ des possibles quant à l'utilisation monétaire sur Internet.

Toutefois, l'apport de Lightning est à nuancer car il n'est pas exempt de défauts. D'abord, il hérite des inconvénients liés au modèle des canaux de paiement où, dans le cas du protocole de Poon-Dryja, une erreur peut mener à la perte des fonds. Puis, les contraintes liées à la capacité et au routage créent nécessairement une tendance à la centralisation, notamment par l'émergence de ce qu'on appelle les *Lightning Service Providers*, ce qui pourrait mener à l'installation d'une certaine censure. Ensuite, contrairement aux idées reçues, la confidentialité sur Lightning est faible, les paiements se faisant entre des clés publiques identifiées et transitant par des intermédiaires. Enfin, le réseau est soumis au niveau des frais sur la chaîne principale, ces derniers étant nécessaires au règlement des contrats, ce qui limite la capacité transactionnelle supplémentaire apportée.

Le réseau Lightning est donc adapté pour traiter les paiements du quotidien et les micropaiements, ne nécessitant pas forcément la confidentialité et la résistance à la censure offertes par la chaîne de blocs, à partir de canaux bien pourvus et régulièrement réapprovisionnés. Il a été mis en œuvre à partir de janvier 2018, principalement en surcouche de BTC, et s'est développé considérablement depuis, tant d'un point de vue technique qu'économique. Trois implémentations logicielles ont été maintenues par trois entités différentes (lnd par Lightning Labs, c-lightning par Blockstream, eclair par ACINQ) et un système de standards techniques (appelés *Bases of Lightning Technology* ou BOLT) a fini par émerger. Du côté économique, le réseau a rencontré un certain succès en attirant les capitaux et, en novembre 2023, une capacité totale de 5 400 BTC, équivalant à environ 200 millions de dollars, était réservée pour fournir de la liquidité pour les paiements.

Les banques chaumiennes de Fedimint

Une autre proposition est Fedimint [20], qui est un protocole de garde et d'échange confidentiel de bitcoins dans un contexte communautaire. D'un point de vue technique, il s'agit de confier la garde des bitcoins à une fédération et d'échanger des billets chaumiens (eCash) émis par ladite fédération. Ce fonctionnement explique le nom du protocole, qui est une abréviation approximative de *Federated Chaumian Mint* (« monnaierie chaumienne fédérée » en français).

Fedimint a été imaginé par le cypherpunk Eric Sirion au cours de l'année 2021 et implémenté sous forme minimale sous le nom de MiniMint. Sirion a été doublement inspiré par les tentatives d'appliquer eCash en surcouche de

Bitcoin comme SCRIT et par les approches communautaires telles que Bitcoin Beach au Salvador. La première transaction d'une fédération Fedimint a eu lieu le 28 septembre 2022 durant le Hackers Congress de Paralelni Polis.

La première composante de Fedimint est la banque chaumienne qui est gérée par la fédération. Celle-ci utilise le procédé de signature aveugle de David Chaum pour émettre des certificats adossés à un certain montant de satoshis, qui peut être récupéré à tout moment sur la chaîne ou sur le réseau Lightning. Cette composante assure la confidentialité financière partielle des participants : la banque n'a pas connaissance des échanges réalisés par les clients, mais son rôle de prévention de la double dépense exige qu'elle voie les revenus des commerçants [21].

L'idée d'utiliser eCash en surcouche de Bitcoin n'est pas une idée nouvelle. Elle a été proposée et implémentée pour la première fois le 17 août 2010, par un individu intervenant sous le pseudonyme fellowtraveller sur le forum de Bitcoin sous la forme de son projet Open Transactions. Le projet ne s'est jamais imposé, car le besoin ne se faisait pas ressentir et le système était probablement trop complexe. Cependant, l'idée est revenue timidement sur les devants de la scène au cours du débat sur la scalabilité avec la proposition des « certificats aveugles au porteur » de Theymos (administrateur du subreddit r/Bitcoin et du forum Bitcointalk) en décembre 2016. Elle a également été reprise en 2019 par Frank Braun et Jonathan Logan (coanimateurs du podcast Cypherpunk Bitstream) au moyen de SCRIT, un projet de système chaumien fédéré dont le nom est l'acronyme de « *Secure, Confidential, Reliable, Instant Transactions* ». Le dernier projet en date d'une mise en œuvre d'un système chaumien centralisé est Cashu, un protocole développé en 2022 par le développeur callebtc, qui permet la création et l'échange de certificats-bitcoin en surcouche de Lightning et de nouveaux jetons.

L'intérêt de Fedimint, tout comme son prédécesseur SCRIT, est de décentraliser la garde de bitcoins. Pour ce faire, il combine le système chaumien avec une approche dite « communautaire », consistant à déployer une banque gérée par les membres de confiance d'une communauté locale.

Cette approche a été illustrée par l'expérience de Bitcoin Beach, un projet de développement économique durable autour de la plage d'El Zonte au Salvador. Une banque communautaire a ainsi vu le jour en 2020 et permet depuis lors aux locaux d'échanger des bitcoins de façon sûre et fiable, par le biais du Bitcoin Beach Wallet (devenu Blink) développé par Galoy. C'est cette expérience qui a inspiré l'adoption du cours légal à l'échelle nationale en septembre 2021.

La deuxième composante de Fedimint est donc une fédération, semblable aux fédérations des chaînes latérales comme Liquid ou RSK, mais composée de personnes de confiance qui possèdent les capacités techniques nécessaires à la gestion d'un nœud. Les membres de cette fédération, appelés gardiens, sont responsables de la mise en place de l'infrastructure et se chargent de conserver les fonds des utilisateurs et d'assurer le bon fonctionnement de la banque chaumienne. Ils se coordonnent en utilisant un algorithme de consensus classique (appelé HBBFT) qui, comme tous les algorithmes de ce type, demande un minimum de 66 % d'acteurs honnêtes pour fonctionner.

L'emploi de cette fédération représente un compromis technique évident entre la propriété entière des fonds et sa délégation auprès d'un acteur unique. Ce compromis apporte des avantages majeurs au niveau des frais de traitement des transactions et de la facilité d'utilisation, mais engendre également des risques importants. Ceux-ci sont le risque de garde (la fédération peut voler ou perdre des fonds), le risque d'émission frauduleuse (elle peut émettre plus de certificats qu'elle n'a de bitcoins), le risque de censure (elle peut refuser de valider une transaction) et le risque réglementaire (la fédération peut être saisie et fermée sur décision étatique).

Tout ceci fait que Fedimint ne peut pas être conçue comme une solution de scalabilité, mais comme une proposition de remplacement des applications dépositaires. L'objectif de Fedimint est d'améliorer la garde de bitcoins en la décentralisant et en accroissant la confidentialité des échanges internes. Son caractère local doit permettre d'échapper aux réglementations financières, et ainsi de ne pas subir le sort réservé aux banques classiques.

Le passage à l'échelle par substitution

Le passage en surcouche est une manière correcte d'accroître le volume économique lié à une chaîne donnée sans trop affecter ses caractéristiques premières. Néanmoins, cette approche présente aussi des limites : non seulement les différentes surcouches ont leurs défauts propres, mais surtout elles reposent en dernier lieu sur le règlement réalisé sur la chaîne de blocs, dont la capacité est limitée. Par conséquent, le plancher d'utilité n'est pas supprimé par le passage en surcouche et on ne peut ainsi pas voir ce dernier comme un moyen miraculeux de traiter une infinité de transactions.

La plage de valeurs desservie par un système cryptomonétaire donné a pour effet de créer une demande pour des systèmes de substitution plus à même d'assurer le transfert hors de cette plage. Un système dont le niveau de frais est

élevé laisse la voie libre à l'utilisation d'un système moins sûr mais moins cher, permettant le traitement des plus petites transactions. À l'inverse, un système dont le niveau de sécurité est faible favorise l'émergence d'un système plus cher mais aussi plus sûr, autorisant les plus gros transferts. Il existe de ce fait une certaine complémentarité entre les différentes mises en œuvre de Bitcoin qui permettent de gérer l'intégralité de l'activité transactionnelle émanant des utilisateurs [22].

Au cours de l'histoire, une telle complémentarité s'est manifestée par l'utilisation de plusieurs métaux précieux comme base monétaire. L'or ne pouvait pas permettre de couvrir toutes les plages de valeurs : celui-ci était adapté au transfert de grosses sommes, chose pour laquelle il a été sélectionné comme monnaie de réserve mondiale, mais pas à l'échange de petite monnaie. C'est pour remplir ce dernier rôle complémentaire que l'argent, et d'autres métaux moins précieux comme le cuivre, ont été utilisés. L'argent, mot qu'on utilise encore aujourd'hui en français comme synonyme de monnaie, était la monnaie du quotidien tandis que l'or servait essentiellement aux règlements plus onéreux.

Cet aspect bimétallique (voire trimétallique) de la monnaie a perduré pendant des siècles, de la Haute Antiquité jusqu'au XIXe siècle. Il était reconnu par les pouvoirs publics qui définissaient leur monnaie comme un poids en or ou en argent, et frappaient des pièces d'or et d'argent en décrétant un taux de change selon le ratio or-argent du marché. On constate d'ailleurs que ce ratio or-argent a été relativement stable au cours de l'histoire en variant entre 10 et 18, ce qui confirme le rôle monétaire de l'argent aux côtés de l'or.

Toutefois, avec l'émergence de l'étalon-or et la disparition du bimétallisme à la fin du XIXe siècle, l'argent a peu à peu perdu son rôle monétaire pour être remplacé par la monnaie papier, dans un premier temps adossée à l'or, bien plus commode pour effectuer des échanges. Le ratio a augmenté en conséquence et est passé de 15,5 en 1870 à 80 aujourd'hui, ce qui correspond à une perte de valeur de l'argent de plus de 80 % par rapport à l'or.

L'analogie avec les métaux précieux est éclairante. Puisque la version principale de Bitcoin (BTC) n'est pas adaptée pour traiter les transferts de plus petite valeur, il s'ensuit que ces transferts potentiels sont réalisés au moyen d'une monnaie de substitution (de la cryptomonnaie, de la monnaie fiat liquide, du crédit déplacé par des services bancaires permissifs, etc.) voire ne sont pas traités du tout. Litecoin, dont la principale narration est qu'il s'agirait d'un argent numérique au même titre que Bitcoin serait un or numérique, répond tout à fait à cette demande. Il était ainsi présenté dès son

lancement comme une « version allégée de Bitcoin » ayant pour but d'être « à l'argent ce que Bitcoin est à l'or[23] ». Cette désignation ne provient pas tant du fait qu'il y a quatre fois plus de litecoins que de bitcoins, ce qui n'a aucune incidence sur le système, mais plutôt du fait que la capacité transactionnelle maximale de LTC est quatre fois plus grande, ce qui amoindrit la sécurité potentielle du système. Cette analyse vaut également pour Bitcoin Cash à une échelle encore plus grande.

Dans cette vision, les mises en œuvre alternatives de Bitcoin serviraient à traiter toutes les transactions, au prix de nécessaires transferts entre les chaînes. Ces derniers seraient assurés par des services de change centralisés ou par des systèmes d'échanges atomiques basés sur des carnets d'ordres publics. Cette solution, bien qu'imparfaite, serait tout à fait naturelle et est d'ailleurs déjà pratiquée aujourd'hui.

L'extensivité est également concernée par cet effet. Le coût technique d'une utilisation complexe de Bitcoin peut être compensé par des systèmes de substitution de moindre qualité. La confidentialité à bas coût peut être assurée par Monero et la programmabilité simplifiée par Ethereum Classic par exemple. Comme le remarquait très justement Satoshi Nakamoto en décembre 2010, à propos de la pertinence de BitDNS (le futur Namecoin) :

> « Le fait de rassembler tous les systèmes de quorum par preuve de travail dans une seule base de données ne passe pas à l'échelle. Bitcoin et BitDNS peuvent être utilisés séparément. [...] Les réseaux ont besoin d'avoir des destins différents. Les utilisateurs de BitDNS pourraient être extrêmement tolérants vis-à-vis de l'ajout de fonctionnalités permettant de traiter des données volumineuses, puisque peu de registraires de noms de domaine seraient nécessaires, tandis que les utilisateurs de Bitcoin pourraient devenir de plus en plus sectaires à propos de la limitation de la taille de la chaîne, pour que son accès reste facile pour beaucoup d'utilisateurs et pour les petits appareils[24]. »

Trois types de compromis

La scalabilité de Bitcoin est un sujet complexe. Contrairement à ce qui est parfois affirmé, un système donné est très peu scalable. Sa capacité à passer à l'échelle ne peut être améliorée qu'au moyen d'optimisations logicielles, matérielles ou algorithmiques. Le gain en performance sur la chaîne se fait la plupart du temps au prix d'un compromis direct, avec l'augmentation de la limite de capacité transactionnelle, ou indirect, avec l'altération du modèle de sécurité.

C'est la raison de l'existence du passage en surcouche, qui consiste à déporter une partie des transferts économiques vers des protocoles ouverts et

décentralisés, préservant partiellement les propriétés de Bitcoin et reposant sur le règlement des litiges sur la chaîne. Dans cette démarche, le compromis de sécurité est partiel et limité dans le temps, contrairement au cas de l'augmentation de capacité transactionnelle où il est total et persistant. Le passage de surcouche s'est développé sur BTC au cours du temps par le biais des chaînes latérales, proposées en 2014 et mises en œuvre en 2018, du réseau Lightning, proposé en 2015 et déployé depuis 2018, et de Fedimint, proposé en 2021.

L'autre alternative est le passage à l'échelle par substitution, qui consiste, en substance, à déplacer les transactions les moins à risque vers des substituts de moins bonne qualité, c'est-à-dire des mises en œuvre moins sécurisées du concept Bitcoin. Cet effet s'est réellement manifesté pour la première fois en 2017 avec les premières congestions du réseau BTC et la hausse de la demande pour des contrats autonomes statiques (Ethereum), qui se sont notamment accompagnées d'une baisse de la dominance économique de la version principale de Bitcoin. Les maximalistes ont tendance à prétendre que le passage en surcouche permet de traiter l'ensemble des utilisations pertinentes de Bitcoin, mais, jusqu'à preuve du contraire, ce n'est pas le cas.

15

L'avenir de Bitcoin

La découverte de Bitcoin par Satoshi Nakamoto constitue une révolution conceptuelle profonde dans le domaine monétaire. C'est ce qui explique pourquoi, depuis 2008, il a suscité les plus grandes passions tant au sein de ses partisans que parmi ses détracteurs. Certains ont voulu y voir la solution à tous les problèmes de ce monde, une monnaie universelle qui devait remplacer l'or et toutes les monnaies fiat, sans résistance de la part de l'adversaire. D'autres ont tenté de le présenter sous les traits d'un système nuisible et pollueur d'escroquerie organisée, dans un rejet épidermique propre aux institutions pour lesquelles ils travaillaient.

Dans cet ouvrage, nous avons tenté de faire la part des choses, en décrivant précisément d'où vient Bitcoin, à quels enjeux il fait face et quels sont les principes qui le soutiennent. Par sa conception, il constitue un outil d'une rare élégance dont les mécanismes méritent d'être détaillés, ce qui a été fait ici. En guise de conclusion, résumons ce que nous avons développé avant de nous concentrer sur l'avenir de Bitcoin en tant que tel.

L'élégance de Bitcoin

D'abord, rappelons que Bitcoin n'est pas sorti de nulle part. Il est un produit de l'évolution technique qui a eu lieu durant la seconde moitié du XX^{e} siècle, en reposant largement sur l'ordinateur personnel, sur la cryptographie asymétrique et sur le réseau Internet. Du côté idéologique, il provient de

mouvements divers, comme l'agorisme, le librisme ou l'extropianisme, dont la particularité commune était d'appeler à la pratique, de recommander d'agir dans le réel au lieu de se contenter de le théoriser. En particulier, il est issu du mouvement des cypherpunks qui, dès le début des années 90, préconisaient d'utiliser la cryptographie de manière proactive en vue de protéger la confidentialité et les droits des personnes dans le cyberespace naissant. La valeur principale derrière Bitcoin est donc la liberté.

En outre, il est le résultat d'une longue quête pour la cybermonnaie, qui avait notamment été entreprise par les cypherpunks. Bitcoin doit son existence au système chaumien d'eCash, qui a eu son heure de gloire au milieu des années 90 avant de disparaître. Il s'inspire des tentatives de monnaies numériques privées comme le Liberty Dollar, e-gold et Liberty Reserve, qui ont toutes été arrêtées par l'État à l'aube du XXIe siècle. Il s'inscrit dans la lignée des concepts de monnaie décentralisée qu'étaient b-money, bit gold, RPOW et, dans une certaine mesure, Ripple.

Bitcoin a été découvert par Satoshi Nakamoto en 2007, qui en a publié le livre blanc descriptif le 31 octobre 2008, avant de finaliser le prototype et de lancer le réseau en janvier 2009. Après des débuts difficiles, la cryptomonnaie a timidement émergé du néant en attirant à elle les personnes intéressées par son potentiel. Ces personnes ont contribué à construire Bitcoin en participant à son développement informatique, au minage et au commerce. Une fois le projet définitivement lancé en 2010, Satoshi a disparu progressivement et a laissé la main à ses collaborateurs de confiance. Son anonymat demeure complet à ce jour.

Après le départ du fondateur, la communauté a dû s'organiser. C'était l'époque des premières conférences, des premières discussions autour de l'avenir du protocole et du développement des premiers portefeuilles légers. Cependant, la décentralisation du développement de Bitcoin a fait qu'il n'y avait plus un seul point de vue dominant à son sujet, ce qui a créé de multiples conflits, à commencer par la querelle de P2SH en 2011–2012. Quatre clivages majeurs ont émergé : le premier concernait la financiarisation, c'est-à-dire la réintroduction partielle de tiers de confiance ; le deuxième se concentrait sur le passage à l'échelle, et le choix de savoir s'il fallait augmenter la capacité transactionnelle de la chaîne ou utiliser des solutions de surcouche ; le troisième gravitait autour du développement des cryptomonnaies alternatives, vivement décrié d'un côté et applaudi de l'autre ; le quatrième se basait sur l'intégration institutionnelle, c'est-à-dire la question de la coopération ou du rejet vis-à-vis de l'autorité. Ces conflits ont fait de Bitcoin ce qu'il est aujourd'hui.

Bitcoin constitue une nouvelle forme de monnaie. Il s'agit d'un intermédiaire d'échange dont la gestion est distribuée, c'est-à-dire qu'elle ne repose pas sur une autorité centrale. Même si sa résistance au changement le rapproche des biens tangibles, le bitcoin n'est pas une monnaie-marchandise, car ses propriétés ne proviennent pas de caractéristiques intrinsèques du monde physique. Même s'il reprend le caractère numérique du système bancaire, ce n'est pas une monnaie scripturale, car les entrées sur son registre ne correspondent pas à des créances. Même s'il n'a pas d'utilisation non monétaire significative, ce n'est pas une monnaie fiduciaire centralisée, car il ne repose pas sur la confiance placée dans un acteur unique. En définitive, le bitcoin appartient à une nouvelle catégorie et peut être décrit comme une monnaie réticulaire (en référence à son réseau) ou une monnaie fiduciaire distribuée, dans le sens où il répartit la confiance sur le réseau de nœuds utilisés par les commerçants plutôt que de la concentrer entre les mains d'une entité unique.

Bitcoin est un « système d'argent liquide électronique pair à pair » qui permet « aux paiements en ligne d'être envoyés directement d'une partie à l'autre sans passer par une institution financière ». Il constitue un concept de monnaie numérique résistante à la censure et à l'inflation, qui rend difficile l'entrave des transactions et la création d'unités supplémentaires. Bitcoin est un outil dont le domaine d'application naturel se situe à la marge, à la limite de la légalité, voire dans l'illégalité. Il est une monnaie de désobéissance utilisée par les activistes politiques, par les lanceurs d'alerte et par les organisations qui s'opposent à l'autorité. Il est une monnaie de la liberté utilisée par les personnes censurées comme celles dont les professions sont jugées déviantes, celles qui font l'erreur d'exprimer une opinion discordante ou celles qui ont eu la malchance de naître dans le mauvais pays. Il est une monnaie du marché noir utilisée par l'économie souterraine, notamment dans le cadre de la résistance fiscale.

Ce statut de monnaie de la liberté fait qu'il s'inscrit dans un rapport antagoniste avec l'État, dont la nature est de chercher à s'étendre toujours plus, notamment par l'affermissement de son contrôle sur la monnaie. Par sa supervision de la banque, l'État a altéré le support de la monnaie en la faisant reposer sur des pièces et des billets fiduciaires plutôt que sur des métaux précieux, et il pourrait recommencer demain en transformant la monnaie physique en une monnaie numérique de banque centrale accessible à tous, sujette à la surveillance et à la censure généralisées. Ce comportement prédateur de l'État est la raison derrière le fonctionnement distribué de Bitcoin, qui partage les risques entre les différents acteurs du système et confère à ce dernier une

robustesse sans précédent.

Bitcoin utilise un certain nombre de briques techniques pour fonctionner correctement. La première est la signature numérique qui permet d'assurer la propriété au sein du système. L'utilisateur peut posséder pleinement ses bitcoins par le contrôle exclusif qu'il exerce sur ses clés privées. Ce mécanisme offre la liberté unique de pouvoir gérer des fonds numériques de manière souveraine, mais demande aussi une certaine responsabilité vis-à-vis de la perte et du vol, qui n'existe pas dans le cadre d'une relation avec un tiers de confiance.

Pour lutter contre la double dépense, Bitcoin repose sur un algorithme de consensus novateur, qui met à jour une chaîne de blocs horodatés de transactions, au moyen d'un procédé de preuve de travail. Son fonctionnement ouvert et robuste le distingue des algorithmes de consensus classiques qui avaient jusqu'alors été mis en œuvre au sein des systèmes distribués. Le génie de Nakamoto est d'avoir sacrifié une partie de la sécurité de l'algorithme (en la rendant probabiliste plutôt qu'absolue) pour garantir la tolérance aux pannes byzantines. Ce modèle se fonde sur les incitations économiques des mineurs, qui estiment que miner la chaîne dans les règles est plus rentable que de l'attaquer.

Toutefois, le génie de la conception de Bitcoin ne s'arrête pas là. Celle-ci ne décourage pas seulement la double dépense, mais aussi la censure financière, qui constitue l'un des fléaux du transfert numérique aujourd'hui. La censure de Bitcoin consiste à miner une chaîne plus longue ne contenant pas les transactions indésirables. Grâce au paiement intégré de frais de transaction et au caractère externe de la preuve de travail, une telle suppression peut être combattue efficacement, conformément à la propriété de résistance à la censure du modèle.

Bitcoin est un concept de monnaie ouvert et libre, de sorte qu'il est par nature changeant et multiple. Il existe ainsi une diversité de mises en œuvre de Bitcoin, qui est affectée par deux effets contraires : l'effet de réseau et l'effet de substitution. Ainsi, la nature monétaire de Bitcoin fait qu'il ne peut subsister qu'un petit nombre de ces mises en œuvres, tandis que son absence de scalabilité invite à penser qu'il en persistera plusieurs.

La détermination du protocole, ou des protocoles, se fait de manière économique, par le biais de l'acceptation de la monnaie par les commerçants. Ces derniers ont le rôle le plus important en ayant le dernier mot sur les règles de consensus grâce à leur activité économique vérifiée par leurs nœuds. Plus généralement, le modèle de gouvernance est en réalité bien plus complexe

sociologiquement, les commerçants étant influencés par d'autres personnes participant au système, comme leurs clients, les détenteurs, les développeurs ou les mineurs, et d'une manière plus diffuse, par des acteurs externes, tels que les relais d'opinion, les puissances financières ou encore l'État.

La résistance à l'inflation, ou la difficulté à créer plus de bitcoins, émerge ainsi de la dynamique économique opposée à l'altération de la politique monétaire. Elle ne provient pas de l'absence d'unanimité de la communauté ou de l'établissement originel de la politique monétaire par Satoshi Nakamoto. La limite des 21 millions, en dépit de son caractère emblématique, n'est ainsi pas absolue et dépend à chaque instant de la décision des commerçants.

Le fonctionnement technique de Bitcoin est optimisé pour la monnaie, comme en témoigne son modèle de représentation des unités qui se base sur des pièces, et non sur des comptes comme Ethereum. Bien qu'aucune technique avancée n'ait été intégrée dans le prototype, Bitcoin est également conçu pour être confidentiel, la préservation de la vie privée étant nécessaire pour la fongibilité de la monnaie et sa résistance à la censure.

De plus, Bitcoin est programmable, de sorte qu'il est possible d'imposer des conditions de dépense à différentes pièces. Cet aspect modulable des transactions donne la possibilité à des inconnus d'échanger de la valeur de manière la plus confidentielle et sûre possible. Il est aussi à la base des protocoles de surcouche, comme le réseau Lightning, qui augmentent la capacité de traitement des échanges sans compromettre la sécurité du système de base.

Toutes ces propriétés font que Bitcoin forme un ensemble cohérent d'une rare élégance. Bitcoin constitue la pièce manquante du puzzle de liberté sur Internet. Bitcoin représente l'espoir d'une génération face à l'autorité étatique grandissante. Bitcoin incarne le projet d'un système monétaire alternatif robuste et durable. Et c'est ce qui explique le formidable élan qui l'a accompagné dans les premières années.

Les quatre menaces qui planent sur Bitcoin

Comme nous l'avons évoqué tout au long de cet ouvrage, Bitcoin n'est pas entièrement à l'abri des assauts de l'adversaire. Dans cette section, nous évoquerons les principales menaces qui planent sur Bitcoin aujourd'hui. Nous ne parlerons pas des risques techniques, que des personnes mieux informées ont déjà traités ; nous décrirons uniquement les dangers liés au comportement humain, qui émanent de l'action des acteurs économiques du système. Ces derniers sont en effet pour nous bien plus importants.

Les menaces humaines sont subtiles, car les attaques qu'elles facilitent surviennent généralement de manière soudaine. L'accroissement de ces menaces est similaire à une sorte de jeu de chaises musicales, où les participants tournent naïvement autour des chaises sans les surveiller. Tant que la musique retentit dans la pièce, tout va bien : l'adversaire enlève les chaises une par une, calmement, mais la ronde continue. C'est au moment où la musique s'arrête que les problèmes se manifestent.

Nous distinguons quatre menaces de ce type susceptibles de nuire à Bitcoin : la centralisation de l'activité économique, la centralisation de l'activité minière, la généralisation de la garde de fonds et l'effacement de la confidentialité. Celles-ci ne sont pas entièrement indépendantes, mais elles correspondent chacune à un comportement différent des acteurs.

La première menace est la centralisation de l'activité économique, qui émerge par l'intermédiaire du commerce important réalisé auprès des plateformes de change réglementées et par le recours quasi systématique à des processeurs de paiement externes et à des fournisseurs de portefeuille tiers. Celle-ci peut mener, comme nous l'avons décrit dans le chapitre 11, à une attaque d'altération du protocole, sous la forme d'un hard fork d'inflation, d'un soft fork taxatoire ou d'un soft fork de censure. Il est probable que cette attaque crée une scission d'une façon ou d'une autre. Elle est spécialement dommageable dans le cas où la chaîne altérée est majoritaire en raison de l'effet de réseau. L'attaque n'est néanmoins pas fatale pour le système car l'économie peut se reconstruire progressivement à partir de la chaîne libre.

La deuxième menace est la centralisation de l'activité minière, qui se manifeste notamment par le rapprochement géographique du matériel de minage, par le regroupement des hacheurs en coopératives et par l'utilisation collective de relais centralisés par les mineurs. Ce risque peut mener, comme vu dans le chapitre 9, à une attaque de censure des transactions par la majorité de la puissance de calcul du réseau. Cette attaque a logiquement des chances de se produire après la tentative d'altération du protocole, sur la chaîne libre ayant refusé les modifications. Elle a pour effet de paralyser une partie de l'activité en empêchant sa confirmation sur la chaîne. Elle bénéficie de l'analyse de chaîne qui lui permet d'isoler les transactions problématiques plutôt que de supprimer l'intégralité de l'activité. Elle n'est cependant pas mortelle pour le système, car du matériel de minage supplémentaire peut être déployé, suite à l'accroissement des frais des transactions censurées, afin de restaurer la situation initiale.

La troisième menace, apparentée à la centralisation de l'activité écono-

mique, est la généralisation de la garde de fonds par des dépositaires qui suivent les réglementations légales. Non seulement cette pratique n'est pas pertinente du point de vue individuel (un dépositaire peut censurer les transactions, saisir les fonds et gonfler la quantité de bitcoins-papiers qu'il distribue), mais sa propagation dans l'écosystème crée aussi un risque systémique. Cette menace se manifeste aujourd'hui par le développement de dépositaires institutionnels comme Coinbase Custody qui détiennent un pourcentage non négligeable des bitcoins en circulation et par l'accroissement des services adressés aux petits porteurs. Elle est plus dangereuse que la centralisation de l'économie, car l'économie « hébergée » ne peut pas se reformer s'il y a une attaque contre le protocole : ce sont les dépositaires réglementés qui sont les réels propriétaires des bitcoins, pas leurs clients. Il s'agit donc d'une dégénérescence persistante du système, qui se résorbe plus difficilement qu'une simple centralisation minière ou commerciale.

La quatrième menace, plus insidieuse, est l'effacement de la confidentialité, qui se matérialise par la surveillance généralisée (connaissance du client, preuve de propriété d'adresse) et, accessoirement, par l'analyse de chaîne qui l'accompagne. À l'instar de la garde de fonds par une entité réglementée, la complète transparence vis-à-vis de l'État constitue non seulement un errement individuel (la personne n'est protégée ni de la censure, ni de la saisie), mais aussi un risque systémique dans le cas où elle se généralise. En effet, une surveillance plus grande crée une économie davantage contrôlable, et rend par conséquent le protocole plus vulnérable. En outre, l'identification des acteurs a pour conséquence de réduire l'ensemble d'anonymat qui profite à tout le monde, et de diminuer la possibilité d'exercer une activité secrète. L'effacement de la confidentialité forme ainsi une dégénérescence subtile du système, qui ne peut être guérie que par la lutte contre les liens d'identification via l'application de bonnes pratiques, comme le mélange des pièces.

Ces menaces dépendent des actions des acteurs économiques de Bitcoin, et notamment de ses utilisateurs. Pour combattre ces menaces, il convient donc de pousser les utilisateurs à retirer leurs bitcoins sur un portefeuille, à arrêter de se soumettre à la connaissance du client, à rendre leurs bitcoins intraçables et à utiliser leurs propres nœuds, individuels ou communautaires. Cela concerne en particulier les nouveaux utilisateurs, ce qui nous amène au thème de l'adoption.

Les deux adoptions de la cryptomonnaie

Bitcoin est un système fondé sur des incitations économiques, dans lequel les personnes qui le font vivre sont récompensées. D'une part, les mineurs sont incités à confirmer les transactions pour toucher les frais de transaction. D'autre part, les commerçants sont incités à vérifier les règles de consensus pour bénéficier en toute quiétude de la proposition de valeur de Bitcoin. En outre, les détenteurs sont incités à promouvoir Bitcoin pour agrandir l'économie et profiter de la hausse résultante du pouvoir d'achat (ou du prix en dollars) de l'unité de compte. Cet agrandissement de l'économie, aussi appelé l'adoption, constitue donc logiquement l'un des objectifs naturels de ceux qui possèdent du bitcoin.

L'adoption de Bitcoin peut avoir lieu de multiples manières, mais deux modèles principaux se distinguent. Le premier est l'adoption par les individus et par les petites entreprises, qui correspond à un apport financier modeste à la valeur agrégée du bitcoin. Le second est l'adoption par les grandes entreprises, par les sociétés de courtage et par les institutions financières, qui représente un plus gros gain pour les détenteurs. Dans les premiers temps, il était impossible de convaincre cette dernière catégorie du bienfondé du bitcoin, mais avec le développement économique et grâce à une certaine conformité de la communication, il est devenu aujourd'hui bien plus aisé de la persuader d'y participer. Puisque cette adoption était beaucoup plus rentable pour les détenteurs, beaucoup d'entre eux ont choisi la voie de la facilité en remplissant leur discours d'éléments de langage destinés aux acteurs réglementés.

Mais cette seconde adoption du bitcoin, bien qu'elle soit certainement rentable sur le moment et qu'elle possède des mérites propres, a pour particularité de devenir stérile à long terme. En effet, elle crée une économie centralisée, surveillée voire entièrement dépositaire, c'est-à-dire une économie fragile à la merci des décisions étatiques. C'est pourquoi on peut la qualifier de « mauvaise adoption ».

Ainsi, la seule adoption à laquelle il vaut la peine de s'intéresser est celle de l'économie libre et indépendante, pour laquelle Bitcoin est adapté en premier lieu. Cette économie possède en effet les caractéristiques qui permettent à Bitcoin de perdurer. Elle est décentralisée et répartit les risques entre tous ses membres, pour bénéficier au maximum de la proposition de valeur de Bitcoin. Elle est désobéissante, dans le sens où elle refuse toute modification du protocole qui altérerait les propriétés fondamentales de Bitcoin. Elle protège sa propre confidentialité, car elle sait qu'elle a quelque chose à craindre de ceux qui la surveillent, quand bien même elle ne ferait rien d'illégal sur le moment.

Elle est circulaire, au sens où elle évite le plus possible le recours à la monnaie étatique, surtout sous sa forme numérique, car elle sent que cette dernière est de plus en plus contrôlée. Enfin, elle est exigeante, en demandant de l'individu un certain discernement et une certaine responsabilité, des qualités trop souvent négligées à notre époque moderne.

Toutefois, les contraintes de cette « bonne adoption » font qu'elle n'est pas accessible à tous. Non seulement l'utilisation souveraine de Bitcoin demande d'être un minimum responsable, mais elle présente aussi des inconvénients majeurs, qui sont (à l'heure actuelle) la volatilité du pouvoir d'achat, le coût de transaction, le manque de scalabilité et la réglementation dissuasive. De ce fait, il est difficile d'envisager que tout le monde fera du bitcoin sa monnaie de prédilection à court ou moyen terme. Pour le dire autrement : l'adoption de masse n'aura pas lieu de sitôt, et l'utilisation de Bitcoin restera dans un premier temps confinée à la portion de la population qui cherche à s'extraire du système étatico-bancaire et à résister aux puissances de ce monde.

Il est donc illusoire de s'attendre à une « hyperbitcoinisation », c'est-à-dire à un remplacement rapide des monnaies fiat par le bitcoin. Tant qu'il y existe une masse de gens qui continuera d'obéir aveuglément au pouvoir, la monnaie étatique subsistera. Seule la nécessité pourra pousser cette masse à faire un usage opportuniste et temporaire de Bitcoin.

Une culture en gestation

La culture est l'ensemble des aspects matériels, intellectuels, affectifs et spirituels, qui caractérisent des sociétés ou des groupes sociaux. Chaque association humaine durable a tendance à développer une culture propre. La communauté de Bitcoin, bien que vaguement délimitée, n'échappe pas à ce phénomène. Des éléments culturels ont émergé dans Bitcoin dès ses débuts et se sont multipliés à mesure que le réseau grandissait, pour finir par donner naissance à une véritable *subculture*.

Cette culture est logiquement pétrie de politique, entre l'animosité à l'égard des représentants de l'autorité et les références multiples aux cypherpunks et aux économistes autrichiens. Elle est aussi constituée de pratiques monétaires ritualisées, de recommandations hygiéniques (notamment à l'encontre des crypto-actifs douteux), d'œuvres d'art futuristes, de livres et de podcasts en tous genres, de regroupements (rencontres mensuelles, conférences) et de commémorations régulières d'évènements qui ont marqué l'histoire de la cryptomonnaie. La culture de Bitcoin, la monnaie d'Internet, repose également beaucoup sur des formules courtes répétées à foison et sur des mèmes

humoristiques, particulièrement adaptés pour la propagation sur les médias sociaux.

La culture, et plus précisément la part de la culture que l'on pourrait qualifier de religieuse, a pour conséquence d'orienter les actions des individus. Puisque Bitcoin est un outil dont la sécurité dépend de l'utilisation qui en est faite, cet aspect culturel est fondamental. Par exemple la phrase « *not your keys, not your bitcoins* » inventée par Andreas Antonopoulos est bien plus convaincante pour pousser les gens à placer leurs fonds dans des portefeuilles que n'importe quel exposé historique des faillites et des gels de compte associés aux plateformes dépositaires. Mais la culture peut aussi, par une mauvaise orientation, induire de mauvais comportements et finalement nuire au système.

En tant qu'objet spéculatif dont le prix a été multiplié par 30 millions en l'espace de 14 ans, le bitcoin a attiré les personnes avides de gains financiers. Celui-ci bénéficiait d'une rareté absolue par conception, ce qui ne s'était jamais vu dans l'histoire, et il était normal qu'il en soit ainsi. C'était là l'un des choix essentiels de Satoshi Nakamoto, car cet attrait spéculatif a permis en partie d'amorcer le processus de monétisation et de faire découvrir Bitcoin à des personnes qui s'en seraient sinon détournées.

Cependant, la culture de Bitcoin en a été profondément influencée dans le même temps. Il s'est ainsi créé une réelle tendance à l'avarice au sein de la communauté, qui s'est reflétée par des mèmes et des formules en tous genres. En particulier, il existe cette présupposition que le nombre, c'est-à-dire le prix en dollars, doit monter (*number go up*), qu'il doit être propulsé « jusqu'à la lune » (*to the moon*) en vertu du fait que la richesse du monde est infinie et qu'il n'y a que 21 millions de bitcoins ($\infty/21\mathrm{M}$). En conséquence, l'individu doit accumuler des satoshis (*stack sats*) et les thésauriser (« HODL ») dans le but de profiter d'une vie meilleure. Cet aspect se retrouve dans les représentations de Bitcoin et des bitcoineurs, comme le taureau du marché haussier ou bien les yeux laser (#LaserRayUntil100K).

Cette volonté d'obtenir un niveau de prix toujours plus haut repose sur la délusion de l'adoption de masse que nous avons évoquée ci-dessus. Pour que le prix atteigne les sommets, il faut en effet que tout le monde finisse par posséder du bitcoin d'une manière ou d'une autre. Comme la plupart des gens ne sont pas prêts à utiliser Bitcoin de manière souveraine, cette adoption a été réalisée au moyen de dépositaires. De ce fait, la culture basée sur le gain financier a conduit à l'affaiblissement subtil de Bitcoin par l'acceptation généralisée des intermédiaires financiers, par le consentement à l'identification de masse et par la promotion auprès des institutions et des États.

L'adoption de masse n'est pas un objectif réaliste ni à court, ni à moyen terme. Lorsque nous vantons les avantages de Bitcoin, nous ne nous adressons pas à la masse proprement dite ; nous nous adressons au reste, aux quelques-uns qui comprennent les tenants et aboutissants des problèmes qu'il permet de résoudre et qui sont susceptibles d'être intéressés. C'est pourquoi il est essentiel de ne pas aseptiser le discours : pour ne pas perdre ces personnes, il faut dire la vérité ; et si cette vérité peut être voilée, elle ne doit jamais être déformée.

Bitcoin vit de la tension qui existe entre l'économie officielle, qui approuve le pouvoir sur la monnaie, et la contre-économie, qui s'y oppose. Du fait de cette tension, la culture cryptomonétaire est également constamment attaquée, notamment par les médias de masse, par les banquiers centraux et par les représentants de l'État. Il existe ainsi un nombre stupéfiant de détracteurs qui, travaillant pour l'adversaire, répètent à l'envi leur argumentaire de mauvaise foi. S'il est utile de se confronter à eux pour rétablir la vérité devant un public qui doute, il est vain de croire qu'ils disparaîtront ou perdront en visibilité. C'est pourquoi Bitcoin a besoin d'une tradition, d'une transmission culturelle d'individu à individu, qui permettrait d'expliquer ses principes de manière saine et organique au nouveau venu.

En particulier, le message de Bitcoin devrait toujours être un appel à la pratique, conformément aux mouvements idéologiques qui l'ont précédé, à commencer par les cypherpunks. Chacun devrait se sentir poussé à écrire (et à lire) du code, à déployer des fermes de minage dans la mesure du possible, à participer à l'économie circulaire, à conserver du bitcoin et à éduquer les autres sur le sujet, quand bien même cela n'apporterait pas un gain financier direct. Car c'est aussi de cette manière que Bitcoin prospère.

Quoi qu'il en soit, Bitcoin ne peut pas être oublié. La découverte de Satoshi Nakamoto est là pour rester. Elle a déjà joué un rôle dans le combat pour la liberté humaine et devra probablement jouer un rôle encore plus grand à l'avenir. Son succès dépendra de l'action des personnes qui la soutiennent. La révolution ne sera pas centralisée.

Notes

La rédaction initiale de cet ouvrage s'est terminée le 30 novembre 2023. Les traductions des textes en anglais sont celles de l'auteur, hormis quand le titre français est précisé en note. Les dates et heures sont données selon le fuseau UTC, sauf indication contraire. Des notes supplémentaires peuvent être retrouvées à l'adresse `https://viresinnumeris.fr/bitcoinelegancenotes-v1-3-0.pdf`. Cette édition (v1.3.0, janvier 2025) contient de multiples corrections, de nouvelles notes et des améliorations de traduction.

Chapitre 1 – Les débuts de Bitcoin

1. Certains partent du principe que Satoshi Nakamoto serait un pseudonyme utilisé par un groupe d'individus. Néanmoins, nous supposerons ici qu'il n'y avait qu'une seule personne derrière les messages et le code attribués au créateur de Bitcoin, sans pour autant nier que cette personne a pu se faire aider.

2. Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, 09/11/2008 01:58:48 UTC : `https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html`.

3. Satoshi a également réservé le nom de domaine Netcoin.org au même moment, ce qui laisse à penser qu'il n'a pas encore finalisé son choix concernant le nom de son modèle. – Or Weinberger sur Twitter, 23/09/2022 08:54 UTC : `https://twitter.com/orweinberger/status/1573234325046558720`.

4. Gwern Branwen, *Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails*, 17 mars 2014 : `https://gwern.net/doc/bitcoin/2008-nakamoto`.

5. Les archives de la liste de diffusion de Metzdowd sont disponibles publiquement à l'adresse `https://www.metzdowd.com/pipermail/cryptography/`. Les cypherpunks présents en 2008 étaient, entre autres : John Gilmore, Hal Finney, James A. Donald, Robert Hettinga, Zooko Wilcox-O'Hearn et Len Sassaman.

6. Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, 31/10/2008 18:10:00 UTC : `https://www.metz`

dowd.com/pipermail/cryptography/2008-October/014810.html.

7. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

8. « Nous avons vraiment, vraiment besoin d'un tel système, mais d'après ce que je comprends de votre proposition, il ne semble pas pouvoir s'adapter à la taille requise. » – James A. Donald, *Re: Bitcoin P2P e-cash paper*, 02/11/2008, 23:46:23 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014814.html.

9. « Les méchants contrôlent couramment des fermes de machines zombies de 100 000 unités ou plus. Les personnes que je connais qui gèrent une liste noire de machines zombies émetteuses de spam me disent qu'elles voient souvent un million de nouvelles machines zombies par jour. C'est la même raison pour laquelle hashcash ne peut pas fonctionner sur l'Internet d'aujourd'hui : les gentils ont une puissance de calcul nettement inférieure à celle des méchants. » – John Levine, *Re: Bitcoin P2P e-cash paper*, 03/11/2008 13:32:39 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014817.html.

10. « Je pense que le vrai problème avec ce système est le marché des bitcoins. Les preuves de travail informatiques n'ont pas de valeur intrinsèque. » – Ray Dillinger, *Re: Bitcoin P2P e-cash paper*, 06/11/2008 05:14:37 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014822.html.

11. Hal Finney, *Re: Bitcoin P2P e-cash paper*, 07/11/2008 23:40:12 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html.

12. Hal Finney, *Bitcoin and me*, 19/03/2013 20:40:02 UTC : https://bitcointalk.org/index.php?topic=155054.msg1643833#msg1643833.

13. Satoshi a écrit à James A. Donald : « Je t'ai envoyé les fichiers principaux. (disponibles sur demande pour le moment, publication complète bientôt) » – Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 17/11/2008 17:24:43 : https://www.metzdowd.com/pipermail/cryptography/2008-November/014863.html.

14. Hal Finney sur Twitter, 11/01/2009 3:33 UTC : https://twitter.com/halfin/status/1110302988.

15. Cette première transaction entre Satoshi et Hal avait pour identifiant f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 et a été confirmée dans le bloc 170 le 12 janvier à 3:30.

16. L'identifiant de la transaction reçue par Dustin (en P2IP) était d71fd2f64c0b34465b7518d240c00e83f6a5b10138a7079d1252858fe7e6b577.

17. Satoshi Nakamoto, *Bitcoin v0.1 released*, 08/01/2009 19:27:40 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.

18. Hal Finney, *Re: Bitcoin v0.1 released*, 11/01/2009 02:22:01 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html.

19. Satoshi Nakamoto, *Bitcoin v0.1 released*, 16/01/2009 16:03:14 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html.

20. Satoshi Nakamoto, *Bitcoin open source implementation of P2P currency*, 11 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

21. Satoshi Nakamoto, *Re: Bitcoin open source implementation of P2P currency*, 18 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:9562.

22. Mike Hearn, *Questions about BitCoin*, 11/04/2009 22:46 UTC : https://plan99.net/~mike/satoshi-emails/thread1.html.

23. Martti Malmi (Trickster), *P2P Currency could make the government extinct?*, 09/04/2009 17:49:47 UTC, archive : https://web.archive.org/web/20150927195115/https://board.freedomainradio.com/topic/17233-p2p-currency-could-make-the-government-extinct/.

24. Cité par Satoshi Nakamoto, *Re: Bitcoin*, 02/05/2009 17:06:58 UTC : https://mmalmi.github.io/satoshi/#email-1. (Note de janvier 2025.)

25. Archive de la page web de Bitcoin : https://web.archive.org/web/20090511173000/http://bitcoin.sourceforge.net/.

26. « J'ai trouvé la première transaction connue de bitcoins en USD dans mes sauvegardes de courriel. J'ai vendu 5 050 BTC pour 5,02 $ le 12-10-2009. » – Martti Malmi sur Twitter, 15/01/2014 : https://twitter.com/marttimalmi/status/423455561703624704. L'identifiant de la transaction était 7dff938918f07619abd38e4510890396b1cef4fbeca154fb7aafba8843295ea2.

27. NewLibertyStandard, *Re: New Exchange Service: "BTC 2 PSC"*, 19/01/2010 08:06:15 UTC : https://bitcointalk.org/index.php?topic=15.msg111#msg111.

28. Satoshi Nakamoto, *New icon/logo*, 24/02/2010 21:24:23 UTC : https://bitcointalk.org/index.php?topic=64.msg504#msg504.

29. Satoshi Nakamoto, *Re: Ummmm... where did my bitcoins go?*, 18/05/2010 20:06:46 UTC : https://bitcointalk.org/index.php?topic=125.msg1149#msg1149.

30. Satoshi Nakamoto, *Re: A few suggestions*, 12/12/2009 17:52:44 UTC : https://bitcointalk.org/index.php?topic=12.msg54#msg54

31. Satoshi Nakamoto, mai 2010, propos rapportés par Nathaniel Popper : https://www.reddit.com/r/Bitcoin/comments/36vnmr/heres_what_satoshi_wrote_to_the_man_responsible/.

32. Laszlo Hanyecz, *Pizza for bitcoins?*, 18/05/2010 00:35:20 UTC : https://bitcointalk.org/index.php?topic=137.msg1141#msg1141.

33. L'identifiant de la transaction de la pizza entre Laszlo Hanyecz et Jeremy Sturdivant était a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d.

34. Gavin Andresen, *Get 5 free bitcoins from freebitcoins.appspot.com*, 11/06/2010, 17:38:45 UTC : https://bitcointalk.org/index.php?topic=183.msg1488#msg1488.

35. Satoshi Nakamoto, *Re: Get 5 free bitcoins from freebitcoins.appspot.com*, 18/06/2010, 23:08:34 UTC : https://bitcointalk.org/index.php?topic=183.msg1620#msg1620.

36. James A. Donald, *Re: [bitcoin-list] New User*, 30/06/2010 22:29:16, archive : https://web.archive.org/web/20131016002646/http://sourceforge.net/p/bitcoin/mailman/bi

tcoin-list/?viewmonth=201006. – Dans un autre courriel, James A. Donald ajoutait : « Je ne voulais pas paraître si négatif. Si nous y arrivons, c'est une grande victoire pour la liberté – mais c'est un long périple, et je suis occupé par un autre projet. ».

37. Teppy, « *Bitcoin Releases Version 0.3* », *Slashdot*, 11 juillet 2010 : https://news.slashdot.org/story/10/07/11/1747245/Bitcoin-Releases-Version-03.

38. Gwern Branwen, *2014 Jed McCaleb MtGox interview*, 16 février 2014 : https://www.gwern.net/docs/bitcoin/2014-mccaleb.

39. Jed McCaleb, *Re: New Bitcoin Exchange*, 18/07/2010 02:53:07 UTC : https://bitcointalk.org/index.php?topic=444.msg3891#msg3891.

40. Le 13 août 2010, la ferme de minage d'ArtForz était constituée de 6 cartes graphiques ATI Radeon HD 5770 ; à la fin, elle se composait de 24 ATI Radeon HD 5970. – Tim Swanson, *How ArtForz changed the history of Bitcoin mining*, 20 avril 2014 : https://www.ofnumbers.com/2014/04/20/how-artforz-changed-the-history-of-bitcoin-mining/.

41. Jeff Garzik, *Strange block 74638*, 15/08/2010, 18:08:49 UTC : https://bitcointalk.org/index.php?topic=822.msg9474#msg9474

42. Satoshi Nakamoto, *Development of alert system*, 22/08/2010 23:55:06 UTC : https://bitcointalk.org/index.php?topic=898.msg10722#msg10722. – Après avoir servi entre 2012 et 2015, ce système d'alerte a été progressivement désactivé pour finir par être définitivement supprimé du logiciel en 2017 (https://bitcoin.org/en/alert/2016-11-01-alert-retirement).

43. Marek Palatinus (slush), *Cooperative mining*, 27/11/2010, 13:45:41 UTC : https://bitcointalk.org/index.php?topic=1976.msg24844#msg24844.

44. « Nous ne voulons pas mettre l'aspect "anonyme" au premier plan. (J'avais l'intention de modifier la page d'accueil) "Les développeurs s'attendent à ce que cela se traduise par une monnaie stable par rapport à l'énergie et hors de portée de tout État." – Je ne fais certainement pas ce genre de provocation ou d'affirmation. » – Satoshi Nakamoto, *Re: Slashdot Submission for 1.0*, 05/07/2010 21:31:14 UTC : https://bitcointalk.org/index.php?topic=234.msg1976#msg1976.

45. L'histoire de Bradley Manning (devenu Chelsea Manning après une transition de genre) est narrée par Andy Greenberg dans son ouvrage *This Machine Kills Secrets* publié en 2012.

46. Amir Taaki, *Wikileaks contact info?*, 10/11/2010 12:49:16 UTC : https://bitcointalk.org/index.php?topic=1735.msg21271#msg21271.

47. ShadowOfHarbringer, *Re: Wikileaks contact info?*, 10/11/2010 13:28:00 UTC : https://bitcointalk.org/index.php?topic=1735.msg21283#msg21283.

48. Wladimir van der Laan (wumpus), *Re: Wikileaks contact info?*, 04/12/2010 08:57:41 UTC : https://bitcointalk.org/index.php?topic=1735.msg26737#msg26737.

49. Satoshi Nakamoto, *Re: Wikileaks contact info?*, 05/12/2010 09:08:08 UTC, https://bitcointalk.org/index.php?topic=1735.msg26999#msg26999.

50. Satoshi Nakamoto, *Re: PC World Article on Bitcoin*, 11/12/2010 23:39:16 UTC, https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280.

51. Le contrôle du site a été cédé à un individu utilisant le pseudonyme Cøbra tandis que la charge du forum a été donnée à Michael Marquardt (Theymos). Les deux personnes cogèrent ces deux plateformes.

52. Gavin Andresen, *Development process straw-man*, 19/12/2010 16:41:39 UTC : https://bitcointalk.org/index.php?topic=2367.msg31651#msg31651.

53. Satoshi Nakamoto, *Re: Holding coins in an unspendable state for a rolling time window*, 23/04/2011 13:40 UTC : https://plan99.net/~mike/satoshi-emails/thread5.html.

54. Allie Jones, « *Former Coworker Regrets Helping Reveal Identity of Bitcoin's Founder* », *The Wire*, 6 mars 2014, archive : https://web.archive.org/web/20140309041730/http://www.thewire.com/technology/2014/03/bitcoin-founders-coworker-regrets-doxxing-him/358878.

55. « WikiLeaks accepte désormais les dons anonymes en bitcoins sur 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v » – WikiLeaks sur Twitter, 14/06/2011 23:12 UTC : https://twitter.com/wikileaks/status/80774521350668288.

56. Ce montant a été retrouvé grâce au Patoshi Pattern, mis en lumière par Sergio Lerner en 2013 dans un article intitulé *The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius* (https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/). L'estimation utilisée ici est celle de Whale Alert publiée en 2020 : https://whale-alert.medium.com/the-satoshi-fortune-e49cf73f9a9b.

57. Un message provenant du compte de Satoshi sur le forum de la Fondation P2P a été publié le 7 mars 2014 pour nier son association à Dorian Nakamoto (https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:52186), et un courriel d'opposition à Bitcoin XT a été envoyé le 15 août 2015 à la liste de diffusion de développement depuis son adresse satoshi@vistomail.com (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-August/010238.html).

58. Parmi les candidats pour être la figure de Satoshi Nakamoto, ceux qui reviennent le plus souvent sont : Nick Szabo, Hal Finney, Adam Back, Len Sassaman.

59. Hal Finney, *Re: Another *Potential* Identifying Piece of Evidence on Satoshi*, 15/06/2013 01:23:42 UTC : https://bitcointalk.org/index.php?topic=234330.msg2479328#msg2479328.

60. Leah McGrath Goodman, « *The Face Behind Bitcoin* », *Newsweek Magazine*, 6 mars 2014 : https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html.

61. Andy Greenberg, « *Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius* », *Forbes*, 25 mars 2014 : https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/.

62. Hal Finney, *Re: Parity Party*, 11/01/2011 21:17:04 UTC : https://bitcointalk.org/index.php?topic=2734.msg37307#msg37307.

63. La première mention publique de Silk Road par Ross Ulbricht remonte au 27 janvier 2011 sur le forum de *The Shroomery*, un site consacré aux champignons hallucinogènes, où il prétendait être tombé par hasard sur la place de marché. – Ross Ulbricht (altoid), *anonymous market online?*,

27/01/2011 22:28 UTC : https://www.shroomery.org/forums/showflat.php/Number/13860995.

Ross Ulbricht a réitéré cette manœuvre sur le *Bitcoin Forum*, où il a écrit le 29 janvier : « Quelqu'un a-t-il déjà visité Silk Road ? C'est un peu comme un amazon.com anonyme. Je ne pense pas qu'il y ait de l'héroïne, mais d'autres choses y sont vendues. Le site utilise essentiellement bitcoin et tor pour négocier des transactions anonymes. » – Ross Ulbricht (altoid), *Re: A Heroin Store*, 29/01/2011 19:44:51 UTC, https://bitcointalk.org/index.php?topic=175.msg42670#msg42670.

64. WeUseCoins, *What is Bitcoin?* (vidéo), 22 mars 2011 : https://www.youtube.com/watch?v=Um63OQz3bjo.

65. Adrian Chen, « *The Underground Website Where You Can Buy Any Drug Imaginable* », *Gawker*, 1er juin 2011 : https://www.gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160; archive : https://www.gawkerarchives.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

66. L'identifiant de la transaction de preuve de solvabilité de Mt. Gox en 2011 était 3a1b9e330d32fef1ee42f8e86420d2be978bbe0dc5862f17da9027cf9e11f8c4.

67. La chaîne Youtube de Bruce Wagner se trouve à l'adresse https://www.youtube.com/@vlogwrap. Les vidéos des présentations à la conférence peuvent y être retrouvées.

68. Jeff Garzik, *[Bitcoin-development] Preparing 0.3.23-rc1 release*, 12/06/2011 02:23:58 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-June/000000.html.

69. Le système des BIP a été initialement proposé le 19 septembre 2011 par Amir Taaki sous le nom de *Bitcoin Enhancement Proposals*, en référence directe aux *Python Enhancement Proposals* (PEP) dont il s'est inspiré. (Amir Taaki, *[Bitcoin-development] Bitcoin Enhancement Proposals (BEPS)*, 19/09/2011 00:31:55 UTC, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-September/000554.html)

70. Pete Rizzo, Aaron van Wirdum, « *The Battle For P2SH: The Untold Story Of The First Bitcoin War* », *Bitcoin Magazine*, 4 décembre 2020 : https://bitcoinmagazine.com/technical/the-battle-for-p2sh-the-untold-story-of-the-first-bitcoin-war.

71. Amir Taaki, *The Truth behind BIP 16 and 17 (important read)*, 29/01/2012 03:54:08 UTC : https://bitcointalk.org/index.php?topic=61705.msg719790#msg719790.

72. Erik Voorhees, *SatoshiDICE.com - The World's Most Popular Bitcoin Game*, 24/04/2012 02:17:31 UTC, archive : https://bitcointalk.org/index.php?topic=77870.msg865877#msg865877.

73. Matt Corallo, *Huge increase in satoshidice spam over the past day*, 13/06/2012 23:21:47 UTC : https://bitcointalk.org/index.php?topic=87444.msg961132#msg961132.

Chapitre 2 – Une croissance conflictuelle

1. Colleen Taylor, « *With $1.5M Led By Winklevoss Capital, BitInstant Aims To Be The Go-To Site To Buy And Sell Bitcoins* », *TechCrunch*, 17 mai 2013 : https://techcrunch.com/2013/05

/17/with-1-5m-led-by-winklevoss-capital-bitinstant-aims-to-be-the-go-to-site-to-buy-and-sell-bitcoins/.

2. Capture du site web Coinbase.com, 20 septembre 2012 : https://web.archive.org/web/20120920091115/https://coinbase.com/.

3. *The Good Wife*, 3x13 : « Bitcoin for Dummies », 15 janvier 2012.

4. Cette animosité à l'égard de Silk Road s'est retrouvée dans les propos tenus par Tyler Winklevoss quelques semaines après la chute de la plateforme : « Les prix sont le double de ce qu'ils étaient avant la fermeture de Silk Road. La demande d'utilisation de bitcoins pour des activités illicites était donc clairement quasi nulle. » – Matthew J. Belvedere, « *Bitcoin is nearly halfway to the $400 billion value predicted by the Winklevoss twins four years ago* », *CNBC*, 12 novembre 2013 : https://www.cnbc.com/2013/11/12/the-winklevoss-brothers-bitcoin-worth-100-times-more.html.

5. Bitcoin Foundation, *Developing a More Open Economy*, archive de 2013 : https://web.archive.org/web/20130702232207/https://bitcoinfoundation.org/about/.

6. Matt Whitlock, *[CHART] Bitcoin Inflation vs. Time*, 13/12/2012 15:08:08 UTC : https://bitcointalk.org/index.php?topic=130619.msg1397456#msg1397456.

7. À cette occasion, GoldMoney et Bitcoin Magazine ont coproduit un documentaire, intitulé *Cyprus: A Wake Up Call*, qui recueillait les témoignages des chypriotes touchés par cette crise. Voir sur Youtube : https://www.youtube.com/watch?v=mGGlYnxSFWM.

8. Deux agents corrompus du FBI ont notamment profité de l'enquête pour subtiliser plus de 20 000 bitcoins (soit environ 350 000 $) et pour simuler un assassinat. – Ludovic Lars, « *Meurtres, escroqueries et vol de bitcoins - Le côté obscur de Silk Road* », *Le Journal du Coin*, 27 juin 2021 : https://journalducoin.com/analyses/cote-obscur-silk-road/.

9. 29 656,52080180 BTC ont été envoyés à l'adresse 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX entre le 2 et le 16 octobre, tandis que 144 336,39429472 BTC ont été transférés vers l'adresse 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH le 25 octobre. – U.S. Attorney's Office, Southern District of New York, *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*, 25 octobre 2013 : https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-seizure-additional-28-million-worth-bitcoins-belonging.

10. Lors du procès, la juge Katherine Forrest a affirmé : « Je rends ce jugement en ayant à l'esprit les crimes que vous avez commis et la nécessité de vous infliger la peine la plus sévère possible. Il ne doit faire aucun doute que le non-respect de la loi ne sera pas toléré. Il ne doit faire aucun doute que personne n'est au-dessus de la loi, quels que soient son éducation ou ses privilèges. » – *Ross Ulbricht's sentencing transcript*, 4 février 2015 : https://freeross.org/wp-content/uploads/2018/02/Doc_36_Jan_12_Vol_VI_Appendix_A1314-A1554.pdf#page=240.

11. Kim Nilsson, *The missing MtGox bitcoins*, 19 avril 2015 : https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html

12. Le 18 mai, la page d'accueil de Bitcoin.org présentait Bitcoin comme un système de monnaie numérique permettant de réaliser des « transactions instantanées de pair à pair [...] dans le monde entier » moyennant des « frais de traitement faibles ou nuls », en précisant que « la gestion des transactions et l'émission des bitcoins sont effectuées collectivement par le réseau ».

– Archive de Bitcoin.org : https://web.archive.org/web/20130518024528/http://bitcoin.org/en/.

13. Le 4 octobre 2010, Satoshi décrivait sur le forum comment mettre en œuvre une augmentation de la taille limite des blocs. – Satoshi Nakamoto, *Re: [PATCH] increase block size limit*, 04/10/2010 19:48:40 UTC, https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366).

14. Bitcoin Core, *Bitcoin Core version 0.9.0 released*, 19 mars 2014 : https://bitcoin.org/en/release/v0.9.0#rebranding-to-bitcoin-core.

15. Keep Bitcoin Free, *Why the blocksize limit keeps Bitcoin free and decentralized* (vidéo), 17 mai 2013 : https://www.youtube.com/watch?v=cZp7UGgBR0I.

16. Nicolas Houy, *The economics of Bitcoin transaction fees*, GATE, 2014. – Cette idée, appelée la « spirale fatale des frais », avait été proposée dès 2011 par un utilisateur sur Bitcointalk. Voir Vandroiy, *[If tx limit is removed] Disturbingly low future difficulty equilibrium*, 22 avril 2011 : https://bitcointalk.org/index.php?topic=6284.msg92187#msg92187.

17. Blockstream, *Why We Founded Blockstream*, 22 octobre 2014, archive : https://web.archive.org/web/20161022162335/https://www.blockstream.com/2014/10/23/why-we-are-co-founders-of-blockstream.html.

18. Joseph Poon et Thaddeus Dryja, *The Bitcoin Lightning Network DRAFT Version 0.5*, 28 février 2015 : https://lightning.network/lightning-network-paper-DRAFT-0.5.pdf.

19. La malléabilité des transactions est la possibilité de modifier légèrement une transaction après sa diffusion sur le réseau, de façon à changer son identifiant. Cette capacité disparaît cependant une fois que la transaction a été confirmée par un mineur qui l'a incluse dans un bloc de la chaîne.

20. Gavin Andresen, *A Scalability Roadmap*, 6 octobre 2014, archive : https://web.archive.org/web/20150321091124/http://blog.bitcoinfoundation.org:80/a-scalability-roadmap.

21. Mike Hearn, *Why is Bitcoin forking?*, 15 août 2015 : https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1.

22. *FAQ – BitcoinXT* (archive) : https://web.archive.org/web/20150908031806/https://bitcoinxt.software/faq.html#who-is-involved.

23. Michael Marquardt (Theymos), *It's time for a break: About the recent mess & temporary new rules*, 17/08/2015 00:50:15 : https://www.reddit.com/r/Bitcoin/comments/3h9cq4/its_time_for_a_break_about_the_recent_mess/.

24. Le terme anglais est issu de l'ouvrage *The Blocksize War* de Jonathan Bier publié en 2021. Le terme français a été inventé par Morgan Phuc en 2017 : https://bitconseil.fr/bitcoin-guerre-blocs/.

25. Alex Hern, « *Bitcoin's forked: chief scientist launches alternative proposal for the currency* », *The Guardian*, 17 août 2015 : https://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist.

26. Gregory Maxwell, *[bitcoin-dev] Capacity increases for the Bitcoin system*, 07/12/2015 22:02:17 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-Decem

ber/011865.html.

27. Mike Hearn, *The resolution of the Bitcoin experiment*, 14 janvier 2016 : https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7.

28. « Bitcoin Classic a émergé des cendres du débat entre XT et Core. Il s'agit d'une version de Bitcoin qui autoriserait une limite de deux mégaoctets, mettant en place des règles pour l'augmenter au cours du temps. Elle semble gagner rapidement du soutien. » – Paul Vigna, « *Is Bitcoin Breaking Up?* », *The Wall Street Journal*, 17 janvier 2016, archive : https://web.archive.org/web/20160117220315/https://www.wsj.com/articles/is-bitcoin-breaking-up-1453044493.

29. Bitcoin Roundtable, *Bitcoin Roundtable Consensus*, 20 février 2016 : https://medium.com/@bitcoinroundtable/bitcoin-roundtable-consensus-266d475a61ff.

30. Craig Wright, *Jean-Paul Sartre, Signing and Significance*, 2 mai 2016, archive : https://web.archive.org/web/20160502072011/http://www.drcraigwright.net/jean-paul-sartre-signing-significance/.

31. BBC News, *Mr Bitcoin: "I don't want money, I don't want fame!"* (vidéo), 2 mai 2016 : https://www.youtube.com/watch?v=5DCAC1j2HTY.

32. La signature fournie par Craig Wright correspond à la clé publique liée à l'adresse 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S qui a servi à recevoir la récompense du bloc 9 et à envoyer le premier paiement à Hal Finney le 12 janvier 2009, et a donc été produite par Satoshi Nakamoto. Néanmoins, un utilisateur de Reddit (JoukeH) a découvert très rapidement qu'il s'agissait de la signature d'une transaction présente sur la chaîne : https://www.reddit.com/r/Bitcoin/comments/4hf4xj/creator_of_bitcoin_reveals_identity/d2pf70v/.

33. Gavin Andresen, *Satoshi*, 2 mai 2016 : http://gavinandresen.ninja/satoshi

34. SegWit annulait notamment les effets de l'AsicBoost secret, une technique d'optimisation du minage. Voir Gregory Maxwell, *[bitcoin-dev] BIP proposal: Inhibiting a covert attack on the Bitcoin POW function*, 05/04/2017 21:37:45 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-April/013996.html.

35. Roger Ver est connu pour son prosélytisme de l'adoption du bitcoin dans le commerce et pour sa participation éclatante au documentaire *The Bitcoin Gospel* diffusé le 1er novembre 2015 sur Youtube. Voir https://www.youtube.com/watch?v=8zKuoqZLyKg&t=2831s.

36. Shaolin Fry, *[bitcoin-dev] Flag day activation of segwit*, 12/03/2017 15:50:27 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-March/013714.html.

37. « Nous nous opposons au New York Agreement et au hard fork Bitcoin SegWit2X de novembre », Change.org, 15 octobre 2017 : https://www.change.org/p/mineurs-et-entreprises-de-l-Ã¯co-systÃ¨me-bitcoin-nous-nous-opposons-au-new-york-agreement-et-au-hard-fork-bitcoin-segwit2x-de-novembre.

38. Mike Belshe, *[Bitcoin-segwit2x] Segwit2x Final Steps*, 08/11/2017 16:58:41 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html.

39. Satoshi Nakamoto, *Re: BitDNS and Generalizing Bitcoin*, 09/12/2010 21:02:42 UTC : https:

//bitcointalk.org/index.php?topic=1790.msg28696#msg28696.

40. Charlie Lee (coblee), *Re: [ANN] Litecoin - a lite version of Bitcoin. Be ready when is launches!*, 09/10/2011 06:14:28 UTC : https://bitcointalk.org/index.php?topic=47417.msg564414#msg564414.

41. Sunny King, *[ANN] [PPC] PPCoin Released! - First Long-Term Energy-Efficient Crypto-Currency*, 19/08/2012 19:54:28 UTC : https://bitcointalk.org/index.php?topic=101820.msg1113938#msg1113938 ; Sunny King, Scott Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, 19 août 2012, archive : https://web.archive.org/web/20121021014644/http://www.ppcoin.org/static/ppcoin-paper.pdf.

42. Gavin Andresen, *The macro-economics of alt-coins*, 19 août 2013 : https://gavintech.blogspot.com/2013/08/the-macro-economics-of-alt-coins.html.

43. Daniel Krawisz, *The Problem with Altcoins*, 22 août 2013 : https://nakamotoinstitute.org/mempool/the-problem-with-altcoins/.

44. Vitalik Buterin, « *In Defense of Alternative Cryptocurrencies* », *Bitcoin Magazine*, 7 septembre 2013 : https://bitcoinmagazine.com/business/defense-alternative-cryptocurrencies.

45. L'adresse BTC utilisée par EthSuisse était 36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2. – Vitalik Buterin, *Launching the Ether Sale*, 22 juillet 2014 : https://blog.ethereum.org/2014/07/22/launching-the-ether-sale.

46. Blockstream, *Why We Founded Blockstream*, 22 octobre 2014, archive : https://web.archive.org/web/20161022162335/https://www.blockstream.com/2014/10/23/why-we-are-co-founders-of-blockstream.html.

47. L'expression utilisée par Vitalik Buterin était « *bitcoin dominance maximalist* », qu'on peut traduire par « maximaliste de la dominance du bitcoin » (https://www.reddit.com/r/Bitcoin/comments/2is4us/whats_wrong_with_counterparty/cl54c0y/). Dans son article publié le 19 novembre 2014, il définissait le maximalisme du bitcoin comme « l'idée qu'un milieu composé de multiples cryptomonnaies concurrentes est indésirable, qu'il est mal de lancer "encore une autre monnaie", et qu'il est à la fois juste et inévitable que la monnaie bitcoin en vienne à acquérir une position de monopole sur le marché cryptomonétaire ». – Vitalik Buterin, *On Bitcoin Maximalism, and Currency and Platform Network Effects*, 19 novembre 2014 : https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects/.

48. L'appartenance au maximalisme est parfois revendiquée aujourd'hui par des gens qui n'embrassent pas son caractère extrémiste (même s'il se trouve dans le terme). C'est pourquoi on peut recourir au pléonasme « maximalisme toxique » pour désigner cette tendance. Jameson Lopp parle aussi de « puritanisme du bitcoin ». Voir Jameson Lopp, *History of Bitcoin Maximalism*, 25 mars 2023 : https://blog.lopp.net/history-of-bitcoin-maximalism/.

49. Kim Zetter, « *FBI Fears Bitcoin's Popularity with Criminals* », *Wired*, 9 mai 2012 : http://www.wired.com/2012/05/fbi-fears-bitcoin/.

50. Tracfin, *Rapport d'activité 2011*, juillet 2012 : https://www.economie.gouv.fr/files/files/directions_services/tracfin/Publications/rapports_activite/2011_rapport_FR.pdf

51. Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, 18 mars 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

52. Code général des impôts, *Article 150 VH bis*, 24 mai 2019.

53. Edward Robinson, Matthew Leising, « *Blythe Masters Tells Banks the Blockchain Changes Everything* », *Bloomberg*, 1er septembre 2015 : https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything.

54. Aux États-Unis, c'est le *Coronavirus Aid, Relief, and Economic Security Act* (« CARES Act »), signé en mars 2020, qui a amené cette dépense supplémentaire. Il s'agissait d'un programme du Département du Trésor, mais on peut supposer qu'il a été financé essentiellement par les « emprunts » réalisés auprès de la Réserve Fédérale. Du côté de la Banque Centrale Européenne, l'injection de liquidités a été mise en place par le programme d'achats d'urgence face à la pandémie (PEPP), qui prévoyait 750 milliards d'euros en mars 2020, auxquels s'ajoutent 600 milliards en juin, puis 500 milliards supplémentaires en décembre.

55. Une illustration plus récente de cette intégration institutionnelle est l'approbation des fonds négociés en bourse (ETF) indexés sur le bitcoin aux États-Unis le 10 janvier 2024. (Note de janvier 2025.)

Chapitre 3 – Des racines monétaires

1. Le concept de cessibilité a été décrit en 1892 par l'économiste autrichien Carl Menger dans son essai *On the Origin of Money*. Le terme en allemand est *Absatzfähigkeit*, qui désigne, pour une marchandise, la capacité à s'écouler facilement, à bien se vendre. Il a été traduit en anglais par *saleability* et *marketability*. Il peut aussi être traduit par vendabilité ou échangeabilité en français.

2. L'économiste Fritz Machlup parlait de « degrés de monétarité » à propos des créances en dollar dans le système bancaire européen (Fritz Machlup, « *Euro-dollar creation: a mystery story* », in *Banca Nazionale del Lavoro Quarterly Review*, vol. 23, no. 94, 1970, p. 225). De même, Hayek écrivait dans *Pour une vraie concurrence des monnaies* en 1976 (p. 93) : « Ceci signifie aussi que, bien que nous supposions habituellement qu'il existe une distinction claire entre ce qui est une monnaie et ce qui n'en est pas – et la législation s'efforce généralement de poser une telle démarcation –, cette dichotomie n'existe pas dès lors qu'on considère les propriétés qui confèrent à un bien la qualité de monnaie. Ce que nous observons est bien davantage un continuum dans lequel des biens dotés de différents degrés de liquidité, ou dont les valeurs fluctuent indépendamment les unes des autres, se confondent partiellement par le degré auquel ils peuvent être utilisés en tant que monnaie. »

3. L'effet Lindy est le fait que l'espérance de vie future d'une chose non périssable, telle qu'une technique ou une idée, est proportionnelle à son âge actuel.

4. C'est le sens qu'on porte au mot *commodity* en anglais.

5. Le mot salaire vient du latin *salarium*, qui désignait la « ration de sel », puis la « solde pour acheter du sel » versés aux soldats romains dans l'Antiquité : https://www.lexilogos.com/latin/gaffiot.php?q=salarium.

6. D'un point de vue légal, la monnaie électronique désigne un type spécifique de monnaie scripturale. L'article L315-1 du *Code monétaire et financier* la définit comme « une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur ». C'est pourquoi nous préférons ici employer le terme de monnaie numérique.

7. Carl Menger, *Principles of Economics*, Ludwig von Mises Institute, 2007, pp. 120–121 : https://cdn.mises.org/principles_of_economics.pdf.

8. Le chartalisme (du latin *charta*, « papier », « lettre ») est une théorie de la monnaie qui a été développée par l'économiste allemand Georg Friedrich Knapp en 1905 dans son ouvrage *Staatliche Theorie des Geldes*. La théorie monétaire moderne (*Modern Monetary Theory*) forme un néochartalisme.

9. Carl Menger, *Principles of Economics*, Ludwig von Mises Institute, 2007, pp. 261–262.

10. Nick Szabo, *Shelling Out: The Origins of Money*, 2002 ; George Selgin, *The Myth of the Myth of Barter*, 2016 : https://www.alt-m.org/2016/03/15/myth-myth-barter/.

11. Bitcoin and Bible Group, *Thank God for Bitcoin: The Creation, Corruption and Redemption of Money*, Whispering Candle, 2020.

12. Ludwig von Mises, *The Theory of Money and Credit*, Yale University Press, 1953, p. 414 : https://cdn.mises.org/Theory%20of%20Money%20and%20Credit.pdf.

13. Friedrich Hayek, *Pour une vraie concurrence des monnaies*, Presses Universitaires de France, 2015.

14. « Il n'y a [...] personne pour agir en tant que banque centrale ou réserve fédérale afin d'ajuster l'offre monétaire au fur et à mesure que le nombre d'utilisateurs augmente. [...] En ce sens, c'est un système qui se comporte davantage comme un métal précieux. » – Satoshi Nakamoto, *Re: Bitcoin open source implementation of P2P currency*, 18 février 2009, https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:9562.

15. Ludwig von Mises, *The Theory of Money and Credit*, Yale University Press, 1953, pp. 120–121.

16. Ludwig von Mises, *The Theory of Money and Credit*, Yale University Press, 1953, p. 110. Voir aussi Ludwig von Mises, *Human Action*, Ludwig von Mises Institute, 1998, p. 405 : https://cdn.mises.org/Human%20Action_3.pdf.

17. Ludwig von Mises, *The Theory of Money and Credit*, Yale University Press, 1953, p. 110.

18. Satoshi Nakamoto, *Re: Bitcoin does NOT violate Mises' Regression Theorem*, 27/08/2010 17:32:07 UTC : https://bitcointalk.org/index.php?topic=583.msg11405#msg11405.

19. Satoshi Nakamoto, *Re: Bitcoin does NOT violate Mises' Regression Theorem*, 27/08/2010 17:32:07 UTC : https://bitcointalk.org/index.php?topic=583.msg11405#msg11405.

20. Hal Finney, *Re: Bitcoin v0.1 released*, 11/01/2009 01:22:01 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html.

21. Satoshi Nakamoto, *Re: Current Bitcoin economic model is unsustainable*, 21/02/2010 05:44:24 UTC : https://bitcointalk.org/index.php?topic=57.msg415#msg415. – Il a réitéré cette objection en juillet 2010 : « [La monnaie] n'est pas stable par rapport à l'énergie. Ce sujet a fait l'objet d'une discussion. Elle n'est pas liée au coût de l'énergie. L'estimation de NLS basée sur l'énergie était un bon point de départ, mais les forces du marché domineront de plus en plus. » (Satoshi Nakamoto, *Re: Slashdot Submission for 1.0*, 05/07/2010 21:31:14 UTC : https://bitcointalk.org/index.php?topic=234.msg1976#msg1976)

22. Konrad S. Graf, *Bitcoins, the regression theorem, and that curious but unthreatening empirical world*, 27 février 2013 : https://www.konradsgraf.com/blog1/2013/2/27/in-depth-bitcoins-the-regression-theorem-and-that-curious-bu.html.

23. Ross Ulbricht, *Bitcoin Equals Freedom*, 25 septembre 2019 : https://rossulbricht.medium.com/bitcoin-equals-freedom-6c33986b4852.

24. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 14/11/2008 18:55:35 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014853.html.

25. Hal Finney, *Re: Bitcoin v0.1 released*, 11/01/2009 01:22:01 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html.

26. Satoshi Nakamoto, *Bitcoin v0.1 released*, 16/01/2009 16:03:14 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html.

27. Satoshi Nakamoto, *Re: Bitcoin open source implementation of P2P currency*, 18 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:9562.

28. Hal Finney, *Re: Bitcoin P2P e-cash paper*, 13/11/2008 15:24:18 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014848.html.

29. « J'ai vu le message [de Hal] et c'est l'une des raisons pour lesquelles j'ai démarré un nœud si rapidement. Mes systèmes ne font pas grand chose d'autre lorsqu'ils sont inactifs, alors pourquoi ne pas créer des BitCoins ? Et s'ils valent quelque chose un jour... ? Bonus ! » – Dustin Trammell, *Re: Bitcoin v0.1 released*, 16/01/2009 01:14:27 UTC.

30. Capture du site web de NewLibertyStandard, décembre 2009 : https://web.archive.org/web/20091229132559/http://newlibertystandard.wetpaint.com/.

31. qbg, *Comment: Bitcoin and the Regression Theorem of Money*, 8 décembre 2012 : https://voluntaryistreader.wordpress.com/2012/12/07/bitcoin-and-the-regression-theorem-of-money/#comment-135.

32. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 06/11/2008 20:15:40 UTC, https://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html.

33. WikiLeaks, *Banking Blockade*, 24/10/2011 13:00 UTC, https://wikileaks.org/Banking-Blockade.html.

34. Jamie Crawley, « *Edward Snowden says use crypto, don't invest in it: 'Bitcoin is what I used to pay for the servers pseudonymously'* », *Fortune*, 11 juin 2022 :https://fortune.com/2022/06/11/edward-snowden-says-use-crypto-dont-invest-in-it-bitcoin-is-what-i-used-to-pay-for-the-servers-pseudonymously/.

35. L'adresse principale d'Alexeï Navalny était 3QzYvaRFY6bakFBW4YBRrzmwzTnfZcaA6E.

36. Alexeï Navalny est mort en prison en février 2024. (Note de janvier 2025.)

37. La page de donation se situe à l'adresse https://sci-hub.se/donate. L'ancienne adresse 1K4t2vSBSS2xFjZ6PofYnbgZewjeqbG1TM (d'après une capture antérieure du site : https://web.archive.org/web/20160202212649/http://sci-hub.la/) a reçu 94,42594975 BTC entre le 03/07/2015 et le 14/11/2020. Les autres adresses liées à Sci-Hub sont 12PCbUDS4ho7vgSccmixKTHmq9qL2mdSns et bc1q7eqheemcu6xpgr42vl0ayel6wj087nxdfjfndf.

38. Le travail domestique (cuisine, ménage, linge, éducation des enfants, etc.) était auparavant principalement assuré par les femmes, avant qu'elles n'abandonnent le foyer et que ce travail ne devienne un travail taxé comme un autre. La société promue par l'État moderne est avant tout une société mercantile, où tout se vend et où tout peut être taxé de la naissance à la mort de l'individu.

39. Joël Drogland, « La France du marché noir », *La Cliothèque*, 2 mai 2008 : https://clio-cr.clionautes.org/la-france-du-marche-noir-1940-1949.html.

40. Le nom est tiré de l'article « *The Second Economy of the USSR* » écrit par Gregory Grossman en 1977.

41. Le terme « *agorism* » a été forgé par Konkin pour sa présentation au *Free Enterprise Forum* de février 1974.

42. Le libertarianisme se base sur l'axiome de non-agression formulé par l'économiste autrichien Murray Rothbard dans *For a New Liberty: The Libertarian Manifesto* en 1973 : « Aucun individu ni groupe d'individus n'a le droit d'agresser quelqu'un en portant atteinte à sa personne ou à sa propriété [...], "agression" étant défini comme le fait de prendre l'initiative d'utiliser la violence physique (ou de menacer de l'utiliser) à l'encontre d'une autre personne ou de sa propriété. »

43. Le terme contre-économie est calqué sur le mot contre-culture, faisant référence à la culture alternative des années 60, à laquelle Konkin avait participé.

44. Samuel Edward Konkin III, *New Libertarian Manifesto*, KoPubCo, 2006.

45. Martti Malmi (Trickster), *P2P Currency could make the government extinct?*, 9 avril 2009, archive : https://web.archive.org/web/20150927195115/https://board.freedomainradio.com/topic/17233-p2p-currency-could-make-the-government-extinct/.

46. Dread Pirate Roberts, *chat*, 20 mars 2012 : https://antilop.cc/sr/users/dpr/threads/20120320-1103-chat.html.

47. Adrian Chen, « *The Underground Website Where You Can Buy Any Drug Imaginable* », *Gawker*, 1er juin 2011 : https://www.gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

48. « Ce sont les médias en ligne agoristes qui m'ont fait découvrir Bitcoin. L'agorisme ne nécessite peut-être pas d'ordinateurs, mais la technique est l'arme la plus puissante que la liberté ait à sa disposition. » – Vitalik Buterin, *Re: Bitcoin on AgoristRadio.com*, 21/05/2011 18:36:45 UTC : https://bitcointalk.org/index.php?topic=9177.msg133853#msg133853.

49. Nugget's News, *Peter McCormack – Bitcoin, Addiction & Podcasts* (vidéo), 19 juillet 2019 : https://www.youtube.com/watch?v=3aDMnE6dnHk.

Chapitre 4 – La nécessité de décentralisation

1. Même si l'on considère que l'impôt constitue un « mal nécessaire », ou qu'il se justifie par l'« intérêt général » ou par la « démocratie », il n'en demeure pas moins, par nature, un transfert de richesse non consenti, c'est-à-dire un vol pour le dire crûment.

2. Comme l'écrivait Max Weber en 1919 : « L'État est l'institution qui possède, dans une collectivité donnée, le monopole de la violence légitime. » – Max Weber, *Le savant et le politique*, 10/18, 2002.

3. L'article 1747 du *Code général des impôts* dispose : « Quiconque, par voies de fait, menaces ou manœuvres concertées, aura organisé ou tenté d'organiser le refus collectif de l'impôt, sera puni des peines prévues à l'article 1er de la loi du 18 août 1936 réprimant les atteintes au crédit de la nation [c'est-à-dire de deux ans de prison et d'une amende de 9 000 euros].

   Sera puni d'une amende de 3 750 € et d'un emprisonnement de six mois quiconque aura incité le public à refuser ou à retarder le paiement de l'impôt. »

4. Voir Hans-Hermann Hoppe, « La préférence temporelle, l'État et le processus de décivilisation », in *Démocratie, le dieu qui a échoué*, 2020, Éditions Résurgence.

5. Le nom « seigneuriage » est issu de l'ancien français *seignorage*, qui désignait le privilège de battre monnaie au Moyen Âge, généralement réservé aux seigneurs féodaux.

6. Jörg Guido Hülsmann, *The Ethics of Money Production*, Ludwig von Mises Institute, 2008.

7. Par exemple, le cours légal de l'argent liquide est imposé en France par l'article R642-3 du code pénal : « Le fait de refuser de recevoir des pièces de monnaie ou des billets de banque ayant cours légal en France selon la valeur pour laquelle ils ont cours est puni de l'amende prévue pour les contraventions de la 2e classe. »

8. La loi de Gresham a été formalisée par l'économiste écossais Henry Dunning Macleod dans ses *Elements of Political Economy* publiés en 1858.

9. L'article 1er de la loi du 18 août 1836 réprimant les atteintes au crédit de la nation dispose : « Sera puni de deux ans de prison et d'une amende de 9 000 euros quiconque, par des voies ou des moyens quelconques, aura sciemment répandu dans le public des faits faux ou des allégations mensongères de nature à ébranler directement ou indirectement sa confiance dans la solidité de la monnaie, la valeur des fonds d'État de toute nature, des fonds des départements et des communes, des établissements publics et, d'une manière générale, de tous les organismes où les collectivités précédentes ont une participation directe ou indirecte. »

   Lors de la rédaction de cette loi en août 1936, le franc avait perdu 80 % de sa valeur en or à la suite de la Grande Guerre et allait en perdre encore 30 % suite à la dévaluation du 25 septembre suivant.

10. Cette définition nous vient de Guido Hülsmann pour qui l'inflation est « l'augmentation de la quantité nominale d'un intermédiaire d'échange au-delà de la quantité qui aurait été produite sur le marché libre ». – Jörg Guido Hülsmann, *The Ethics of Money Production*, p. 85.

11. Richard Cantillon, *Essai sur la Nature du Commerce en Général*, McMaster University Archive for the History of Economic Thought, 1755.

12. Le rôle de prêteur en dernier ressort de la banque centrale a été théorisé au cours du XIXe siècle. – Henry Thornton, *An Enquiry into the Nature and Effects of the Paper Credit of Great Britain*,

1802 ; Walter Bagehot, *Lombard Street: A Description of the Money Market*, 1873.

13. Les clients des banques commerciales sont encouragés à garder leurs fonds en banque en étant partiellement couverts contre le risque de faillite par un système de garantie des dépôts, géré par exemple par le Fonds de Garantie des Dépôts et de Résolution (FGDR) en France et par la *Federal Deposit Insurance Corporation* (FDIC) aux États-Unis.

14. Satoshi Nakamoto, *Bitcoin open source implementation of P2P currency*, 11 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

15. James Tobin, « *The Case for Preserving Regulatory Distinctions* », in *Proceedings - Economic Policy Symposium - Jackson Hole*, 1987, pp. 167–205 : https://www.kansascityfed.org/documents/3828/1987-S87TOBIN.pdf.

16. peculium, *Fedcoin: A centrally-issued alternative to peer-to-peer currencies*, 26 mars 2013, archive : https://web.archive.org/web/20130404231341/http://peculium.net/2013/03/26/fedcoin-a-centrally-issued-alternative-to-peer-to-peer-currencies/.

17. Jean-Luc (Bitcoin.fr), *Naissance de l'Eurocoin*, 1er avril 2014 : https://bitcoin.fr/naissance-de-l-eurocoin/.

18. John Paul Koning, *Fedcoin*, 19 octobre 2014 : https://jpkoning.blogspot.com/2014/10/fedcoin.html.

19. David Andolfatto, *Fedcoin: On the Desirability of a Government Cryptocurrency*, 3 février 2015 : https://andolfatto.blogspot.com/2015/02/fedcoin-on-desirability-of-government.html.

20. Ben Broadbent, *Central banks and digital currencies*, 2 mars 2016 : https://www.bankofengland.co.uk/speech/2016/central-banks-and-digital-currencies.

21. Digital Currency Initiative, *About the MIT Digital Currency Initiative* : https://dci.mit.edu/about.

22. James Lovejoy, Cory Fields, Madars Virza, Tyler Frederick, David Urness, Kevin Karwaski, Anders Brownworth, Neha Narula, *A High Performance Payment Processing System Designed for Central Bank Digital Currencies*, 3 février 2022 : https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx.

23. Fabio Panetta, *Demystifying wholesale central bank digital currency*, 26 septembre 2022 : https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220926~5f9b85685a.en.html.

24. Le point 5 du programme dressé dans le Manifeste du parti communiste prône la « centralisation du crédit entre les mains de l'État, au moyen d'une banque nationale, dont le capital appartiendra à l'État et qui jouira d'un monopole exclusif ». – Karl Marx, *Manifeste du parti communiste*, Ère Nouvelle, 1895.

25. Edward Snowden, *Your Money AND Your Life*, 9 octobre 2021 : https://edwardsnowden.substack.com/p/cbdcs.

26. William Rees-Mogg, James Dale Davidson, *The Sovereign Individual: Mastering the Transition to the Information Age*, Touchstone, 1999, p. 247.

27. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 8 février 1996 : https://www.eff.org/fr/cyberspace-independence.

28. Kevin Kelly, « *E-Money* », in *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*, Addison-Wesley, 1994 : https://kk.org/mt-files/outofcontrol/ch12-f.html.

29. Cette dynamique a été formalisée par Parker Lewis sous la forme d'un dilemme du prisonnier appliqué à la question de l'interdiction de Bitcoin. Voir Parker Lewis, *Bitcoin Cannot be Banned*, 11 août 2019 : https://unchained.com/blog/bitcoin-cannot-be-banned/.

30. Voir à ce sujet Hans-Hermann Hoppe, « *Banking, Nation States, and International Politics: A Sociological Reconstruction of the Present Economic Order* », in *The Review of Austrian Economics*, vol. 4, no. 3, 1990, pp. 55–87 : https://mises.org/library/banking-nation-states-and-international-politics-sociological-reconstruction-present.

31. Cette loi du 8 juin 1864 est devenue la section 486 du titre 18 du Code des États-Unis (intitulée *18 U.S. Code § 486 - Uttering coins of gold, silver or other metal*) qui dispose : « Quiconque, sauf dans le cas où cela est autorisé par la loi, fabrique, met en circulation ou fait passer, ou tente de mettre en circulation ou de faire passer, des pièces d'or ou d'argent ou d'autres métaux, ou des alliages de métaux, destinées à être utilisées comme monnaie courante, qu'elles ressemblent à des pièces des États-Unis ou de pays étrangers, ou qu'elles soient de conception originale, sera condamné à une amende en vertu du présent titre ou à une peine d'emprisonnement de cinq ans au maximum, ou aux deux. »

32. Wendy McElroy, « *Anthony L. Hargis And The Trusted Third Party Trap* », *Agorist Nexus*, 14 mai 2020 : https://www.agoristnexus.com/anthony-l-hargis-and-the-trusted-third-party-trap/.

33. Samuel Edward Konkin III, *Counter-Economics: From the Back Alleys... To the Stars*, KoPubCo, 2018.

34. P. Carl Mullan, *A History of Digital Currency in the United States*, Palgrave Macmillan, 2016.

35. United States Mint, *Liberty Dollars Not Legal Tender, United States Mint Warns Consumers*, 14 septembre 2006 : https://www.usmint.gov/news/press-releases/20060914-liberty-dollars-not-legal-tender-united-states-mint-warns-consumers.

36. Dustin Trammell, *The Problem With the Liberty Dollar*, 7 décembre 2008 : https://blog.dustintrammell.com/the-problem-with-the-liberty-dollar/.

37. « Il est intéressant de noter que l'un des systèmes d'e-gold a déjà une forme de spam appelé "dusting". Les spammeurs envoient une minuscule quantité de poussière d'or afin de placer un message de spam dans le champ de commentaire de la transaction. » – Satoshi Nakamoto, *Re: Bitcoin v0.1 released*, 25/01/2009 15:47:10 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015041.html.

38. Correspondance par courriel entre Ross Ulbricht et Arto Bendiken (GX-270), septembre 2009 : https://antilop.cc/sr/exhibits/253456462-Silk-Road-exhibits-GX-270.pdf

39. United States District Court for the Southern District of New York, *Liberty Reserve, et al. Indictment*, 28 mai 2013 : https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve%2C%20et%20al.%20Indictment%20-%20Re

dacted_0.pdf.

40. Lawrence H. White, « *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-Gold* », in *Cato Journal*, vol. 34, no. 2, 2014, pp. 281–301 : https://ciaotest.cc.columbia.edu/journals/cato/v34i2/f_0031473_25521.pdf.

41. En particulier, la vision originelle de PayPal, produit développé par Confinity Inc. au tout début, était révolutionnaire. Voici quel était le discours de son PDG Peter Thiel à l'automne 1999, rapporté par Eric Jackson en 2012 : « Ce que nous qualifions de "pratique" pour les utilisateurs américains sera révolutionnaire pour les pays en développement. Les États de nombre de ces pays jouent avec leur monnaie. Ils ont recours à l'inflation et parfois à des dévaluations monétaires massives, comme nous l'avons vu en Russie et dans plusieurs pays d'Asie du Sud-Est l'année dernière, pour priver leurs citoyens de leurs richesses. La plupart des gens ordinaires n'ont jamais l'occasion d'ouvrir un compte à l'étranger ou de mettre la main sur plus de quelques billets d'une monnaie stable comme le dollar américain. Un jour, PayPal sera en mesure de changer cette situation. À l'avenir, lorsque notre service sera disponible en dehors des États-Unis et que la pénétration d'Internet continuera à s'étendre à tous les niveaux économiques, PayPal permettra aux citoyens du monde entier d'exercer un contrôle plus direct sur leurs monnaies qu'ils ne l'ont jamais fait auparavant. Il sera pratiquement impossible pour les États corrompus de voler les richesses de leurs citoyens par leurs anciens moyens, car, dans le cas où ils essaient, les citoyens se tourneront vers le dollar, la livre ou le yen, abandonnant ainsi leur monnaie locale sans valeur pour quelque chose de plus sûr. » – Voir Eric M. Jackson, *The PayPal Wars: Battles With Ebay, the Media, the Mafia, and the Rest of Planet Earth*, World Ahead Pub., 2012.

Chapitre 5 – Un mouvement technologique

1. Whitfield Diffie et Martin Hellman, « *New Directions in Cryptography* », *IEEE Transactions on Information Theory*, vol. 22, no. 6, novembre 1976, pp. 644–654 : https://ee.stanford.edu/~hellman/publications/24.pdf.

2. Soit $G = (\mathbb{Z}_n^*, \cdot)$ un groupe cyclique fini et soit g un point générateur. Le problème du logarithme discret consiste, pour $x \in G$, à retrouver $k < n$ tel que $x = g^k$. On écrit alors $\log_g(x) = k$.

3. Les détails concernant l'utilisation de ces éléments cryptographiques (ECDSA, SHA-256, arbres de Merkle) dans Bitcoin seront discutés dans les chapitres 7 et 8.

4. David L. Chaum, « *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* », in *Communications of the ACM*, vol. 24, no. 2, 1981, pp. 84—90.

5. David L. Chaum, « *Blind signatures for untraceable payments* », in *Advances in Cryptology: Proceedings of CRYPTO '82*, 1982, pp. 199–203 : https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

6. David L. Chaum, « *Security without identification: transaction systems to make big brother obsolete* », in *Communications of the ACM*, vol. 28, no. 10, octobre 1985, pp. 1030—1044 : https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf.

7. David L. Chaum, *Testimony for US House of Representatives*, 25 juillet 1995, archive : https://web.archive.org/web/19970111170802/http://digicash.com/publish/testimony.html.

8. Martin Gardner, « *Mathematical Games: A new kind of cipher that would take millions of years to break* », in *Scientific American*, août 1977 : https://simson.net/ref/1977/Gardner_RSA.pdf.

9. L'algorithme de chiffrement symétrique dans la version 1 était BassOmatic, conçu par Zimmermann lui-même. Il a été remplacé par IDEA dans la version 2 et les versions supérieures. La version 3 ajoutait les algorithmes ElGamal et DSA pour la partie asymétrique, et l'algorithme CAST-128 pour le côté symétrique.

10. Philip R. Zimmermann, « *Why do you need PGP?* », in *PGP User's Guide*, 5 juin 1991 : https://www.tech-insider.org/free-software/research/acrobat/910605.pdf.

11. Stuart Haber, Wakefield Scott Stornetta, « *How to time-stamp a digital document* », in *Journal of Cryptology*, vol. 3, 1991, pp. 99–111 : http://www.staroceans.org/e-book/Haber_Stornetta.pdf.

12. Daniel Oberhaus, *The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995*, 27 août 2018 : https://www.vice.com/en/article/j5nzx4/what-was-the-first-blockchain.

13. Paul Baran, « *On Distributed Communications Networks* », in *IEEE Transactions on Communications Systems*, vol. 12, no. 1, mars 1964, pp. 1–9 : https://web.cs.ucla.edu/classes/cs217/Baran64.pdf.

14. L'ARPA (*Advanced Research Projects Agency*, « Agence pour les projets de recherche avancée ») a été créée en 1958. Elle a été rebaptisée DARPA (*Defense Advanced Research Projects Agency*, « Agence pour les projets de recherche avancée de défense ») en 1972. Elle est brièvement redevenue l'ARPA en 1993 avant d'adopter définitivement le nom de DARPA en 1996.

15. Vinton G. Cerf, Robert E. Kahn, « *A Protocol for Packet Network Intercommunication* », in *IEEE Transactions on Communications*, vol. 22, no. 5, mai 1974, pp. 637–648 : https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf.

16. « Le mois de septembre 1993 entrera dans l'histoire du net comme le mois de septembre qui n'a jamais pris fin. » – Dave Fischer, *Re: longest USENET thread ever*, 26/01/1994 01:58:52 UTC : https://groups.google.com/g/alt.folklore.computers/c/wF4CpYbWuuA/m/jS6ZOyJd10sJ.

17. Bram Cohen, *BitTorrent - a new P2P app*, 2 juillet 2001, archive : https://web.archive.org/web/20080129085545/http://finance.groups.yahoo.com/group/decentralization/message/3160.

18. David M. Goldschlag, Michael G. Reed, Paul F. Syverson, « *Hiding Routing Information* », in *Proceedings of the First International Workshop on Information Hiding*, mai 1996, pp. 137—150 : https://www.onion-router.net/Publications/IH-1996.pdf.

19. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 06/11/2008 20:15:40 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html.

20. N. Stephan Kinsella, « *Against Intellectual Property* », in *Journal of Libertarian Studies*, vol. 15, no. 2, 2001, pp. 1–53 : https://cdn.mises.org/Against%20Intellectual%20Property_2.pdf.

21. Thomas Jefferson, *Letter to Isaac McPherson*, 13 août 1813 : https://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html.

22. Richard M. Stallman, *The GNU Manifesto*, mars 1985 : https://www.gnu.org/gnu/manifesto.en.html.

23. Richard M. Stallman, *What is the Free Software Foundation?*, février 1986 : https://www.gnu.org/bulletins/bull1.txt.

24. En thermodynamique, l'entropie est une grandeur physique qui caractérise le degré de désorganisation d'un système physique. Le deuxième principe de la thermodynamique énonce que l'entropie d'un système isolé croît avec le temps, ce qui implique que l'entropie de l'univers croît à mesure de son vieillissement, et qu'il finira par mourir. L'extropie se rapproche ainsi de la néguentropie, la baisse locale d'entropie à certains endroits, sans être définie de façon aussi formelle.

25. Don Lavoie, Howard Baetjer, William Tulloh, « *High-Tech Hayekians: Some Possible Research Topics in the Economics of Computation* », in *Market Process*, vol. 8, 1990 : http://www.philsalin.com/hth/hth.html.

26. Ed Regis, *Meet the Extropians*, 1er octobre 1994 : https://www.wired.com/1994/10/extropians/.

27. Max More, « *The Extropian Principles* », in *Extropy*, vol. 6, 1er juillet 1990 : https://github.com/Extropians/Extropy/blob/master/ext6.pdf.

28. « Le progrès durable et la prise de décision intelligente et rationnelle requièrent des sources d'information et des points de vue diversifiés, rendus possibles par les ordres spontanés. La gestion centralisée limite l'exploration, la diversité, la liberté et les opinions divergentes. Respecter l'ordre spontané, c'est soutenir les institutions volontaristes qui maximisent l'autonomie, par opposition aux groupements hiérarchiques rigides et autoritaires, qui se caractérisent par leur structure bureaucratique, la suppression de l'innovation et de la diversité, et l'étouffement des incitations individuelles. Notre compréhension des ordres spontanés nous rend très méfiants à l'égard des "autorités" qui nous sont imposées, et sceptiques à l'égard des dirigeants politiques, de l'obéissance inconditionnelle et des traditions non remises en question. » – Max More, « *The Extropian Principles v. 2.0* », *Extropy*, vol. 9, 1992 : https://github.com/Extropians/Extropy/blob/master/ext9.pdf.

29. Hal Finney, *Protecting privacy with electronic cash*, *Extropy*, vol. 10, 1993 : https://github.com/Extropians/Extropy/blob/master/Extropy-10.pdf.

30. *Extropy*, vol. 15, 1995 : https://github.com/Extropians/Extropy/blob/master/ext15.pdf.

31. Le terme « cyberespace » (*cyberspace*) a été forgé par William Gibson dans sa nouvelle *Gravé sur Chrome* publiée en juillet 1982, pour désigner la représentation virtuelle des flux de données sur Internet. Le terme « matrice » (*matrix*) était utilisé en tant que synonyme.

32. Timothy C. May, *The Crypto Anarchist Manifesto*, 22/11/1992 20:11:24 UTC : https://cypherpunks.venona.com/date/1992/11/msg00204.html.

33. Certains détails de la formation des cypherpunks sont issus de l'ouvrage *Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age* (pp. 257–266) de Steven Levy

publié en 2001.

34. « Et si nous pouvions construire une société dans laquelle les informations ne seraient jamais collectées ? [...] C'est le genre de société que je veux construire. Je veux que soit garantie - par la physique et la mathématique, pas par des lois - la possibilité de bénéficier de choses telles qu'une véritable confidentialité des communications personnelles, [...] une véritable confidentialité des enregistrements personnels, [...] une véritable liberté de commerce, [...] une véritable confidentialité financière [et] un véritable contrôle de l'identification. » – John Gilmore, *Privacy, Technology, and the Open Society*, 28 mars 1991 : `http://www.toad.com/gnu/cfp.talk.txt` ; archive : `https://web.archive.org/web/19991003163945/http://www.toad.com/gnu/cfp.talk.txt`.

35. Judith Milhon, *secretions*, 25/09/1992 10:01:26 UTC : `https://cypherpunks.venona.com/date/1992/09/msg00013.html`.

36. « De plus, cela donne à tort l'impression que "cypherpunk" est synonyme d'"anarchiste". Il se trouve que je suis anarchiste, mais ce n'est pas ce en quoi croient la plupart des personnes associées au terme "cypherpunk", et il n'est pas juste de les dépeindre ainsi – bon sang, de nombreuses personnes sur cette liste de diffusion sont ouvertement hostiles à l'anarchisme. Je ne veux pas que les gens pensent qu'il faut détester l'idée même d'État pour aimer la cryptographie. » – Perry E. Metzger, *Re: PC Expo summary!!*, 01/07/1994 12:13:09 UTC : `https://cypherpunks.venona.com/date/1994/07/msg00014.html`.

37. Hal Finney, *Why remailers...*, 16/11/1992 01:30:02 UTC : `https://cypherpunks.venona.com/date/1992/11/msg00108.html`.

38. Eric Hughes, *RANTS: A Cypherpunk's Manifesto*, 17/03/1993 19:51:06 UTC : `https://cypherpunks.venona.com/date/1993/03/msg00392.html`.

39. Steven Levy, « *Crypto Rebels* », *Wired*, 1er février 1993 : `https://www.wired.com/1993/02/crypto-rebels/`. – Par la suite, le mouvement a également été présenté dans les revues *Whole Earth Review* et *The Village Voice*.

40. *Comprehensive Counter-Terrorism Act of 1991*, 24 janvier 1991 : `https://www.congress.gov/bill/102nd-congress/senate-bill/266/text`.

41. The White House, *White House Annoucement of the Clipper Initiative*, 16 avril 1993 : `https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/clipper-announcement.html`.

42. Cette victoire contre la puce Clipper n'a pas empêché les agences étasuniennes d'espionner leur propre population de manière massive, comme l'ont montré les révélations d'Edward Snowden en 2013. – Voir Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, 6 juin 2013 : `https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order`.

43. Timothy C. May, *no subject (file transmission)*, 17 août 1993, `https://cypherpunks.venona.com/date/1993/08/msg00538.html`.

44. Damien Cave, *The Mojo solution*, 9 octobre 2000 : `https://www.salon.com/2000/10/09/mojo_nation/`.

Chapitre 6 – La cybermonnaie avant Nakamoto

1. Robert A. Hettinga, *Digital Bearer Settlement*, avril 1998 : http://www.systemics.com/legal/digigold/discovery/postings/Geoecon.pdf.

2. Le terme « *credit card* » a été utilisé en 1888 par Edward Bellamy, écrivain et journaliste socialiste américain et précurseur du mouvement technocratique, dans son roman de fiction spéculative *Looking Backward*, pour désigner la carte de paiement des citoyens de sa supposée utopie. Ce type de carte s'est ensuite développé dans les années 1920–1930 aux États-Unis sous la forme de cartes délivrées indépendamment par Western Union, par les grands magasins, par les compagnies pétrolières et compagnies aériennes.

3. Sur les origines du réseau Visa, voir David L. Stearns, *Electronic Value Exchange: Origins of the VISA Electronic Payment System*, Springer, 2011. Le titre du livre est une référence au projet ambitieux de Dee Hock (le fondateur de Visa) de créer un protocole d'échange de valeur électronique (EVE) permettant d'effectuer l'intégralité des transactions sous forme électronique, ce qui donnerait lieu à « la genèse d'une nouvelle forme de monnaie mondiale ».

4. Sur l'histoire des débuts du service PayPal, voir Eric M. Jackson, *The PayPal Wars: Battles With Ebay, the Media, the Mafia, and the Rest of Planet Earth*, World Ahead Pub., 2012.

5. Hadon Nash, *Digital gold*, 24/08/1993 20:23:30 UTC : https://cypherpunks.venona.com/date/1993/08/msg00698.html.

6. David L. Chaum, « *Security without identification: transaction systems to make big brother obsolete* », in *Communications of the ACM*, vol. 28, no. 10, octobre 1985, pp. 1030—1044 : https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf.

7. David L. Chaum, Christian Grothoff, Thomas Moser, *How to Issue a Central Bank Digital Currency*, mars 2021 : https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf.

8. « Magic Money est un système d'argent liquide numérique conçu pour être utilisé par courrier électronique. Le système est en ligne et intraçable. En ligne signifie que chaque transaction implique un échange avec un serveur, pour éviter les doubles dépenses. Intraçable signifie qu'il est impossible pour quiconque de retracer les transactions, de faire correspondre un retrait avec un dépôt, ou de faire correspondre deux pièces de quelque manière que ce soit. » – Pr0duct Cypher, *Magic Money Digicash System*, 04/02/1994 20:44:27 UTC : https://cypherpunks.venona.com/date/1994/02/msg00247.html.

9. Timothy C. May, *Why Digital Cash is Not Being Used*, 03/05/1994 19:48:18 UTC : https://cypherpunks.venona.com/date/1994/05/msg00155.html.

10. Jim Crawley, « Electronic Cash », *The Computists' Weekly*, vol. 5, no. 25, 11 juillet 1995 : https://www.nzdl.org/cgi-bin/library?e=d-00000-00---off-0tcc--00-0----0-10-0---0---0direct-10---4-------0-1l--11-ro-50---20-preferences---10-0-1-00-0--4----0-0-11-10-0utfZz-8-00&a=d&cl=CL2.5&d=HASH0199d48acda6ba6861de2d9e.2.

11. « Mark Twain est arrivée sur le marché avec de l'argent liquide numérique *réel*, et les gens ont complètement cessé d'échanger les certificats bêta. Je ne me souviens même pas du dernier prix de règlement, mais il s'agissait de quelques centimes de dollars. » – Robert Hettinga, *e$: Interbank*

Digital Cash Clearing, Better Living through Walletware, Microintermediation, Net.Currencies and ECM, 3 juin 1996, archive : https://web.archive.org/web/19980204144728/http://www.shipwright.com/rants/rant_14.html.

12. Antoine Champagne, « *L'argent liquide numérique (crypto-curency) est né en 1995 : souvenirs* », *Reflets.info*, 11 janvier 2014 : https://reflets.info/articles/l-argent-liquide-numerique-crypto-curency-est-ne-en-1995-souvenirs.

13. « *Hoe DigiCash alles verknalde* », *Next! Magazine*, 1er janvier 1999, archive : https://web.archive.org/web/19990427142412/https://www.nextmagazine.nl/ecash.htm. Une traduction (en anglais) est disponible à l'adresse https://cryptome.org/jya/digicrash.htm.

14. Milton Friedman, *Milton Friedman Full Interview on Anti-Trust and Tech* (vidéo), 1999 : https://www.youtube.com/watch?v=mlwxdyLnMXM, 14:32.

15. libtech-l@netcom.com – Timothy C. May, *Re: Regional Lists*, 28/06/1994 05:48:50 UTC : https://cypherpunks.venona.com/date/1994/06/msg01156.html ; Timothy C. May, *Cyphernomicon*, 2.4.27.

16. Nick Szabo, *Smart Contracts*, 1994, archive : https://web.archive.org/web/20011102030833/http://szabo.best.vwh.net:80/smart.contracts.html.

17. On peut retrouver les écrits de Nick Szabo sur son ancienne page personnelle szabo.best.vwh.net et sur son blog Unenumerated débuté en 2005. – Archive de la page personnelle : https://web.archive.org/web/20160709091851/http://szabo.best.vwh.net/ ; Unenumerated : https://unenumerated.blogspot.com/.

18. Nick Szabo, *Trusted Third Parties are Security Holes*, 2001, archive : https://web.archive.org/web/20020423191203/http://szabo.best.vwh.net/ttps.html.

19. « Lorsque j'ai découvert les travaux de Chaum, j'ai été époustouflé. Le premier article que j'ai trouvé, je crois, était son article dans CACM, qui donnait un aperçu des nombreuses possibilités offertes. J'ai commencé à essayer de retrouver d'autres articles de Chaum. On y trouvait toutes les techniques nécessaires pour faire fonctionner le monde de Vinge, des techniques que Vinge connaissait apparemment déjà, bien avant moi. » – Hal Finney, *Why remailers...*, 16/11/1992 01:30:02 UTC : https://cypherpunks.venona.com/date/1992/11/msg00108.html.

20. Wei Dai, *b-money*, 26/11/1998 23:33:49 UTC, archive : https://web.archive.org/web/19990219124653/http://www.eskimo.com/~weidai/bmoney.txt.

21. Pour une explication technique de la preuve de travail, se référer à la section dédiée dans le chapitre 8.

22. Adam Back, *Re: Bypassing the Digicash Patents*, 30/04/1997 09:09:37 UTC : https://cypherpunks.venona.com/date/1997/04/msg00822.html.

23. Morgen E. Peck, « *Bitcoin: The Cryptoanarchists' Answer to Cash* », *IEEE Spectrum*, 30 mai 2012 : https://spectrum.ieee.org/bitcoin-the-cryptoanarchists-answer-to-cash.

24. Wei Dai, *PipeNet 1.1 and b-money*, 26/11/1998 23:33:49 UTC : https://cypherpunks.venona.com/date/1998/11/msg00941.html.

25. Ce fonctionnement pour garantir la stabilité de la b-money ne manque pas de rappeler le stablecoin géré par Maker DAO sur Ethereum, appelé précisément le dai ! Plus tard, Wei Dai a reproché à Satoshi Nakamoto la politique monétaire fixe de Bitcoin, qui devait entraîner selon lui « une forte volatilité du prix qui impose un coût élevé pour ses utilisateurs ». – Wei Dai, *Re: Bitcoins are not digital greenbacks*, 20/04/2013 07:56 UTC : https://www.lesswrong.com/posts/P9jggxRZTMJcjnaPw/bitcoins-are-not-digital-greenbacks?commentId=3XvTroRzb23NpHQDc.

26. Satoshi avait pensé lui-même au problème de l'oracle. Il écrivait ainsi en février 2009 : « Il n'y a en effet personne pour agir en tant que banque centrale ou réserve fédérale afin d'ajuster l'offre monétaire au fur et à mesure que le nombre d'utilisateurs augmente. Il aurait fallu qu'un tiers de confiance se charge de déterminer la valeur, car je ne sais pas comment un logiciel pourrait connaître la valeur des choses dans le monde réel. S'il existait un moyen astucieux de le faire, ou si nous voulions faire confiance à quelqu'un pour gérer activement l'offre monétaire afin de l'ancrer à quelque chose, les règles auraient pu être programmées à cet effet. » – Satoshi Nakamoto, *Re: Bitcoin open source implementation of P2P currency*, 18 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:9562.

27. Wei Dai, *Re: AALWA: Ask any LessWronger anything*, 15/03/2014 20:34 UTC : https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything?commentId=XKwphuwm366RegQ3d.

28. Nick Szabo, *Bit Gold: Towards Trust-Independent Digital Money*, 2005, archive : https://web.archive.org/web/20140406003811/http://szabo.best.vwh.net/bitgold.html.

29. Nick Szabo, *Bit gold*, 29 décembre 2005 : https://unenumerated.blogspot.com/2005/12/bit-gold.html.

30. Le calcul de la preuve de travail dans bit gold ne passait pas par l'inversion partielle d'une fonction de hachage (Hashcash) mais par une *secure benchmark function* qui mesurait la difficulté du problème à résoudre sur une machine précise. Cela devait permettre d'approximer le niveau d'énergie utilisé. – Voir Nick Szabo, *Intrapolynomial Cryptography*, 1999, archive : https://web.archive.org/web/20011217091748/http://szabo.best.vwh.net/intrapoly.html.

31. « [Bit gold] bénéficierait grandement d'une démonstration, d'un marché expérimental (avec par ex. un tiers de confiance pour se substituer à la sécurité complexe nécessaire au système réel). Quelqu'un veut m'aider à en programmer une ? » – Nick Szabo, *Re: Bit gold markets*, 10 avril 2008, archive : https://web.archive.org/web/20171227190431/http://unenumerated.blogspot.com/2008/04/bit-gold-markets.html?showComment=1207799580000#c3741843833998921269.

32. Voir Hal Finney, *RPOW Theory*, 15 août 2004, archive : https://web.archive.org/web/20040815154951/http://rpow.net/theory.html.

33. Hal Finney, *RPOW Security*, 15 août 2004, archive : https://web.archive.org/web/20040815154806/http://rpow.net/security.html.

34. Hal Finney, *Reusable Proofs of Work*, 1er février 2005, archive : https://web.archive.org/web/20050204193327/http://rpow.net/slides/slide001.html.

35. Ryan Fugger, *Money as IOUs in Social Trust Networks & A Proposal for a Decentralized Currency Network Protocol*, version 2, 18 avril 2004, archive : https://web.archive.org/web/20060221162102/http://ripple.sourceforge.net/decentralizedcurrency.pdf.

36. fiatjaf, *Ripple and the problem of the decentralized commit*, 17/10/2020 13:56 UTC : https://fiatjaf.com/3cb7c325.html.

37. Ce problème a été résolu d'une certaine manière par le réseau Lightning qui possède la même structure que Ripple, à l'exception que l'unité échangée n'est pas du crédit à proprement parler. – Voir fiatjaf, *The Lightning Network solves the problem of the decentralized commit*, 19/10/2020 19:09 UTC : https://fiatjaf.com/e3624832.html.

38. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

39. Satoshi Nakamoto, *[p2p-research] Re: Bitcoin open source implementation of P2P currency*, 12/02/2009 19:01:24 UTC : https://diyhpl.us/~bryan/irc/bitcoin-satoshi/p2presearch-again/p2pfoundation.net/backups/p2p_research-archives/2009-February.txt.gz.

40. Satoshi Nakamoto, *Re: Bitcoin v0.1 released*, 13/01/2009 07:55:20 UTC, archive : http://web.archive.org/web/20131204164149/http://www.dustintrammell.com/files/Satoshi_Nakamoto.zip. – Il a fait une remarque similaire sur le forum de la Fondation P2P. Voir Satoshi Nakamoto, *Re: Bitcoin open source implementation of P2P currency*, 15 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:9493.

41. Gwern Branwen, *Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails*, 17 mars 2014 : https://gwern.net/doc/bitcoin/2008-nakamoto.

42. Hal Finney, *Bitcoin P2P e-cash paper*, 07/11/2008 23:40:12 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html.

43. Satoshi Nakamoto, *Re: They want to delete the Wikipedia article*, 20/07/2010 18:38:28 UTC : https://bitcointalk.org/index.php?topic=342.msg4508#msg4508.

44. Satoshi Nakamoto a en réalité fait mention de RPOW à Martti Malmi dans un courriel privé qui a été rendu public en février 2024. Voir Satoshi Nakamoto, *Re: Bitcoin*, 21/07/2009 03:14:43 UTC : https://mmalmi.github.io/satoshi/#email-24. (Note de janvier 2025.)

45. « Je m'intéressais depuis longtemps aux systèmes de paiement cryptographiques. De plus, j'avais eu la chance de rencontrer et de correspondre longuement avec Wei Dai et Nick Szabo, qui sont généralement reconnus pour avoir créé des idées qui allaient se concrétiser avec Bitcoin. J'avais tenté de créer ma propre monnaie basée sur la preuve de travail, appelée RPOW. J'ai donc trouvé Bitcoin fascinant. » – Hal Finney, *Bitcoin and me*, 19/03/2013 20:40:02 UTC : https://bitcointalk.org/index.php?topic=155054.msg1643833#msg1643833.

46. Satoshi Nakamoto, *[p2p-research] Re: Bitcoin open source implementation of P2P currency*, 13/02/2009 02:31:20 : https://diyhpl.us/~bryan/irc/bitcoin-satoshi/p2presearch-again/p2pfoundation.net/backups/p2p_research-archives/2009-February.txt.gz.

47. Satoshi Nakamoto, *Re: Questions about BitCoin*, 12/04/2009 20:44 UTC : https://plan99.net/~mike/satoshi-emails/thread1.html.

48. Ryan Fugger, *Re: Is the cryptocurrency Bitcoin a good idea?*, 17/05/2011 07:44:33 UTC : `https://www.quora.com/Is-the-cryptocurrency-Bitcoin-a-good-idea/answer/Ryan-Fugger`.

49. Zooko Wilcox-O'Hearn, *Decentralized Money*, 26 janvier 2009, archive : `https://web.archive.org/web/20090303195936/http://testgrid.allmydata.org:3567/uri/URI:DIR2-RO:j74uhg25nwdpjpacl6rkat2yhm:kav7ijeft5h7r7rxdp5bgtlt3viv32yabqajkrdykozia5544jqa/wiki.html#%5B%5BDecentralized%20Money%5D%5D`.

Chapitre 7 – La valeur de l'information

1. Le mot « codage » est également largement utilisé en français.

2. Le terme satoshi a été initialement proposé par ribuck sur le forum de Bitcoin, d'abord en novembre 2010 pour désigner 0,01 bitcoin, puis en février 2011 pour nommer la plus petite unité. L'appellation a ensuite été adoptée par la communauté. – ribuck, *Re: How did "satoshi" become the name of the base unit?*, 09/01/2014 20:49:00 UTC : `https://bitcointalk.org/index.php?topic=407442.msg4415850#msg4415850`.

3. Le nom secp256k1 est un peu barbare, mais chaque lettre à une importance. Le sigle SEC désigne *Standards for Efficient Cryptography*, l'ouvrage dont elle est issue (`https://www.secg.org/SEC2-Ver-1.0.pdf`). Le P-256 indique que le nombre premier p utilisé est encodé sur 256 bits. Le k indique qu'il s'agit d'une courbe de Koblitz : les paramètres sont choisis pour rendre les opérations plus efficaces, et n'ont donc pas été sélectionnés aléatoirement (r). Le 1 désigne l'index de la courbe par rapport aux autres courbes similaires.

4. Le nombre premier choisi pour secp256k1 est : $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

5. L'addition est définie par $P + Q = R$ où $x_R = \lambda_{P,Q}^2 - x_P - x_Q \pmod p$ et $y_R = \lambda_{P,Q}\,(x_P - x_R) - y_P \pmod p$ avec $\lambda_{P,Q} = \{\frac{3x_P^2}{2y_P} \pmod p$ si $P = Q\,;\, \frac{y_Q - y_P}{x_Q - x_P} \pmod p$ sinon$\}$.

6. Le point de base de secp256k1 est :

   $G =$ (`0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798`,
   `0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8`) .

   Il a pour ordre le nombre premier

   $n =$ `0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141` ,

   de sorte que $n\,G = 0$.

7. Dans le corps fini $\mathbb{F}_p$, prendre l'opposé d'un élément non nul y inverse sa polarité. En effet, si $y \in [\![1, p-1]\!]$, alors $-y + p \in [\![1, p-1]\!]$.

8. L'algorithme de signature ECDSA est le suivant. En notant $H(m)$ l'empreinte cryptographique du message à signer, la signature est obtenue en appliquant les étapes suivantes :
   - Choisir aléatoirement une clé éphémère l inférieure à $n - 1$;
   - Calculer les coordonnées (i, j) du point $l\,G$;
   - Calculer $r = i \mod n$; si $r = 0$, choisir un autre l ;
   - Calculer $s = l^{-1}(H(m) + kr) \mod n$; si $s = 0$, choisir un autre l ;
   - La signature est (r, s).

L'algorithme de vérification est le suivant :
— Vérifier que $K \neq 0$ et que K appartient à la courbe ;
— Vérifier que $n\ K = 0$;
— Vérifier que $1 \leq r \leq n-1$ et $1 \leq s \leq n-1$;
— Calculer $(i, j) = (H(m)s^{-1} \mod n)\, G + (rs^{-1} \mod n)\, K$;
— Vérifier que $r = i \mod n$.

9. Il s'agit de la signature de la transaction d'identifiant `08e5ce0783ab6d5534e234136df02e0e240f76108eb6af04b8b624646b66f5eb`. Sous forme sérialisée (DER), cette signature est `3044022019b83a5e354ef62e98413e6ef3f37ad0c69f75cea7daa6a352cf66f4668a9a0b02204c13f9b6f2c8ea7af224b3f6a3d9cfdfe5085bbafa150fb1aa72a20ce7cac6b001`.

10. Il s'agit de suppositions et certaines fonctions satisfont ces caractéristiques plus que d'autres. Ainsi, des collisions ont été trouvées au sein des fonctions MD5 et SHA-1 alors qu'on les croyait sûres.

11. « Les adresses Bitcoin sont le seul endroit où le hachage de 160 bits est utilisé. » – Satoshi Nakamoto, *Re: Stealing Coins*, 25/07/2010 20:48:01 UTC : `https://bitcointalk.org/index.php?topic=571.msg5754#msg5754`.

12. On peut observer l'adresse `1EHNa6Q4Jz2uvNExL497mE43ikXhwF6kZm` (correspondant à la clé 1) pour se convaincre qu'il ne s'agit pas d'un bon choix.

13. BitMEX Research, *Call me Ishmael*, 13 octobre 2020 : `https://blog.bitmex.com/call-me-ishmael/`.

14. Bitcoin.org, *Android Security Vulnerability*, 11 août 2013 : `https://bitcoin.org/en/alert/2013-08-11-android`.

15. Supposons qu'une population mondiale de 10 milliards d'êtres humains utilise Bitcoin activement de sorte que chaque individu génère 1 million d'adresses en moyenne. La probabilité d'une collision serait alors de :

$$10^{16} \,/\, 2^{160} \simeq 0.00000000000000000000000000000684\ \% \,.$$

Même si un individu tentait de construire une machine spécialisée générant et vérifiant un trillion (10^{18}) d'adresses par seconde et fonctionnant en continu, la probabilité d'accéder à une adresse déjà utilisée serait toujours négligeable (de l'ordre de 10^{-21}). Nos cerveaux ne sont pas faits pour nous représenter de tels nombres.

16. On utilise aussi parfois la lettre `h` (pour *hardened*).

17. Tous les portefeuilles ne respectent néanmoins pas ce standard. Le BRD wallet (ex Bread Wallet) utilise ainsi le chemin `m/0'` pour dériver le compte principal, conformément aux recommandations initiales du BIP-32.

18. Clément Wardzala, « *Bitcoin : la police allemande à la recherche d'un mot de passe à 65 millions de dollars* », *Cryptoast*, 5 février 2021 : `https://cryptoast.fr/bitcoin-police-allemande-recherche-mot-de-passe-65m/`.

19. Andreas Antonopoulos, *Bitcoin Q&A: How Do I Secure My Bitcoin?* (vidéo), 7 juillet 2017 : `https://www.youtube.com/watch?v=vt-zXEsJ61U`.

20. Paul Grewal, *Using Crypto Tech to Promote Sanctions Compliance*, 7 mars 2022 : `https:`

//blog.coinbase.com/using-crypto-tech-to-promote-sanctions-compliance-8a17b1dabd68.

21. Department of Justice, *Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox*, 26 juillet 2017 :https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

22. Patrick Thompson, « *Crypto exchanges delisting, denying access and stealing BSV* », *CoinGeek* 17 janvier 2020 : https://coingeek.com/crypto-exchanges-delisting-denying-access-and-stealing-bsv/.

23. Satoshi Nakamoto, *Re: Dying bitcoins*, 21/06/2010, 17:48:26 UTC : https://bitcointalk.org/index.php?topic=198.msg1647#msg1647.

24. James Howells a miné entre le 15 février (bloc 4 334) et le 24 avril 2009 (bloc 12 098). Il a accumulé son revenu de minage à l'adresse 198aMn6ZYAczwrE5NvNTUMyJ5qkfy4g3Hi. En date du 26 avril 2009, cette adresse contenait exactement 8 000 bitcoins.

25. Alex Hern, « *Missing: hard drive containing Bitcoins worth £4m in Newport landfill site* », *The Guardian*, 27 novembre 2013 : https://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site.

26. Nathaniel Popper, « *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes* », *The New York Times*, 12 janvier 2021 : https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html.

27. Les adresses de Stefan Thomas sont 1AYLzYN7SGu5FQLBTADBzqKm4b6Udt6Bw6 et 17eSZivDJpuJp9TxezTXVxkgLbsr3XZM1i. En date du 8 juin 2011, leur solde combiné était de 7 003,21 bitcoins.

28. Jean-Luc (Bitcoin.fr), *Sortie de la version 1.0 de Liana*, 12 mai 2023 : https://bitcoin.fr/sortie-de-la-version-1-0-de-liana/.

29. Satoshi Nakamoto, *Re: Version 0.3.13, please upgrade*, 03/10/2010 20:54:07 UTC : https://bitcointalk.org/index.php?topic=1327.msg15136#msg15136.

30. Pamela Morgan, *Cryptoasset Inheritance Planning*, Merkle Bloom LLC, 2018.

31. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

Chapitre 8 – Le consensus par le minage

1. Leslie Lamport, Robert Shostak, Marshall Pease, « *The Byzantine Generals Problem* », in *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, 1982, pp. 382—401 : https://lamport.azurewebsites.net/pubs/byz.pdf.

2. Selon Leslie Lamport, l'appellation byzantine a été choisie pour ne pas offenser le sentiment patriotique du lecteur (l'armée dans la métaphore comporte des traîtres), car cette appellation a été faite *a posteriori* par les historiens et les Byzantins eux-mêmes se considéraient comme romains. – Voir Leslie Lamport, *My Writings* : http://lamport.azurewebsites.net/pubs

/pubs.html#byz.

3. Cette propriété est démontrée dans l'article original de Lamport et al. La condition plus précise est $n \geq 3m + 1$ où n est le nombre total de généraux et m le nombre de traîtres.

4. L'infrastructure du Boeing 777 repose notamment sur le bus informatique ARINC 629 qui réplique en quadruple les messages envoyés afin de garantir un résultat avec une latence très faible. – Elaine Ou, *Byzantine Fault Tolerant Airplanes*, 12 février 2017 : https://elaineou.com/2017/02/12/byzantine-fault-tolerant-airplanes/.

5. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

6. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 13/11/2008, 22:56:55 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014849.html.

7. Plus précisément, il s'agit de sacrifier un peu de la propriété de sécurité au sens de Lamport pour améliorer la tolérance aux pannes byzantines.

8. Cynthia Dwork, Moni Naor, *Pricing via Processing or Combatting Junk Mail*, 1992.

9. Markus Jakobsson, Ari Juels, *Proofs of Work and Bread Pudding Protocols (Extended Abstract)*, 1999.

10. Adam Back, *[ANNOUNCE] hash cash postage implementation*, 28/03/1997 16:52:26 UTC : https://cypherpunks.venona.com/date/1997/03/msg00774.html ; Adam Back, *Hashcash – A Denial of Service Counter-Measure*, 1er août 2002 : http://www.hashcash.org/hashcash.pdf.

11. Hal Finney, *Bitcoin v0.1 released*, 24/01/2009 16:48:03 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015036.html.

12. « Si la majorité était basée sur le principe de vote par adresse IP (une adresse IP, une voix), elle pourrait être détournée par toute personne capable de s'octroyer de nombreuses adresses IP. La preuve de travail est essentiellement basée sur la puissance de calcul : un processeur, une voix. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

13. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

14. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

15. La dénomination *timechain* a été utilisée par Satoshi dans les commentaires du code source de novembre 2008.

16. Hal Finney, *Re: Bitcoin P2P e-cash paper*, 07/11/2008 23:40:12 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html

17. « La chaîne de blocs est une structure en forme d'arbre qui a pour racine le bloc de genèse, chaque bloc pouvant avoir plusieurs candidats à sa suite. pprev et pnext établissent un chemin à travers la chaîne principale / la chaîne plus longue. Un blockindex peut avoir plusieurs pprev qui pointent vers lui, mais pnext ne pointera que vers la branche la plus longue, ou sera nul si le bloc ne fait pas partie de la chaîne la plus longue. » – Satoshi Nakamoto, code source de la version 0.1 du logiciel Bitcoin : https://github.com/trottier/original-bitcoin/blob/4184ab26345d19e87045ce7d9291e60e7d36e096/src/main.h#L1001-L1008.

18. Démontrer qu'une feuille fait partie d'un arbre de Merkle requiert de calculer un nombre d'empreintes proportionnel au logarithme binaire du nombre de feuilles ($\log_2(n)$), et non pas proportionnel au nombre de feuilles n. Pour un bloc de 3 000 transactions (moyenne haute sur BTC), cela représente 12 empreintes de 32 octets à obtenir et 12 hachages à effectuer.

19. En notant c la valeur cible, la difficulté est définie par :

$$d = \frac{C_{\max}}{c}$$

où $C_{\max} = \texttt{0x00ffff} \times 256^{26}$ est la valeur cible maximale du réseau.

20. En termes mathématiques, le travail d'un bloc est le quotient du nombre d'empreintes possibles par le nombre d'empreintes satisfaisant le problème. En notant c la valeur cible, le travail est :

$$T = \frac{2^{256}}{c+1}\,.$$

21. Une étymologie populaire prétend qu'il serait une contraction de l'expression « *number used once* », mais celle-ci est incorrecte.

22. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

23. En décembre 2017, le mineur du bloc 501 726 s'est ainsi rémunéré de la coquette somme de 0 BTC !

24. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

25. Dans Bitcoin Core, l'algorithme d'ajustement est décrit par la fonction `CalculateNextWorkRequired` dans le fichier `pow.cpp`. La variation est limitée à un facteur 4 (multiplication comme division) pour éviter les instabilités. L'algorithme *surestime* la puissance de calcul déployée car le temps écoulé est mesuré sur 2 015 intervalles, et non pas 2 016 comme cela devrait se faire.

26. Satoshi Nakamoto, *Bitcoin v0.1 released*, 08/01/2009 19:27:40 UTC : `https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html`.

27. Cette convergence est illustrée par le paradoxe d'Achille et de la tortue formulé par le philosophe grec Zénon. La suite $\left(\sum_{i=1}^{n}(1/2)^i\right)$ converge vers 1 lorsque $n \to +\infty$.

28. « Une fois qu'un nombre prédéterminé de pièces a été mis en circulation, l'incitation peut être entièrement financée par les frais de transaction et ne plus requérir aucune inflation. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 24 mars 2009.

29. Le seul cas envisageable de transaction gratuite est celui d'une grande transaction de consolidation qui amoindrirait la charge des mineurs en réduisant considérablement l'ensemble des sorties transactionnelles non dépensées.

30. Peter Todd, *Surprisingly, Tail Emission Is Not Inflationary*, 9 juillet 2022 : `https://petertodd.org/2022/surprisingly-tail-emission-is-not-inflationary`.

31. Jorge Timón, *Freicoin: bitcoin with demurrage*, 24/02/2011 11:56:03 UTC : `https://bitcointalk.org/index.php?topic=3816.msg54170#msg54170`.

32. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

33. En réalité, au début c'était bel et bien la chaîne possédant le plus de blocs qui était sélectionnée.

Mais ce principe a été redéfini le 25 juillet 2010 au sein de la version 0.3.3 du logiciel pour prendre en compte la notion de travail.

34. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

35. L'appellation (quelque peu ambigüe) de « bloc orphelin » a été introduite par Satoshi Nakamoto au sein de la première version du logiciel. On parle aussi de « bloc oncle » (en référence au fait qu'il ne donne pas de descendance fertile) ou bien de « bloc périmé » (*stale block*).

36. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

37. Satoshi Nakamoto, *Re: Anonymity*, 08/07/2010, 19:12:00 UTC : `https://bitcointalk.org/index.php?topic=241.msg2071#msg2071`.

38. Dans un message sur le forum en juillet 2010, Satoshi écrivait à propos de l'acceptation des transactions non confirmées : « Je pense qu'il sera possible pour une entreprise de traitement des paiements de fournir comme service une distribution rapide de transactions avec une vérification suffisante en 10 secondes ou moins. Les nœuds du réseau n'acceptent que la première version d'une transaction qu'ils reçoivent pour l'incorporer dans le bloc qu'ils essaient de générer. Lorsqu'on diffuse une transaction et que quelqu'un d'autre diffuse une double dépense au même moment, c'est une course à la propagation vers le plus grand nombre de nœuds qui a lieu. Si l'une d'elles a une légère avance, elle se propagera géométriquement plus vite sur le réseau et atteindra la plupart des nœuds. [...] Le processeur de paiement a des connexions avec de nombreux nœuds. Lorsqu'il reçoit une transaction, il l'envoie et, en même temps, surveille le réseau pour détecter les doubles dépenses. S'il reçoit une double dépense sur l'un de ses nombreux nœuds d'écoute, il signale que la transaction est mauvaise. » – Satoshi Nakamoto, *Re: Bitcoin snack machine (fast transaction problem)*, 17/07/2010 22:29:13 UTC : `https://bitcointalk.org/index.php?topic=423.msg3819#msg3819`.

39. Hal Finney, *Re: Best practice for fast transaction acceptance - how high is the risk?*, 13/02/2011, 21:48:44 UTC : `https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384`.

40. vector76, *Re: Fake Bitcoins?*, 17/08/2011 17:37:56 UTC : `https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391`.

41. Ittay Eyal, Emin Gün Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, 2013.

42. « Nous considérons le scénario d'un attaquant qui tente de générer une chaîne alternative plus rapidement que la chaîne honnête. Même en cas de réussite, cela n'expose pas le système à des modifications arbitraires [...]. Un attaquant peut seulement essayer de modifier l'une de ses propres transactions afin de récupérer l'argent qu'il a récemment dépensé. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

43. « Même si un individu malintentionné parvenait à maîtriser le réseau, ce n'est pas comme s'il devenait instantanément riche. Tout ce qu'il pourrait faire, c'est récupérer l'argent qu'il a lui-même dépensé, comme un chèque sans provision. Pour tirer parti de cette possibilité, il faudrait qu'il achète une chose à un commerçant, qu'il attende qu'elle soit expédiée, puis qu'il prenne le contrôle du réseau et essaie de récupérer son argent. Je ne pense pas qu'il puisse se faire autant d'argent en essayant de monter un tel stratagème qu'en générant des bitcoins. Avec une ferme de machines zombies aussi grande, il pourrait générer plus de bitcoins que tous les autres réunis. » – Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 03/11/2008 16:23:49 : `https:`

//www.metzdowd.com/pipermail/cryptography/2008-November/014818.html.

44. Braiins, *How Much Would it Cost to 51% Attack Bitcoin?*, 11 janvier 2021 : https://braiins.com/blog/how-much-would-it-cost-to-51-attack-bitcoin.

45. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

46. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

47. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 03/11/2008, 01:37:43 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html.

48. La puissance de hachage apparente P du réseau sur une période donnée peut être retrouvée grâce aux informations de la chaîne que sont la difficulté d et le temps de bloc moyen Δt. La formule est :

$$P = \frac{T}{\Delta t} = \frac{1}{\Delta t}\left(\frac{2^{256}}{\frac{C_{\max}}{d}+1}\right).$$

où T est le travail d'un bloc et $C_{\max} = \texttt{0x00ffff} \times 256^{26}$ est la valeur cible maximale du réseau.

49. Matt Corallo, *The Future of The Bitcoin Relay Network(s)*, 7 juillet 2016 : https://bluematt.bitcoin.ninja/2016/07/07/relay-networks/.

50. Braiins, *Stratum V2 Protocol Overview* : https://braiins.com/stratum-v2#job-selection.

Chapitre 9 – La résistance à la censure

1. Voir par exemple l'affaire des Twitter Files qui a révélé les manœuvres internes et l'intervention de l'État fédéral des États-Unis dans la politique de censure de la plateforme. – Evan Perez, Donie O'Sullivan, Brian Fung, « *No directive: FBI agents, tech executives deny government ordered Twitter to suppress Hunter Biden story* », *CNN*, 23 décembre 2022 : https://edition.cnn.com/2022/12/23/politics/twitter-files-elon-musk-fbi-hunter-biden-laptop/index.html.

2. Students for Liberty, *Financial Censorship* : https://studentsforliberty.org/blog/freedom-of-expression/financial-censorship/.

3. Marco Pagani, George Whaley, David Czerwinski, « *Frameworks for Assessing Financial Censorship and Its Implications* », in *Journal of Accounting and Finance*, vol. 22, no. 1, 2022 : https://articlegateway.com/index.php/JAF/article/download/4989/4759.

4. Code pénal, Article 421-2-2, 15 novembre 2001.

5. Jonathan Thornburg, *Re: Bitcoin v0.1 released*, 17/01/2009 16:49:45 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015016.html.

6. Rob Gillies, « *Judge: Canada right to invoke emergency act in truck protest* », *Associated Press News*, 17 février 2023 : https://apnews.com/article/canada-government-justin-trudeau-ottawa-montana-9c1e37aa86d4315703e69f7794637e7f.

7. Dans son livre *Cryptomonnaie : la nouvelle guerre*, François-Xavier Thoorens explique par

exemple comment lui et sa famille ont été expulsés de leur banque familiale après avoir voulu ouvrir un compte professionnel pour recevoir des fonds récupérés lors de l'ICO d'Ark (pp. 91 – 97). Mais son cas est loin d'être une exception.

8. Cet effet de l'expérience de la censure a été décrit par Nick Szabo au micro de Peter McCormack en 2019 : « Certaines personnes doivent être frappées par la réalité. Si vous êtes censuré par une banque, comme c'est de plus en plus le cas – et c'est d'ailleurs l'un des risques de la centralisation numérique – c'est que les gens soient censurés et les activistes politiques de différents bords commencent à découvrir qu'on peut aller voir les banques et faire taire ses ennemis politiques et les gens qui font des choses qu'on ne veut pas qu'ils fassent, on les fait taire. On n'a pas nécessairement besoin de faire passer une loi, on peut convaincre certains régulateurs ou certains politiciens, et puis ils mettent la pression sur les banques, et boum : c'est notre loi de facto juste là. Ça se produit de plus en plus souvent parce que la centralisation numérique rend les choses si vulnérables à ça. Il s'agit donc d'une tendance opposée et tout dépend de la vitesse à laquelle elle se développe, car à chaque fois que quelqu'un est censuré, boum : c'est une réalité qui s'impose à lui et il devient fan de Bitcoin. » – What Bitcoin Did Podcast, *Nick Szabo on Cypherpunks, Money and Bitcoin* (audio), 1er novembre 2019 : `https://www.whatbitcoindid.com/podcast/nick-szabo-on-cypherpunks-money-and-bitcoin`.

9. Ap 13:16-17.

10. Sur Ethereum, les adresses liées au contrat de mélange Tornado Cash ont été placées sur la liste de l'OFAC en août 2022. Mais sur BTC, aucune loi ni liste liée au mélange n'est connue : il y a juste une suspicion généralisée.

11. Communiqué de Marathon et de DMG Blockchain Solutions, *Marathon Patent Group and DMG Blockchain Solutions to Form the Digital Currency Miners of North America (DCMNA) and Launch North America's First Cooperative Mining Pool*, 5 janvier 2021, archive : `https://web.archive.org/web/20210128112455/https://www.marathonpg.com/news/press-releases/detail/1220/marathon-patent-group-and-dmg-blockchain-solutions-to-form`.

12. La valeur extractible maximale (*maximal extractable value*), initialement appelée valeur extractible par les mineurs (*miner extractable value*), est la valeur maximale que le validateur peut générer en modifiant l'ordre ou en excluant des transactions au sein de son bloc, profitant des différentes irrégularités des contrats autonomes, notamment en ce qui concerne les places de marché décentralisées. En octobre 2022, la quantité de validation passant par des relais appliquant ce type d'optimisation a dépassé les 50 %, indiquant la potentialité d'une attaque. – Voir MEV Watch : `https://www.mevwatch.info/`.

13. On a vu dans le chapitre 8 que le coût d'une telle attaque se chiffre en milliards de dollars sur le réseau Bitcoin principal.

14. Juraj Bednar, *Bitcoin censorship will most likely come, pt 2*, 18 novembre 2020 : `https://juraj.bednar.io/en/blog-en/2020/11/18/bitcoin-censorship-will-most-likely-come-pt-2/`.

15. Joshua A. Kroll, Ian C. Davey, Edward W. Felten, « *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries* », in *Workshop on the Economics of Information Security*, 2013 : `https://asset-pdf.scinapse.io/prod/2188530018/2188530018.pdf`.

16. Satoshi Nakamoto, *Bitcoin v0.1 released*, 08/01/2009 19:27:40 UTC : `https://www.metzdo`

wd.com/pipermail/cryptography/2009-January/014994.html.

17. Le mécanisme de résistance à la censure a initialement été décrit par Eric Voskuil en janvier 2018 : https://github.com/libbitcoin/libbitcoin-system/wiki/Other-Means-Principle/77d7556a14f89d1704f1bb97ca0aed04606363d0. Voir aussi Eric Voskuil, « Propriété de résistance à la censure », in *Cryptoéconomie : Principes fondamentaux de Bitcoin*, Amazon KDP, 2022, pp. 24–25.

18. Eric Voskuil, « Modèle de sécurité qualitatif », in *Cryptoéconomie : Principes fondamentaux de Bitcoin*, Amazon KDP, 2022, pp. 59–62.

19. Dans Bitcoin, les frais sont aujourd'hui payés proportionnellement à la charge des données (taille ou poids de la transaction). Cependant, la menace de plus en plus claire de la censure pourrait pousser les utilisateurs à payer des frais proportionnels au montant transféré comme cela se fait dans le domaine financier en général.

20. « Je dis que quiconque tremble en ce moment est coupable ; car jamais l'innocence ne redoute la surveillance publique. » – Maximilien de Robespierre, *Discours du 11 germinal, an II*, 31 mars 1794.

21. Dans Monero et dans les systèmes apparentés, la révélation des transactions liées à une adresse se fait par l'intermédiaire d'une clé privée d'inspection (*private view key*).

22. Dans le monde bancaire, la *Travel Rule* a originellement été promulguée par le FinCEN étasunien en 1996 (voir 31 CFR 103.33(g)). Elle exige que toutes les institutions financières transmettent des informations sur les expéditeurs à l'institution financière suivante lors de certains transferts de fonds. Dans le cas de Bitcoin et des cryptomonnaies, il s'agit d'émuler ce voyage en considérant que les utilisateurs sont des institutions financières lorsqu'ils réalisent des transactions souveraines. Le GAFI a ajouté le transfert d'« actifs virtuels » à ses recommandations en juin 2019, notamment en ce qui concerne la recommandation 16. Cette règle du voyage cryptomonétaire pourrait être appliquée par l'intégration dans les portefeuilles du protocole de preuve de propriété d'adresse (AOPP) proposé en janvier 2022.

23. Jean-Pierre Claris de Florian, « Le Grillon », in *Fables de Florian*, 1793.

24. Vitalik Buterin, *A Proof of Stake Design Philosophy*, 30 décembre 2016 : https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51.

25. Un seul bloc (le bloc 662 687 d'identifiant 000000000000000000709b858a6a0c8610e604e77072ef4407763afb0780ce712) de l'attaquant a été invalidé, faisant que 172 blocs ont été mis de côté, et que la chaîne non censurée est devenue la chaîne correcte. – Nikita Zhavoronkov sur Twitter, 01/12/2020 21:59 UTC : https://twitter.com/nikzh/status/1333893457920876550.

26. Le point de contrôle le plus récent est celui du bloc 295 000 miné le 9 avril 2014 (au même moment de l'arrivée de Wladimir van der Laan au poste de mainteneur principal) et ayant pour identifiant 00000000000000004d9b4ef50f0f9d686fd69db2e03af35a100370c64632a983. Voir le fichier chainparams.cpp dans Bitcoin Core.

27. BSV Association sur Twitter, 03/09/2021 21:17 UTC : https://twitter.com/BitcoinAssn/status/1422668065024663554.

28. Amaury Séchet (deadalnix) sur Twitter, 12/11/2018 11:42 UTC : https://twitter.com/de

adalnix/status/1061947426096009216.

29. Satoshi Nakamoto, *Re: BitDNS and Generalizing Bitcoin*, 09/12/2010 21:02:42 UTC : https://bitcointalk.org/index.php?topic=1790.msg28696#msg28696.

30. Luke-Jr, *Re: [DEAD] Coiledcoin - yet another cryptocurrency, but with OP_EVAL!*, 06/01/2012 18:56:03 UTC : https://bitcointalk.org/index.php?topic=56675.msg678006#msg678006.

31. Vitalik Buterin, *Proof of Stake: How I Learned to Love Weak Subjectivity*, 25 novembre 2014 : https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity.

32. Ce problème peut être atténué par une intervention sociale en décrétant un certain nombre de blocs comme valides par défaut. Mais on en revient alors à la situation discutée dans la section précédente.

33. À propos de l'acceptation de la plus longue chaîne par le logiciel, Satoshi ajoutait : « La seule exception à cette règle, ce sont les points de contrôle manuels que j'ai ajoutés. S'ils n'étaient pas là, le logiciel pourrait se recoordonner en remontant jusqu'au premier bloc. » – Voir Satoshi Nakamoto, *Re: checkpointing the block chain*, 16/08/2010 20:20:53 UTC : https://bitcointalk.org/index.php?topic=834.msg9816#msg9816.

34. Vitalik Buterin et al., *Combining GHOST and Casper*, 11 mai 2020 : https://arxiv.org/pdf/2003.03052.pdf.

35. QuantumMechanic, *Proof of stake instead of proof of work*, 11/07/2011 04:12:45 UTC : https://bitcointalk.org/index.php?topic=27787.msg349645#msg349645.

36. Eric Wall, *The Case for Social Slashing*, 22 août 2022 : https://ercwl.medium.com/the-case-for-social-slashing-59277ff4d9c7.

37. Vitalik Buterin, *Why Proof of Stake (Nov 2020)*, 6 novembre 2020 : https://vitalik.ca/general/2020/11/06/pos2020.html.

38. La première critique de la consommation d'énergie de Bitcoin a été faite par l'ancien cypherpunk John Gilmore en janvier 2009 : « La dernière chose dont nous avons besoin est de déployer un système conçu pour brûler tous les cycles disponibles, consommant de l'électricité et générant du dioxyde de carbone, partout sur internet, afin de produire de petites quantités de dollars binaires pour faire passer des courriels ou des spams. » – John Gilmore, *Proof of Work -> atmospheric carbon*, 25/01/2009 22:40:45 : https://www.metzdowd.com/pipermail/cryptography/2009-January/015042.html.

    Cette préoccupation a conduit Hal Finney à écrire son troisième et dernier tweet sur Bitcoin où il affirmait réfléchir « à la manière de réduire les émissions de CO_2 que produirait une mise en œuvre généralisée de Bitcoin ». – Hal Finney sur Twitter, 27/01/2009 20:14 UTC : https://twitter.com/halfin/status/1153096538.

Chapitre 10 – Le changement de la monnaie

1. « Le code source ouvert signifie que n'importe qui peut examiner le code de manière indépendante. S'il s'agissait d'une source fermée, personne ne pourrait vérifier la sécurité. Je pense qu'il est

essentiel pour un programme de cette nature d'avoir un code source ouvert. » – Satoshi Nakamoto, *Re: Questions about Bitcoin*, 10/12/2009 20:49:02 UTC : https://bitcointalk.org/index.php?topic=13.msg46#msg46.

2. *Bitcoin Core integration/staging tree* : https://github.com/bitcoin/bitcoin.

3. Satoshi Nakamoto, *Re: Switch to GPL*, 12/09/2010 19:24:53 UTC : https://bitcointalk.org/index.php?topic=989.msg12494#msg12494.

4. « Les mainteneurs prendront en considération un correctif s'il est en accord avec les principes généraux du projet ; s'il répond aux normes minimales d'inclusion ; et jugeront du consensus général des contributeurs. » – *Contributing to Bitcoin Core*, 26 mai 2023 : https://github.com/bitcoin/bitcoin/blob/25.x/CONTRIBUTING.md.

5. Wladimir J. van der Laan, *The widening gyre*, 21 janvier 2021, archive : https://web.archive.org/web/20210121201607/https://laanwj.github.io/2021/01/21/decentralize.html ; Wladimir J. van der Laan, *Remove laanwj from trusted-keys (git commit)*, 07/02/2023 09:12 UTC : https://github.com/bitcoin/bitcoin/commit/aafa5e945cef7a4f65ddadcf548932dd4e27ada1.

6. Awemany, *600 Microseconds*, 21 septembre 2018 : https://medium.com/@awemany/600-microseconds-b70f87b0b2a6.

7. Comme le faisait remarquer Hal Finney en 2011 : « Chaque jour qui passe sans que Bitcoin ne s'effondre en raison de problèmes juridiques ou techniques apporte de nouvelles informations au marché. Cela augmente les chances de succès de Bitcoin et justifie un prix plus élevé. » – Hal Finney, *Re: Bitcoin and the Efficient Market Hypothesis*, 04/06/2011 23:36:04 UTC : https://bitcointalk.org/index.php?topic=11765.msg169026#msg169026.

8. Eric Lombrozo, *BIP-123: BIP Classification*, 26 août 2015 : https://github.com/bitcoin/bips/blob/master/bip-0123.mediawiki.

9. Satoshi Nakamoto décrivait la vérification de paiement simplifiée comme suit : « Il est possible de vérifier les paiements sans faire fonctionner un nœud complet du réseau. Un utilisateur a seulement besoin de conserver une copie des entêtes des blocs de la plus longue chaîne de preuves de travail, qu'il peut obtenir en interrogeant les nœuds du réseau jusqu'à ce qu'il soit convaincu qu'il possède la plus longue chaîne, et obtenir la branche de Merkle liant la transaction au bloc dans lequel elle est horodatée. Il ne peut pas vérifier la transaction par lui-même, mais en la reliant à un endroit de la chaîne, il peut voir qu'un nœud du réseau l'a acceptée, et les blocs ajoutés après le confirment. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

10. Ce cas a été décrit par Satoshi Nakamoto dans le livre blanc : « De ce fait, la vérification est fiable tant que les nœuds honnêtes contrôlent le réseau, mais est plus vulnérable si le réseau est maîtrisé par un attaquant. Alors que les nœuds du réseau peuvent vérifier les transactions par eux-mêmes, la méthode simplifiée peut être trompée par des transactions forgées par l'attaquant aussi longtemps que celui-ci maîtrise le réseau. Une stratégie pour se protéger serait d'accepter les alertes des nœuds du réseau lorsqu'ils détectent un bloc invalide, invitant le logiciel de l'utilisateur à télécharger le bloc complet et les transactions suspectes pour confirmer l'incohérence. Les entreprises qui reçoivent fréquemment des paiements voudront probablement toujours faire fonctionner leurs propres nœuds afin d'obtenir une sécurité plus indépendante et une vérification plus rapide. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre

2008.

Les alertes décrites par Satoshi sont aujourd'hui appelées preuves de fraude mais sont toujours en phase de développement.

11. Une première façon de remédier au problème de confidentialité était de mettre en place des filtres de Bloom, tels que décrits dans le BIP-37, mais cette méthode était peu efficace. Voir Arthur Gervais, Srdjan Capkun, Ghassan O. Karame, Damian Gruber, « *On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients* », in *Proceedings of the 30th Annual Computer Security Applications Conference*, décembre 2014, pp. 326—335 : `https://eprint.iacr.org/2014/763.pdf`. Il existe également Neutrino, décrit dans le BIP-157 et le BIP-158, qui fait usage du codage de Golomb-Rice et demande une plus grande bande passante.

12. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 03/11/2008, 01:37:43 UTC : `https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html`.

13. Understanding Bitcoin, *Not Your Node Not Your Rules! w/ Ketominer, Udi Wertheimer, Francis Pouliot & Mir Liponi* (vidéo), 5 avril 2019 : `https://www.youtube.com/watch?v=jwaKVIEm-rI`.

14. Satoshi Nakamoto, code source de la version 0.1 du logiciel Bitcoin : `https://github.com/trottier/original-bitcoin/blob/4184ab26345d19e87045ce7d9291e60e7d36e096/src/main.h#L1001-L1008`.

15. Notez que les concepts sont liés. Ainsi, un fork logiciel (copie et modification) peut implémenter un fork des règles de consensus (hard fork ou soft fork) qui finira par créer un fork persistant de la chaîne (scission).

16. David François (davout), *Re: Small protocol changes for flexibility*, 07/12/2010 15:08:02 UTC : `https://bitcointalk.org/index.php?topic=894.msg27757#msg27757`.

17. Le 11 mars 2013, le passage de la version 0.7 du logiciel à la version 0.8 implémentait la migration du système de base de données de Berkeley DB à LevelDB. Toutefois, il s'avérait que Berkeley DB faisait intervenir une limite par défaut (*lock limit*) qui n'était pas présente dans LevelDB. Par conséquent, la migration constituait un hard fork accidentel et a provoqué un embranchement à partir du bloc 225 430 qui a duré environ 6 heures. La décision a finalement été prise de revenir à la version 0.7, invalidant la branche de 24 blocs minée du côté de la version 0.8, et de procéder à la migration quelques mois plus tard. – Voir Vitalik Buterin, « *Bitcoin Network Shaken by Blockchain Fork* », *Bitcoin Magazine*, 13 mars 2013 : `https://bitcoinmagazine.com/technical/bitcoin-network-shaken-by-blockchain-fork-1363144448` ; et Gavin Andresen, *BIP-50: March 2013 Chain Fork Post-Mortem*, : `https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki`.

    Une double dépense conséquente a été réalisée : macbook-air, *A successful DOUBLE SPEND US$10000 against OKPAY this morning.*, 12/03/2013, 18:22:02 UTC : `https://bitcointalk.org/index.php?topic=152348.msg1616747#msg1616747`.

18. En octobre 2010, à la suite de la proposition de Jeff Garzik d'augmenter la limite directement à 7,168 Mo afin d'« égaler le taux transactionnel moyen de PayPal », Satoshi – bien conscient qu'il s'agissait d'un correctif « incompatible avec le réseau » – écrivait : « [La mise à niveau] peut être introduite progressivement, par exemple : if (blocknumber > 115000) maxblocksize = largerlimit. Elle peut commencer à être intégrée dans les versions bien avant, de sorte qu'au moment où elle atteint le numéro de bloc et entre en vigueur, les anciennes versions qui ne l'ont

pas sont déjà obsolètes. Lorsque nous approchons du numéro de bloc limite, je peux envoyer une alerte aux anciennes versions pour qu'elles sachent qu'elles doivent effectuer une mise à jour. » – Satoshi Nakamoto, *Re: [PATCH] increase block size limit*, 04/10/2010 19:48:40 UTC : https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366.

19. Nicolas van Saberhagen (ByteCoin), *OP_EVAL proposal*, 02/10/2011 00:49:19 UTC : https://bitcointalk.org/index.php?topic=46538.msg553689#msg553689.

20. « Je lis probablement mal le code, mais je pense que OP_EVAL ne provoquerait pas de scission de la chaîne de blocs ! » s'est exprimé Gavin Andresen sur IRC. – #bitcoin-dev IRC logs, 2 octobre 2010, archive : https://web.archive.org/web/20131201200245/http://bitcoinstats.com/irc/bitcoin-dev/logs/2011/10/02.

21. Satoshi Nakamoto, *reverted makefile.unix wx-config – version 0.3.6 (git commit)*, 29/07/2010 18:27:12 UTC : https://sourceforge.net/p/bitcoin/code/119/.

22. La façon dont un soft fork peut introduire de l'inflation dans Bitcoin a été exposée par le développeur Peter Todd en 2016. – Peter Todd, *Forced Soft Forks*, 18 janvier 2016 : https://petertodd.org/2016/forced-soft-forks.

23. Mircea Popescu, *There's a one Bitcoin reward for the death of Pieter Wuille. Details below.*, 10 décembre 2015 : http://trilema.com/2015/theres-a-one-bitcoin-reward-for-the-death-of-pieter-wuille-details-below/.

24. Amaury Séchet, *Bitcoin ABC's plan for the November 2020 upgrade*, 6 août 2020 : https://amaurysechet.medium.com/bitcoin-abcs-plan-for-the-november-2020-upgrade-65fb84c4348f.

25. Vitalik Buterin, *Hard Forks, Soft Forks, Defaults and Coercion*, 14 mars 2017 : https://vitalik.ca/general/2017/03/14/forks_and_markets.html.

Chapitre 11 – La détermination du protocole

1. Nathaniel Popper, Peter Lattman, « *As Big Investors Emerge, Bitcoin Gets Ready for its Close-Up* », *CNBC*, 11 avril 2013 : https://www.cnbc.com/id/100635418.

2. Pierre Rochard, *Bitcoin Governance*, 9 juillet 2018 : https://pierre-rochard.medium.com/bitcoin-governance-37e86299470f.

3. Arthur Breitman parlait de *social consensus* dès août 2014 dans la première description formelle de Tezos. – Arthur Breitman, *Tezos: A Self-Amending Crypto-Ledger*, 3 août 2014 : https://tezos.com/position-paper.pdf.

4. Meni Rosenfeld, *Re: How could the bitcoin protocol be changed? Has this ever occurred?*, 14/06/2012 13:53:19 UTC : https://bitcoin.stackexchange.com/questions/3945/how-could-the-bitcoin-protocol-be-changed-has-this-ever-occurred#comment4983_3948.

5. Gavin Andresen, *[Bitcoin-development] Proposed alternatives to the 20MB step function*, 29/05/2015 12:39:30 UTC, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/008340.html.

6. Eric Voskuil, « Principe de risque de garde », in *Cryptoéconomie : Principes fondamentaux de Bitcoin*, Amazon KDP, 2022, pp. 34–35.

7. Cette réalité a été perçue en janvier 2010 par NewLibertyStandard, le premier commerçant de Bitcoin, lorsqu'il a déclaré : « Toutes les personnes qui achètent ou vendent des biens en utilisant des bitcoins, y compris les changeurs, font progresser l'économie de Bitcoin. » – NewLibertyStandard, *Re: New Exchange Service: "BTC 2 PSC"*, 19/01/2010 08:06:15 UTC : `https://bitcointalk.org/index.php?topic=15.msg111#msg111`.

8. Jeff Garzik écrivait très justement en octobre 2010 que « l'effort visant à augmenter la limite du taux de transaction [était] le même que celui visant à modifier la nature fondamentale des bitcoins : convaincre la grande majorité de se mettre à niveau ». – Jeff Garzik, *Re: [PATCH] increase block size limit*, 04/10/2010 18:33:55 UTC : `https://bitcointalk.org/index.php?topic=1347.msg15342#msg15342`.

9. Arthur Breitman, *Tezos: A Self-Amending Crypto-Ledger*, 3 août 2014 : `https://tezos.com/position-paper.pdf`.

10. Satoshi Nakamoto, *Re: A few suggestions*, 13/12/2009 16:51:25 UTC : `https://bitcointalk.org/index.php?topic=12.msg62#msg62`.

11. Eric Voskuil, « Modèle de sécurité qualitatif », in *Cryptoéconomie : Principes fondamentaux de Bitcoin*, Amazon KDP, 2022, pp. 59–62.

12. Le premier commerçant, NewLibertyStandard, a « vendu » 5,02 $ contre 5 050 BTC à Martti Malmi, le premier client, le 12 octobre 2009. On peut aussi arguer que le mineur du bloc 2 817 qui a reçu 2 BTC en frais de transaction le 3 février 2009 a techniquement été le premier commerçant pour son service, mais la somme impliquée était négligeable.

13. La loi de Metcalfe tient son nom de Robert Metcalfe, cocréateur du protocole Ethernet et fondateur de 3com, qui avait observé cet effet en 1980 au sujet de dispositifs communicants compatibles. La loi a été formellement énoncée par George Gilder en 1993 dans un article publié dans Forbes. Elle faisait varier l'utilité du réseau en n^2 où n est le nombre d'utilisateurs, ce qui surestimait grossièrement l'effet de réseau réel. Une deuxième loi plus conservatrice, la loi d'Odlyzko, a été proposée en 2006 pour faire varier l'utilité du réseau en $n \log(n)$. – George Gilder, *Metcalf's Law and Legacy*, 1er septembre 1993 : `https://www.discovery.org/a/41/`; Bob Briscoe, Andrew Odlyzko, Benjamin Tilly, *Metcalfe's Law is Wrong*, 1er juillet 2006 : `https://spectrum.ieee.org/metcalfes-law-is-wrong`.

14. Vitalik Buterin, *On Bitcoin Maximalism, and Currency and Platform Network Effects*, 19 novembre 2014 : `https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects`.

15. Le point de Schelling est, en théorie des jeux, une solution à laquelle les participants à un jeu de coordination pure ne pouvant communiquer auront tendance à se rallier, parce qu'elle leur semble présenter une caractéristique qui la fera choisir aussi par l'autre. L'exemple typique est l'endroit où peuvent se retrouver des gens en voyage dans un lieu, qui sera généralement un monument connu de tous, la Tour Eiffel à Paris par exemple. – Thomas C. Schelling, *The Strategy of Conflict*, Harvard University Press, 1960.

16. L'implémentation des solutions de surcouche telles que le réseau Lightning ne font qu'améliorer la capacité effective de transfert de valeur, comme nous le montrerons dans le chapitre 14.

17. Le déplacement effectif des transferts vers des systèmes apparentés moins chers a notamment été observé par Matt Ahlborg, consultant en étude de marché pour Bitrefill, une plateforme de vente de recharge téléphonique et de cartes-cadeaux. – Matt Ahlborg sur Twitter, 17/04/2023 14:14 UTC : https://twitter.com/MattAhlborg/status/1647966711126147072.

18. Ce concept de *rough consensus* provient de son utilisation en 1998, par l'*Internet Engineering Task Force* (IETF), qui le décrivait comme suit dans ses procédures pour les groupes de travail : « Les groupes de travail prennent des décisions au moyen d'un processus de "consensus approximatif". Le consensus IETF ne requiert pas que chaque participant soit d'accord, bien que cela soit bien entendu préférable. De façon générale, l'opinion dominante du groupe de travail doit prévaloir (cependant, cette "dominance" ne doit pas être déterminée sur la base du volume ou de l'insistance, mais plutôt selon une impression plus générale d'accord). Le consensus peut être déterminé au moyen d'un vote à main levée, ou de n'importe quel autre moyen sur lequel le groupe de travail est d'accord. Il convient de noter que 51 % des voix ne peut être considéré comme un "consensus approximatif", et qu'en sens inverse, 99 % est mieux qu'approximatif. C'est au président de déterminer si un consensus approximatif est atteint. » – *IETF Working Group Guidelines and Procedures*, septembre 1998 : https://datatracker.ietf.org/doc/html/rfc2418.

19. dEBRUYNE, *Re: Monero inception - how did bitmonero become monero?*, 11/08/2016 16:21 : https://monero.stackexchange.com/questions/1011/monero-inception-how-did-bitmonero-become-monero/1024#1024.

20. Une « guerre du hachage » s'est déroulée entre les mineurs de Bitcoin SV, soutenus par Craig Wright et Calvin Ayre, et ceux de Bitcoin ABC, soutenus par Roger Ver et Jihan Wu, notamment par la redirection de la puissance de calcul de leurs coopératives de minage respectives. – Aaron van Wirdum, *Week 2: How the Bitcoin Cash "Hash War" Came and Went and Not Much Happened*, 30 novembre 2018 : https://bitcoinmagazine.com/technical/week-2-how-bitcoin-cash-hash-war-came-and-went-and-not-much-happened.

21. Peter Todd, *Forced Soft Forks*, 18 janvier 2016 : https://petertodd.org/2016/forced-soft-forks.

22. C'était, par exemple, la conception du PDG de Coinbase, Brian Armstrong, qui écrivait le 3 janvier 2016 : « Heureusement, Bitcoin dispose d'un mécanisme de mise à niveau intégré et élégant. Si la majorité des mineurs de Bitcoin "votent" pour une mise à niveau particulière, il s'agit par définition de la nouvelle version de Bitcoin. Le nombre de votes obtenus par chaque mineur est proportionnel à la quantité de puissance de calcul qu'il apporte au réseau (les votes ne peuvent donc pas être truqués). » – Brian Armstrong, *Scaling Bitcoin: The Great Block Size Debate*, 3 janvier 2016 : https://www.coinbase.com/blog/scaling-bitcoin-the-great-block-size-debate.

23. « Le réseau Bitcoin n'appartient à personne, tout comme la technique derrière le courriel n'appartient à personne. Bitcoin est contrôlé par l'ensemble de ses utilisateurs autour du monde. Alors que les développeurs améliorent les logiciels, ils ne peuvent pas imposer de modification dans le protocole Bitcoin parce que chaque utilisateur est libre de choisir quel logiciel et quelle version il utilise. Afin de rester compatibles avec les autres, tous les utilisateurs doivent utiliser des logiciels se conformant aux mêmes règles. Bitcoin ne peut fonctionner correctement qu'avec un consensus total entre ses utilisateurs. » – Bitcoin.org FAQ : https://bitcoin.org/fr/faq#qui-controle-le-reseau-bitcoin.

24. GameKyuubi, *I AM HODLING*, 18/12/2013 10:03:03 UTC : https://bitcointalk.org/in

dex.php?topic=375643.msg4022997#msg4022997.

25. Le terme de « monnaie acéphale » a été popularisé par Jacques Favier et Adli Takkal Bataille dans *Bitcoin, la monnaie acéphale* en 2017.

26. Divers modèles de financement ont été proposés : celui de la Fondation Bitcoin entre 2012 et 2014, celui du capital-risque avec le financement de Blockstream à partir de 2014, celui du financement participatif avec Lighthouse (BTC) en 2014 et Flipstarter (BCH) en 2020, et enfin celui de l'utilisation de la subvention de minage (Dash, Zcash, XEC) depuis 2015.

Chapitre 12 – Les rouages de la machine

1. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

2. Satoshi Nakamoto, *Re: Transactions and Scripts: DUP HASH160 ... EQUALVERIFY CHECKSIG*, 17/06/2010 18:46:08 : `https://bitcointalk.org/index.php?topic=195.msg1611#msg1611`.

3. Andreas M. Antonopoulos, « *Transactions* », in *Mastering Bitcoin: Programming the Open Blockchain*, 2e édition, 2017, pp. 117–148.

4. Gavin Andresen, *svn r197: IsStandard check for transactions*, 07/12/2010 13:58:33 UTC : `https://bitcointalk.org/index.php?topic=2129.msg27744#msg27744`.

5. Nicolas van Saberhagen (ByteCoin), *OP_EVAL proposal*, 02/10/2011 00:49:19 UTC : `https://bitcointalk.org/index.php?topic=46538.msg553689#msg553689`.

6. Gavin Andresen, *Re: OP_EVAL proposal*, 02/10/2011 20:42:32 UTC : `https://bitcointalk.org/index.php?topic=46538.msg554620#msg554620`.

7. Gavin Andresen, *BIP-16: Pay to Script Hash*, 3 janvier 2012 : `https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#rationale`.

8. L'instruction `OP_RETURN` servait initialement à retourner la valeur au sommet de la pile, d'où son nom. Cependant, en juillet 2010, la découverte du « *1 RETURN bug* », qui permettait de dépenser toute sortie transactionnelle via le script de déverrouillage `TRUE RETURN`, a poussé Satoshi Nakamoto à désactiver cette fonctionnalité en lui faisant renvoyer `FALSE` systématiquement. Voir Satoshi Nakamoto, *reverted makefile.unix wx-config – version 0.3.6 (git commit)*, 29/07/2010 18:27:12 UTC : `https://sourceforge.net/p/bitcoin/code/119/`.

9. Joseph Poon, *[bitcoin-dev] SIGHASH_NOINPUT in Segregated Witness*, 26/02/2016 01:07:46 UTC : `https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-February/012460.html`.

10. Sur l'attaque de méalléabilité contre Mt. Gox, voir Ken Shirriff, *The Bitcoin malleability attack graphed hour by hour*, 15 février 2014 : `https://www.righto.com/2014/02/the-bitcoin-malleability-attack-hour-by.html`. Voir aussi Christian Decker, Roger Wattenhofer, *Bitcoin Transaction Malleability and MtGox*, 26 mars 2014 : `https://arxiv.org/pdf/1403.6676.pdf`.

11. SF Bitcoin Developers, *Sidechains: Bringing New Elements to Bitcoin* (vidéo), 8 juin 2015 : `https://www.youtube.com/watch?v=Twynh6xIKUc`.

12. SegWit Resources, *Why a discount factor of 4? Why not 2 or 8?*, 13 janvier 2017 : `https://medium.com/segwit-co/why-a-discount-factor-of-4-why-not-2-or-8-bbcebe91721e`.

13. Une transaction à 2 entrées et 2 sorties de type P2WPKH mesure 372 octets et pèse 834 unités de poids au maximum. De ce fait, il est possible d'inclure 4 796 transactions dans un bloc, ce qui nous permet de calculer sa taille réelle.

14. Voir le bloc 774 628, d'identifiant `00000000000000000000515e202c8ae73c8155fc472422d7593af87aa74f2cf3d` dont la taille était de 3 955 272 octets et qui incluait une transaction qui mesurait à elle seule 3 938 383 octets.

15. Gavin Andresen, *[bitcoin-dev] Time to worry about 80-bit collision attacks or not?*, 07/01/2016 19:02:05 UTC : `https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-January/012198.html`.

16. « Le modèle bancaire traditionnel atteint un certain niveau de confidentialité en limitant l'accès aux informations aux parties concernées et au tiers de confiance. La nécessité d'annoncer publiquement toutes les transactions exclut cette méthode, mais la confidentialité peut toujours être préservée en interrompant le flux d'informations à un autre endroit : en gardant les clés publiques anonymes. Le public peut voir que quelqu'un envoie un montant à quelqu'un d'autre, mais ne dispose pas d'informations reliant la transaction à qui que ce soit. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

17. « Comme pare-feu supplémentaire, une nouvelle paire de clés devrait être utilisée pour chaque transaction afin de les empêcher d'être liées à un propriétaire commun. Certains liens sont toujours inévitables avec les transactions à entrées multiples, qui révèlent nécessairement que leurs entrées appartiennent au même propriétaire. Le risque est que si le propriétaire d'une clé est révélé, la liaison pourrait révéler d'autres transactions qui lui appartiennent. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

18. Gregory Maxwell, *CoinJoin: Bitcoin privacy for the real world*, 22/08/2013 02:32:31 UTC : `https://bitcointalk.org/index.php?topic=279249.msg2983902#msg2983902`.

19. Loïc Morel, *Comprendre et utiliser le CoinJoin sur Bitcoin*, 19 juillet 2022 : `https://www.pandul.fr/post/comprendre-et-utiliser-le-coinjoin-sur-bitcoin`.

20. Adam Ficsor (nopara73), William Hill (TDevD), *ZeroLink: The Bitcoin Fungibility Framework*, 14 août 2017 : `https://github.com/nopara73/ZeroLink/tree/32ad53927a343383534bea28fffb098af65fe62a`.

21. Le système de mélange Whirlpool, ainsi que le portefeuille Samourai, ont été interrompus le 24 avril 2024 sur ordre du département de la Justice des États-Unis. Les cofondateurs de ces services, Keonne Rodriguez et William Hill, ont été arrêtés le même jour par les autorités. – United States Attorney for the Southern District of New York, *Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses*, 24 avril 2024 : `https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering`. (Note de janvier 2025.)

22. Chris Belcher, *Design for a CoinSwap Implementation for Massively Improving Bitcoin Privacy and Fungibility*, 25 mai 2020 : `https://gist.github.com/chris-belcher/9144bd57a91c194e332fb5ca371d0964`.

23. Satoshi Nakamoto, *Re: Not a suggestion*, 11/08/2010 00:14:22 UTC : https://bitcointalk.org/index.php?topic=770.msg8637#msg8637.

24. Nicolas van Saberhagen (ByteCoin), *Untraceable transactions which can contain a secure message are inevitable*, 17/04/2011, 02:34:24 UTC : https://bitcointalk.org/index.php?topic=5965.msg87757#msg87757 ; Peter Todd, *[Bitcoin-development] Stealth Addresses*, 06/01/2014 12:03:38 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html.

25. En termes mathématiques, si on note r et R les clés éphémères de transaction, v et V les clés d'inspection et k et K les clés de dépense, alors la méta-adresse est $M = (K, V)$, le secret partagé est :

$$S = r\,V = r\,v\,G = v\,r\,G = v\,R$$

et la clé publique de réception est :

$$P = K + H(S)\,G\,.$$

Le destinataire peut aussi n'utiliser qu'une seule paire de clés (k, K). Dans ce cas, $M = K$.

26. Ruben Somsen, *Silent Payments*, 13 mars 2022 : https://gist.github.com/RubenSomsen/c43b79517e7cb701ebf77eec6dbb46b8.

27. Nicolas van Saberhagen, *CryptoNote v2.0*, 17 octobre 2013 : http://cryptonote.org/whitepaper.pdf ; archive : https://web.archive.org/web/20140529235502/http://cryptonote.org/whitepaper.pdf.

28. Adam Back, *bitcoins with homomorphic value (validatable but encrypted)*, October 01, 2013, 02:19:53 PM : https://bitcointalk.org/index.php?topic=305791.msg3277431#msg3277431 ; Gregory Maxwell, *Confidential Transactions*, 2015, archive : https://web.archive.org/web/20150628230410/https://people.xiph.org/~greg/confidential_values.txt.

29. Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Gregory Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More*, 2018 : https://eprint.iacr.org/2017/1066.pdf.

30. Tom Elvis Jedusor, *Mimblewimble*, 19 juillet 2016, archive : https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt.

31. Andrew Poelstra, *Mimblewimble*, 6 octobre 2016 : https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf.

32. Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin, « *Zerocoin: Anonymous Distributed E-Cash from Bitcoin* », in *2013 IEEE Symposium on Security and Privacy*, 2013, pp. 397–411 : https://ieeexplore.ieee.org/document/6547123 ; Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, « *Zerocash: Decentralized Anonymous Payments from Bitcoin* », *2014 IEEE Symposium on Security and Privacy*, 2014, pp. 459–474 : https://ieeexplore.ieee.org/document/6956581.

33. Zooko Wilcox-O'Hearn, *The Design of the Ceremony*, 26 octobre 2016 : https://electriccoin.co/blog/the-design-of-the-ceremony/.

Chapitre 13 – Les contrats autonomes

1. L'appellation « contrat autonome » visant à traduire *smart contract* a été proposée par Jacques Favier, Adli Takkal-Bataille et Benoît Huguet dans *Bitcoin : Métamorphoses* (pp. 105–107) en 2018.

2. Nick Szabo, *Smart Contracts*, 1994, archive : `https://web.archive.org/web/20011102030833/http://szabo.best.vwh.net:80/smart.contracts.html`.

3. L'adresse multisignatures 3-parmi-5 de Bitfinex est `bc1qgdjqv0av3q56jvd82tkdjpy7gdp9ut8tlqmgrpmv24sq90ecnvqqjwvw97`.

4. « Les acheteurs pourraient être facilement protégés par la mise en œuvre de mécanismes de dépôt fiduciaire routiniers. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

5. Sergio Demian Lerner, *P2PTradeX: P2P Trading between cryptocurrencies*, 05/07/2012 23:49:48 UTC : `https://bitcointalk.org/index.php?topic=91843.msg1011737#msg1011737` ; Gregory Maxwell, *Re: P2PTradeX: P2P Trading between cryptocurrencies*, 06/07/2012 02:17:02 UTC : `https://bitcointalk.org/index.php?topic=91843.msg1011956#msg1011956`.

6. Pour assurer la bonne exécution du contrat (éviter le remplacement de la transaction durant l'attente de confirmation), des clés publiques sont assignées à chacune de ces conditions de sorte qu'une signature est systématiquement demandée au destinataire des fonds.

7. Les adresses des contrats sur LTC et DCR étaient (respectivement) `MLp49daA411aoZ1TmGEdyLuTCE9YA6xhpc` et `DccPF1yt9cV8vhr97fq3umBx7RqV53MYGDY`. L'échange était de 1,337 LTC contre 2,4066 DCR. – *Decred-compatible cross-chain atomic swapping*, 20 septembre 2017 : `https://github.com/decred/atomicswap/blob/master/README.md#first-mainnet-dcr-ltc-atomic-swap`.

8. Joseph Poon et Thaddeus Dryja, *The Bitcoin Lightning Network DRAFT Version 0.5*, 28 février 2015 : `https://lightning.network/lightning-network-paper-DRAFT-0.5.pdf`.

9. Andreas M. Antonopoulos, Olaoluwa Osuntokun, René Pickhardt, « Payment Channels », in *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments*, O'Reilly Media, 2022, pp. 149–184.

10. Christian Decker, Rusty Russell, Olaoluwa Osuntokun, *eltoo: A Simple Layer2 Protocol for Bitcoin*, 30 avril 2018 : `https://blockstream.com/eltoo.pdf`.

11. La transaction `c0b2cf75b47d1e7f48cdb4287109ff1dd5bcf146d5f77a9e8784c0c9c0ef02ad`, confirmée le 13 décembre 2012, contient par exemple la chaîne de caractères `TheCakeIsA Lie\n` en référence au jeu vidéo Portal.

12. Bitcoin Core, *Bitcoin Core version 0.9.0 released*, 19 mars 2014 : `https://bitcoin.org/en/release/v0.9.0#opreturn-and-data-in-the-block-chain`.

13. Ken Shirriff, *Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software*, 16 février 2014 : `https://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html`.

14. Hal Finney, *Re: [bitcoin-list] Bitcoin v0.1.5 released*, 27/02/2009 20:00:12 UTC, archive : `https:`

//web.archive.org/web/20131016004925/http://sourceforge.net/p/bitcoin/mailman/bitcoin-list/?viewmonth=200902.

15. CoinGeek, *Jerry Chan: Bitcoin's value is as a universal source of truth*, 17 juillet 2019 : https://coingeek.com/jerry-chan-bitcoins-value-is-as-a-universal-source-of-truth-video/.

16. Yoni Assia, *bitcoin 2.X (aka Colored Bitcoin) – initial specs*, 27 mars 2012 : https://yoniassia.com/coloredbitcoin/ ; Meni Rosenfeld, *Overview of Colored Coins*, 4 décembre 2012 : https://bitcoil.co.il/BitcoinX.pdf.

17. J.R. Willett, *The Second Bitcoin Whitepaper*, 6 janvier 2012, archive : https://cryptochainuni.com/wp-content/uploads/Mastercoin-2nd-Bitcoin-Whitepaper.pdf.

18. Tous les bitcoins envoyés à l'adresse 1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P étaient transformés en MSC à raison de 100 MSC au début, taux dégressif au fil des semaines.

19. Tous les bitcoins envoyés à l'adresse 1CounterpartyXXXXXXXXXXXXXXXUWLpVr entre le 2 janvier et le 3 février 2014 étaient convertis en XCP à un taux qui variait entre 1 000 et 1 500 XCP par BTC

20. Hal Finney, *Crypto trading cards.*, 17/01/1993 18:48:02 UTC : https://cypherpunks.venona.com/date/1993/01/msg00152.html.

21. Jeff Garzik, *Resist the urge to use block chain for generalized storage*, 07/12/2010 22:04:54 UTC : https://bitcointalk.org/index.php?topic=2129.msg27884#msg27884.

22. BitMEX Research, *The OP_Return Wars of 2014 – Dapps Vs Bitcoin Transactions*, 12 juillet 2022 : https://blog.bitmex.com/dapps-or-only-bitcoin-transactions-the-2014-debate/.

23. pourteaux, *Illegitimate bitcoin transactions*, 25 janvier 2023 : https://read.pourteaux.xyz/p/illegitimate-bitcoin-transactions.

24. Yoni Assia, Vitalik Buterin, Meni Rosenfeld, Rotem Lev, *Colored Coins whitepaper*, 2013 : http://www.ma.senac.br/wp-content/uploads/2018/05/ColoredCoinswhitepaper-DigitalAssets.pdf ; Vitalik Buterin, *A Prehistory of the Ethereum Protocol*, 14 septembre 2017 : https://vitalik.ca/general/2017/09/14/prehistory.html.

25. Andrew Poelstra, *Using the Chain for what Chains are Good For* (vidéo), Scaling Bitcoin IV, 5 novembre 2017 : https://www.youtube.com/watch?v=3pd6xHjLbhs&t=5755s ; Aaron van Wirdum, « *Scriptless Scripts: How Bitcoin Can Support Smart Contracts Without Smart Contracts* », *Bitcoin Magazine*, 27 novembre 2017 : https://bitcoinmagazine.com/technical/scriptless-scripts-how-bitcoin-can-support-smart-contracts-without-smart-contracts.

26. L'acronyme MAST signifie originellement *Merklized Abstract Syntax Trees*, ou « arbre syntaxique abstrait merkélisé » en français, et se réfère aux structures de données décrites par le BIP-114. Dans Taproot, ce ne sont pas vraiment des arbres syntaxiques abstraits qui interviennent, mais le terme reste utilisé. Les arbres de hachage de Taproot peuvent dans ce cas être appelés des *Merklized Alternative Script Trees*, par rétroacronymie. Voir Anthony Towns, *[bitcoin-dev] Safer sighashes and more granular SIGHASH_NOINPUT*, 23/11/2018 05:03:30 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-November/016500.html.

27. RGB FAQ, *What does 'RGB' stand for?*, 14 décembre 2020 : https://www.rgbfaq.com/faq/what-does-rgb-stand-for.

28. Timothy C. May, *The Crypto Anarchist Manifesto*, 22/11/1992 20:11:24 UTC : https://cypherpunks.venona.com/date/1992/11/msg00204.html.

Chapitre 14 – Le passage à l'échelle

1. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

2. James A. Donald, *Re: Bitcoin P2P e-cash paper*, 02/11/2008, 23:46:23 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014814.html.

3. Voir Eric Voskuil, « Propriété du seuil d'utilité », in *Cryptoéconomie : Principes fondamentaux de Bitcoin*, Amazon KDP, 2022, pp. 317–318.

4. Parmi les versions alternatives de Bitcoin, la voie de l'augmentation progressive de la taille limite des blocs a été choisie par Bitcoin Cash, qui prévoit d'intégrer un algorithme permettant de gérer cette augmentation automatiquement. Voir bitcoincashautist, *CHIP-2023-04: Adaptive Blocksize Limit Algorithm for Bitcoin Cash*, 2 septembre 2023 : https://gitlab.com/0353F40E/ebaa/-/blob/f4edacd134103a7e232740463a5f26379bf90f18/README.md.

   Elle a également été favorisée de manière plus conservatrice par Monero, qui possède une taille de bloc dynamique basée sur un mécanisme de pénalité pour compenser les *excès* par rapport à la normale. Voir SerHack, *Mastering Monero: The Future of Private Transactions*, Amazon KDP, 2018, pp. 136–139.

5. Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 03/11/2008, 01:37:43 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html.

6. Voir par exemple l'article de Jameson Lopp sur l'évolution de la performance de Bitcoin Core dans lequel décrit comment la première synchronisation sur sa machine s'est améliorée au cours des années. – Jameson Lopp, *Bitcoin Core Performance Evolution*, 5 mars 2022 : https://blog.lopp.net/bitcoin-core-performance-evolution/.

7. La loi de Moore est une conjecture énoncée par Gordon E. Moore en 1965 ayant postulé que la complexité des semi-conducteurs doublait chaque année. Cette loi était citée par Satoshi Nakamoto dans le livre blanc, qui écrivait : « La loi de Moore prédisant une croissance actuelle de 1,2 Go par an, le stockage ne devrait pas poser de problème même si les entêtes de blocs doivent être conservés en mémoire. » – Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

8. Bitcoin Core, *Bitcoin Core 0.14.0*, 8 mars 2017 : https://bitcoincore.org/en/2017/03/08/release-0.14.0/#assumed-valid-blocks.

9. James O'Beirne, *AssumeUTXO Proposal*, 24 avril 2019 : https://github.com/jamesob/assumeutxo-docs/tree/2019-04-proposal/proposal.

10. Mark Friedenbach, *[soft fork] Block v3: miner commitments with compact proofs*, 28 mars 2014 : https://github.com/bitcoin/bitcoin/pull/3977 ; Pieter Wuille, *[bitcoin-dev] Rolling UTXO set hashes*, 15/05/2017 20:01:14 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-May/014337.html.

11. Cory Fields, *UHS: Full-node security without maintaining a full UTXO set*, 16/05/2018 16:36:35 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-May/015967.html.

12. Thaddeus Dryja, *Utreexo: A dynamic hash-based accumulator optimized for the Bitcoin UTXO set*, 6 juin 2019 : https://eprint.iacr.org/2019/611.pdf.

13. Hal Finney, *Re: Bitcoin Bank*, 30/12/2010 01:38:40 UTC,https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211.

14. « Bitcoin peut être vu comme un système nouveau et émergent de monnaie de réserve pour les transactions en ligne, dans lequel les banques en ligne émettront des jetons adossés au bitcoin pour leurs utilisateurs, tout en gardant leurs réserves en bitcoins dans un stockage hors-ligne. Chaque individu pourra auditer en temps réel les possessions de l'intermédiaire, et des systèmes de vérification et de réputation permettront de s'assurer qu'aucune inflation n'a lieu. » – Saifedean Ammous, *The Bitcoin Standard*, Wiley Publishing, 2018, p. 206.

15. Peter Todd, *Fidelity-bonded banks: decentralized, auditable, private, off-chain payments*, 23/02/2023 17:49:34 UTC : https://bitcointalk.org/index.php?topic=146307.msg1553349#msg1553349.

16. Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, Pieter Wuille, *Enabling Blockchain Innovations with Pegged Sidechains*, 22 octobre 2014 : https://blockstream.com/sidechains.pdf.

17. Paul Sztorc, *Drivechain - The Simple Two Way Peg*, 24 novembre 2015 : https://www.truthcoin.info/blog/drivechain/.

18. Taariq Lewis, *SF Bitcoin Devs Seminar: Scaling Bitcoin to Billions of Transactions Per Day*, 5 mars 2015 : https://www.youtube.com/watch?v=8zVzw912wPo.

19. En pratique, ces HTLC sont souvent aussi utilisés pour mettre à jour les canaux directement, afin de simplifier la mise en œuvre et d'améliorer la confidentialité. – Voir Andreas M. Antonopoulos, Olaoluwa Osuntokun, René Pickhardt, « Routing on a Network of Payment Channels », in *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments*, O'Reilly Media, 2022, pp. 185–207.

20. Le fonctionnement de Fedimint est décrit dans la documentation présente sur le site web : https://fedimint.org/docs/intro.

21. Le fonctionnement technique des systèmes chaumiens a été décrit dans la section « eCash : l'argent liquide chaumien » du chapitre 6.

22. Eric Voskuil, « Principe de substitution », in *Cryptoéconomie : Principes fondamentaux de Bitcoin*, Amazon KDP, 2022, pp. 315–316.

23. Charlie Lee, *Re: [ANN] Litecoin - a lite version of Bitcoin. Be ready when is launches!*, 09/10/2011 06:14:28 UTC : https://bitcointalk.org/index.php?topic=47417.msg564414#msg564414.

24. Satoshi Nakamoto, *Re: BitDNS and Generalizing Bitcoin*, 10/12/2010, 17:29:28 : https://bitcointalk.org/index.php?topic=1790.msg28917#msg28917.

Bibliographie

Ammous, Saifedean. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley Publishing, 2018.

Ammous, Saifedean. *The Fiat Standard: The Debt Slavery Alternative to Human Civilization*. Saif House, 2021.

Antonopoulos, Andreas M. *Mastering Bitcoin: Programming the Open Blockchain*. 2e édition. O'Reilly Media, 2017.

Antonopoulos, Andreas M. *The Internet of Money: A Collection of Talks by Andreas M. Antonopoulos*. The Internet of Money Series. Merkle Bloom, 2016.

Antonopoulos, Andreas M., Osuntokun, Olaoluwa et Pickhardt, René. *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments*. O'Reilly Media, 2022.

Bastiat, Frédéric. *Pamphlets*. Les Belles Lettres, 2009.

Bastiat, Frédéric. *Sophismes économiques*. Les Belles Lettres, 2005.

Bickers, Kiara. *Bitcoin Clarity: The Complete Beginners Guide to Understanding*. Bickers & Son, 2020.

Bier, Jonathan. *The Blocksize War: The Battle Over Who Controls Bitcoin's Protocol Rules*. Amazon KDP, 2021.

Bitcoin and Bible Group. *Thank God for Bitcoin: The Creation, Corruption and Redemption of Money*. Whispering Candle, 2020.

Brunton, Finn. *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton University Press, 2019.

Champagne, Phil. *The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*. e53 Publishing, 2014.

Chaum, David L. « Security without Identification: Transaction Systems to Make Big Brother Obsolete ». In : *Communications of the ACM* 28.10 (oct. 1985), pp. 1030-1044.

Dai, Wei. *b-money*. 26 nov. 1998. url : `http://www.weidai.com/bmoney.txt`.

Favier, Jacques. *La Monnaie à pétales - Bitcoin et le mythe de la tulipe*. PVH Éditions, 2022.

Favier, Jacques, Huguet, Benoît et Takkal-Bataille, Adli. *Bitcoin : Métamorphoses - De l'or des fous à l'or numérique ?* Dunod, 2018.

Favier, Jacques et Takkal-Bataille, Adli. *Bitcoin, la monnaie acéphale*. CNRS Éditions, 2017.

Gigi, Der. *21 Lessons: What I've Learned from Falling Down the Bitcoin Rabbit Hole*. Amazon KDP, 2019.

Greenberg, Andy. *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*. Penguin Publishing Group, 2013.

Hayek, Friedrich A. *Pour une vraie concurrence des monnaies*. Presses Universitaires de France, 2015.

Hoppe, Hans-Hermann. « Banking, Nation States, and International Politics: A Sociological Reconstruction of the Present Economic Order ». In : *The Review of Austrian Economics* 4.3 (1990), pp. 55-87. url : `https://cdn.mises.org/rae4_1_3_3.pdf`.

Hughes, Eric. *A Cypherpunk's Manifesto*. 17 mars 1993. url : `https://cypherpunks.venona.com/date/1993/03/msg00392.html`.

Hülsmann, Jörg Guido. *The Ethics of Money Production*. 2e édition. Ludwig von Mises Institute, 2018.

Konkin, Samuel Edward. *An Agorist Primer*. KoPubCo, 2008.

Konkin, Samuel Edward. *New Libertarian Manifesto*. 4e édition. KoPubCo, 2006.

May, Timothy C. *The Crypto Anarchist Manifesto*. 22 nov. 1992. url : https://cypherpunks.venona.com/date/1992/11/msg00204.html.

May, Timothy C. *The Cyphernomicon*. 10 sept. 1994. url : https://ia600208.us.archive.org/10/items/cyphernomicon/cyphernomicon.txt.

Menger, Carl. *On the Origins of Money*. Ludwig von Mises Institute, 2009.

Mill Hill Books. *Kicking the Hornet's Nest: The Complete Writings, Emails, and Forum Posts of Satoshi Nakamoto, the Founder of Bitcoin and Cryptocurrency*. Lulu.com, 2019.

Morgan, Pamela. *Cryptoasset Inheritance Planning: A Simple Guide for Owners*. Merkle Bloom, 2018.

Mullan, P. Carl. *A History of Digital Currency in the United States*. Palgrave Macmillan, 2016.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 31 oct. 2008. url : https://gwern.net/doc/bitcoin/20081003-nakamoto-bitcoindraft.pdf.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Mars 2009. url : https://bitcoin.org/bitcoin.pdf.

Popper, Nathaniel. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Harper Paperbacks, 2016.

Pritzker, Yan. *Inventing Bitcoin: The Technology Behind the First Truly Scarce and Decentralized Money Explained*. Amazon KDP, 2019.

Provoost, Sjors. *Bitcoin - A Work in Progress: Technical innovations from the trenches*. Purple Dunes, 2022.

ROTHBARD, Murray N. *What Has Government Done to Our Money?* Ludwig von Mises Institute, 1990.

SERHACK. *Mastering Monero: The Future of Private Transactions*. Amazon KDP, 2018.

SZABO, Nicholas J. *Bit gold*. 29 déc. 2005. URL : https://unenumerated.blogspot.com/2005/12/bit-gold.html.

THOORENS, François-Xavier. *Cryptomonnaie - La nouvelle guerre*. Éditions du Cerf, 2021.

VAN WIRDUM, Aaron. *The Genesis Book: The Story of the People and Projects That Inspired Bitcoin*. Bitcoin Magazine Books, 2024.

VINGE, Vernor. *True Names and the Opening of the Cyberspace Frontier*. Tor Publishing Group, 2001.

VOSKUIL, Eric. *Cryptoeconomics: Fundamental Principles of Bitcoin*. Amazon KDP, 2020.

Ordinals

Cet ouvrage est lié à 21 jetons non fongibles (NFT) émis grâce au protocole Ordinals, dont les inscriptions ont pour identifiants :

1) c3ed7ac0cd0bf8586e4e115bf4b5f1a66ad4a2447d2522d6bc71c706d01ddee3i0
2) f9a1f95f7cc9862ca02cdc770565a2766a36b97365417b2a35fc9e0cd399ecaai0
3) b252e48d7d340047b3d1c80de7be9ed5230c235d5f137ddab19829061ec60956i0
4) 19a8d407d37e6c629c0e73fbbd8d30bc7af15d38ca11c389314a6b8d8189fb44i0
5) 7e9415a062dda7d90511aa023143b8c5276d6200efe60bffacb9786d79ac1c07i0
6) 4ae6456348ce94bf1d718488766d99b0d6885e03793a40e29a1d72ced77b6955i0
7) 30214cfa989a2da1cad2d8ba4a38921124b8171815c48eb5f68c14de7a256c26i0
8) ec07ec6ee204b69ec8901f2e0d7745971cef9f5d767bfbbb25adbbd41cf60f68i0
9) b66e1e7f930a1c1ca6b40982cc8df3268cf49c42816acf662db123a890f60456i0
10) 17d4a288947cd581d5f2f0e8b8d85ca4adbad14fdcbc13160d6f86f397a51b5di0
11) cacc4812c50b2fc324f6ebe550b670e2786fbd289fb6368203c81f6103aa42c2i0
12) f0b48c45889400c775f7bae8f20667c30492a944614fc3d643472bc12dc35ab8i0
13) 3d11766b28aceecad850f288765676369161af9c5316032b502e4f71e703917di0
14) 732dddc094b7b2a8ccbdc21eb0c9846ef793ddd93fcae89f36bb39692c9713e9i0
15) 9bf621cc5d3dd725439d0381db287b20ee2f3cd1e26c698941110c96cf32e0efi0
16) d85100401bad5afa5358fff0569f80fde3cdd7fc7ff55027503e739b563dd18ci0
17) bafb8659c6261766123185609235238f29b02aa76ef5963ec834b779fd6aafa7i0
18) 7cf36f6bdc7eddcb669a0977504c5ea505aa959bf7ce03604b7cdf8ea7d98e44i0
19) 9a22171981d2b9ca05ba15673a113169b47d80d472f27ead67e694a08a70c2bbi0
20) aa6f4be48a6ccec912e8a66f469b70d9ce905cd2e22056122b6baa453fb31d22i0
21) de5c7219da2fd9b160e987df7fc818e7db9c8e7f9e168f563f5945a5025c9452i0