Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions

Maël Rolland et Assen Slim

Édition électronique

URL : <http://journals.openedition.org/ei/6023>

DOI : 10.4000/ei.6023

ISSN : 2553-1891

Éditeur

Association Économie et Institutions

Référence électronique

Maël Rolland et Assen Slim, « Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », *Économie et institutions* [En ligne], 26 | 2017, mis en ligne le 03 juillet 2018, consulté le 30 avril 2019. URL : <http://journals.openedition.org/ei/6023> ; DOI : 10.4000/ei.6023

Ce document a été généré automatiquement le 30 avril 2019.

Revue Économie et institutions

Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions

Maël Rolland et Assen Slim

Nous avons proposé un système pour les
transactions électroniques qui ne repose pas sur la
confiance¹

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic
Cash System*, 2008.

Introduction

- ¹ La monnaie n'est pas un outil exclusivement économique. Elle n'est pas détachée des relations sociales existantes. Au contraire, elle est étroitement insérée dans les systèmes politiques, sociaux et culturels dans lesquels elle existe (Polanyi 1944). Elle est légitime parce qu'elle est une convention socialement construite (Aglietta & Orléan 1998 ; Dodd 2014). Dans la monnaie, ce qui se joue, c'est l'unanimité du groupe polarisé sur une même croyance (Orléan 2005), voire la représentation d'un ordre social idéal (Dodd 2007 ; Simmel 1900). En temps de crise, il n'est pas rare de voir émerger des monnaies ou systèmes de paiement alternatifs ayant pour finalité la définition de nouvelles relations de pouvoir et l'établissement de liens sociaux différents entre acteurs (North 2007). L'émergence du Bitcoin en 2009 se fondait explicitement sur l'espoir d'un changement dans les relations de pouvoir au sein de la société. Pour la communauté des *cypherpunks* (ou *crypto-anarchistes*) ayant porté le projet, le Bitcoin est la réalisation de leurs espoirs : préserver la vie privée et l'anonymat en réduisant le contrôle des gouvernements et des firmes sur l'information et les canaux de sa circulation (Chaum 1985 ; May 1992 ; Hughes 1993 ; Dai, 1998). Par extension, le Bitcoin peut aussi être perçu comme la réalisation, voire le dépassement, des ambitions de Von Mises (1912) et Hayek (1990) consistant à mettre fin au monopole des États et des banques centrales dans l'émission et la circulation de la monnaie (De Filippi 2014 ; Lakomski-Laguerre & Desmedt 2015 ; Rolland

& Slim 2015). De fait, un tel système autonomise l'émission et la régulation monétaire et encadre (par le code) la quantité totale d'unités monétaires censées être émises (21 millions d'unités au total) ainsi que sa distribution. Enfin, par les propriétés de son protocole ouvert, transparent et difficilement modifiable, le Bitcoin constitue pour ses promoteurs un projet de plus grande justice sociale en ce sens qu'il évite à la fois toute collusion anti-démocratique entre les représentants du capital et les gouvernements et qu'il rend accessible à tous des services financiers minimums (compte personnel, virements, etc.). Ces différentes représentations du Bitcoin proviennent du fait qu'il est bâti sur un ensemble de règles techniques dont l'ambition est de réaliser une gouvernance sans gouvernement. En d'autres termes, son projet est de se passer d'acteurs tiers, prompts à être corrompus, par le biais de la technologie.

- 2 Mais le Bitcoin relève d'une gouvernance duale (Rolland & Slim 2015 ; De Filippi & Loveluck 2016). À la gouvernance *par* l'infrastructure (interne) se superpose une gouvernance *de* l'infrastructure (externe) concernant le code et ses modifications. C'est sur le consensus interne *par* l'infrastructure que nombre de travaux académiques se sont penchés. Ils se sont intéressés à la fois à son protocole – nommé Bitcoin (avec un grand B) – ainsi qu'à la devise émergente – appelé bitcoin (avec un petit b)². Nous aborderons ici la question sous l'angle de la gouvernance *de* l'infrastructure (appelé aussi « superstructure »), ce qui constitue la principale valeur ajoutée du présent article. On dénombre quelques rares travaux s'étant intéressés au sujet, qu'ils partent d'une démarche sociologique (De Filippi 2014 ; De Filippi & Loveluck 2016) ou bien institutionnaliste monétaire (Lakomski-Laguerre & Desmedt 2015 ; Rolland & Slim 2015). De telles grilles d'analyse contribuent à montrer que le Bitcoin est un espace institutionnel, un construit sociotechnique (au sens où il est formé par des acteurs, des réseaux, des représentations) et qu'il n'est aucunement exempt de jeux de pouvoir. Constat paradoxal pour un Bitcoin dont l'ambition initiale des promoteurs était précisément de se prémunir contre ces derniers, en reléguant la superstructure au plan technique d'une infrastructure conçue comme autonome. Ce projet, pour ambitieux qu'il soit, questionne : est-il possible de construire un système sociotechnique déconnecté de son contexte social, culturel et politique ?
- 3 Une première partie est consacrée à l'infrastructure technique du Bitcoin, depuis sa genèse jusqu'à son fonctionnement actuel. Cette infrastructure est censée éliminer le recours à un tiers de confiance et assurer une gouvernance autonome du Bitcoin. Toutefois, une deuxième partie montre qu'elle n'y parvient pas complètement. La dimension institutionnelle et politique du Bitcoin devient particulièrement visible lorsqu'émergent des débats quant au développement et à l'évolution de ladite infrastructure. Il existe ainsi une superstructure composée, entre autres, d'une poignée de développeurs hautement qualifiés et d'ingénieurs informatiques ayant le pouvoir de faire évoluer l'infrastructure du Bitcoin (De Filippi & Lovelock 2016). Le Bitcoin peut alors apparaître comme ambivalent puisque d'un côté il échappe au contrôle de toute autorité centrale, mais de l'autre il garde une structure de gouvernance qui peut sembler fortement technocratique. Toutefois, ces développeurs, formant un groupe hétérogène, doivent composer en permanence avec les utilisateurs qui peuvent adhérer ou non à leurs décisions. S'établit alors un jeu complexe de rapports de force entre les parties en présence dont le résultat est l'édification progressive de structures visant à réaliser des objectifs collectifs, gérer les conflits et contrôler les relations de pouvoir. Ce processus en

cours, en assurant la légitimité des actions décidées collectivement, garantit pour le moment la viabilité du Bitcoin.

1. L'infrastructure technique du Bitcoin

- 4 Bitcoin a été pensé par ses fondateurs comme un système de paiement « sans confiance »³, au sens où la confiance ne reposerait plus sur un tiers (autorités monétaires, institutions bancaires et financières). Il est l'aboutissement d'une réflexion libertarienne ancienne qui affiche une défiance contre toute autorité centrale et qui, paradoxalement, peut être rapprochée de la thèse du *Free Banking* développée par Von Mises et Hayek (1.1. La genèse du Bitcoin). La confiance est censée être garantie par une infrastructure technique originale et sophistiquée reposant sur un réseau décentralisé de pair-à-pair avec un protocole cryptographique, une chaîne de blocs (appelée *Blockchain*) et une activité de minage (1.2. Une infrastructure technique).

1.1. La genèse du Bitcoin

- 5 Le projet d'un système de paiement affranchi de toute institution centrale trouve son origine dans la pensée libertarienne développée dans les années 1980 par les courants *cypherpunk*⁴ et *crypto-anarchiste*⁵. Ces courants accordent une importance très grande à l'anonymat⁶. À la fin des années 1980, les *crypto-anarchistes* voient dans l'évolution des technologies (*hardwares* et *softwares*) et dans la possibilité de développer la cryptographie à grande échelle, le moyen de mettre fin à l'omniprésence des contrôles étatiques. Chaum lance alors la première tentative de cryptomonnaie, nommée *Digicash*, afin d'explorer les possibilités offertes par la cryptographie (Chaum 1985). À l'issue de cette première expérience, Dai, fasciné par le projet de la crypto-anarchie de May, présente dans une brève note sa *b-money* : une monnaie qui pourrait être échangée de pair-à-pair, dans un système décentralisé, fondé sur un réseau non traçable du fait de l'utilisation de clés cryptographiques. Un pas de plus vers l'obsolescence de gouvernements rendus inutiles⁷. Et May d'annoncer l'avènement prochain de « marchés parfaits » totalement liquides et anonymes (May 1992). Se succèdent alors plusieurs projets de cryptomonnaies dont le *Bitgold* (Szabo 2005). Ces projets ont en commun de reposer non seulement sur la cryptographie mais également sur un système distribué d'échange de l'information (dit pair-à-pair). Ils préparent l'arrivée du Bitcoin.
- 6 Paradoxalement, la défiance des *crypto-anarchistes* vis-à-vis de toute autorité centrale et leur croyance dans la primauté des rapports interindividuels les rapprochent du courant libéral autrichien qui met l'accent, depuis Menger (1871), sur l'individualisme méthodologique, la subjectivité de la valeur, l'importance des signaux envoyés par le marché et la responsabilité des États dans la survenue de crises économiques. À la suite de Menger, les auteurs relevant de ce courant ont considéré que seul le marché était en mesure d'envoyer les bons signaux (prix, taux d'intérêt, etc.) permettant aux agents économiques de réaliser leurs calculs économiques et de choisir des plans d'actions cohérents (Von Mises 1912). Toute manipulation artificielle de l'offre de monnaie par les autorités se traduirait par des niveaux de prix et taux d'intérêt incohérents et conduirait les agents économiques à valider des plans d'action inadaptés aux besoins de la société. La thèse du *Free Banking* est l'une des options (l'autre étant le régime de l'étalon-or) imaginée par les économistes de ce courant pour limiter l'offre de monnaie. Dans cette approche, la

monnaie est une marchandise comme une autre et doit être gérée directement par le marché, ce dernier étant le lieu où s'exerce la concurrence directe entre banques privées, sans recours à aucune banque centrale. Le marché sans entrave apparaît alors comme le mécanisme par lequel les mauvais acteurs sont sanctionnés et les acteurs vertueux récompensés. L'autorégulation de l'offre de monnaie est ainsi assurée et sans intervention d'un gouvernement ou d'une banque centrale (Hayek 1976). D'après Hayek, le droit « illégitime » dont disposerait l'État en matière de monnayage (émission de monnaie, taux, règles d'usage) disparaîtrait par la mise en concurrence de toutes les monnaies privées entre elles. L'échange marchand est ici réduit aux seules relations interindividuelles contractuelles hors de toute épaisseur sociale. Depuis le lancement en 2009 du bitcoin par Satoshi Nakamoto, plus de mille trois-cent-vingt autres cryptomonnaies ont vu le jour⁸. Dréan y voit « un processus de sélection naturelle des monnaies analogue à ce que propose Hayek dans *The Denationalization of money* » (Dréan 2013).

1.2. Une infrastructure technique distribuée

- 7 Le Bitcoin a été conçu pour offrir « un nouvel espace de liberté » via son infrastructure technique (Nakamoto 2008). Cette gouvernance interne par l'infrastructure est censée générer de la confiance en se passant de toute autorité centrale (De Filippi & Loveluck 2016).
- 8 Le protocole du Bitcoin est distribué de manière à éliminer les points uniques de contrôle et renforcer la résilience de l'ensemble du système. Il repose sur la cryptographie asymétrique à double clé. Cela permet en principe de garantir le pseudonymat des parties prenantes, tout en rendant impossible la falsification des identifiants et des montants de bitcoins inscrits dans les porte-monnaie électroniques (*wallets*) des utilisateurs. Lors d'un paiement, l'émetteur signe et authentifie son ordre de paiement avec sa clé privée. Le bénéficiaire du règlement recevra les sommes envoyées sur sa propre adresse si cette clé correspond à la clé publique diffusée par l'émetteur pour décrypter le transfert et en authentifier l'origine sans pour autant révéler l'identité des acteurs.
- 9 La chaîne de blocs (ou *blockchain*) correspond, quant à elle, à un historique de toutes les transactions traitées et validées par le système Bitcoin depuis sa création. Toute transaction validée est placée dans un nouveau bloc (une sorte de page de transactions⁹) qui est intégré à la chaîne de blocs¹⁰. Cette dernière est répliquée à l'identique dans certains ordinateurs du système, appelés des « nœuds complets ». Il n'existe, en effet, pas un mais plusieurs milliers d'exemplaires de la chaîne de blocs, construits et gérés par autant d'ordinateurs sur toute la planète. Les « nœuds complets » maintiennent à jour un exemplaire de la chaîne de blocs, téléchargent et vérifient la validité des nouveaux blocs aux règles reconnues par tous, puis les diffusent sur le réseau. Il existe également des « nœuds légers », utilisés par des services ou portefeuilles qui, pour des raisons pratiques, ne téléchargent pas la totalité des informations contenues dans la chaîne des blocs. Ces derniers ne jouent donc pas de rôle direct dans la vérification des nouveaux blocs. En retenant la chaîne de blocs qui respecte les critères de validité reconnus par la majorité et dont la construction a demandé la plus grande somme de travail, le protocole produit un consensus et dissuade les fraudeurs éventuels en exigeant d'eux un travail supérieur à celui des membres du système.

- 10 Le minage, enfin, par résolution de « preuves de travail » (ou PoW ou *Proof of Work*), correspond à l'étape où les nouvelles transactions émises sont validées et inscrites dans un nouveau bloc s'ajoutant à la chaîne de blocs. Il est réalisé par des « mineurs », des utilisateurs volontaires qui, en plus de maintenir des nœuds complets, sont dotés de logiciels particuliers permettant de réaliser les nouveaux blocs. Les blocs qu'ils émettent sont diffusés par et via les autres nœuds complets, qui peuvent en vérifier facilement l'authenticité. Lorsqu'un mineur résout le premier la PoW (et qu'il a donc prouvé l'authenticité de toutes les transactions inscrites dans le bloc), sa solution est diffusée à tous les autres mineurs qui la valident et enregistrent la nouvelle chaîne de blocs augmentée en lieu et place de la leur. Cette procédure qui dure environ dix minutes permet d'éviter les problèmes de double dépense frauduleuse des mêmes bitcoins (*double spending problem*). Les mineurs sont en concurrence les uns avec les autres pour la résolution de chaque PoW. Leur chance de trouver la bonne solution avant les autres dépend directement de la puissance qu'ils y dédient, relativement à la puissance totale cumulée dans le réseau. Les mineurs sont « rémunérés » en nouveaux bitcoins émis pour le travail accompli et pour les ressources mobilisées. À l'origine, 50 bitcoins étaient émis toutes les dix minutes, mais cette émission est divisée par deux tous les 210 000 blocs émis (soit tous les quatre ans environ). Depuis juillet 2016, seuls 12,5 bitcoins sont émis toutes les dix minutes environ¹¹. C'est ce protocole, avec son maintien, qui se fait monnayage crédible, assurant une création monétaire limitée et transparente (quantité, rythme de croissance et modalités de distribution sont connus de tous).
- 11 L'infrastructure technique du Bitcoin, en vertu de ses présupposés de décentralisation (absence d'attaquant ayant plus de 51 % de la puissance totale du réseau) est efficace, sûre, difficilement censurable et corruptible. Elle permet l'interaction directe entre les individus sans aucun recours à un tiers. Elle exclut toute forme de coercition. Les coûts de transaction sont quasiment nuls et les délais réduits. C'est à cette infrastructure technique que l'essentiel de la littérature académique sur le Bitcoin s'est intéressé. Certains ont étudié ses propriétés et tenté d'en mesurer les implications économiques et monétaires (Ali *et al.* 2013 ; Yermack 2013 ; Böhme *et al.* 2015). D'autres ont porté leur attention sur les propriétés mathématiques de l'infrastructure du Bitcoin (Delahaye 2014). D'autres encore se sont intéressés à la sécurité de son protocole (Karame *et al.* 2012) ou à la garantie de pseudonymat et aux moyens de contourner celui-ci (Meiklejohn *et al.* 2016). Un vaste pan de la littérature a aussi porté plus spécifiquement sur les problèmes posés par l'encadrement légal du Bitcoin et des autres cryptomonnaies, plateformes et pratiques auxquelles le Bitcoin a ouvert la voie (Walch 2017). Les risques et les enjeux macroéconomiques de telles cryptomonnaies ont également été analysés (Aglietta *et al.* 2014 ; ECB 2012 et 2015 ; Raskin *et al.* 2016). Enfin, plusieurs travaux se sont intéressés exclusivement à la chaîne de blocs et à ses multiples applications, y compris par les banques centrales elles-mêmes (Danezis *et al.* 2015 ; Raskin *et al.* 2016 ; Koning 2017).
- 12 Mais ne s'intéresser au Bitcoin que sous l'angle de sa gouvernance par l'infrastructure reviendrait à passer à côté de l'essentiel. Car, contre l'attente même de ses concepteurs, une gouvernance par l'infrastructure conduit, comme elle contraint, à l'émergence d'une gouvernance de l'infrastructure. Cette dernière devient visible lorsqu'il s'agit de faire évoluer l'infrastructure technique. Redéfinir les moyens mobilise par essence une perception de fins, de contraintes et d'opportunités qui sont socialement situées. Problèmes et solutions prennent alors place hors du champ de la technique, au sein d'espaces de débats et de prise de décision socialement construits et organisés.

2. La gouvernance de l'infrastructure du Bitcoin : un équilibre fragile

- ¹³ La gouvernance par l'infrastructure du Bitcoin suppose une gouvernance de l'infrastructure, extérieure et sociale. Se pose alors la question de sa structure et de sa capacité à apporter des réponses à des problématiques relevant de coordination non uniquement technique. En repartant des quelques articles ayant traité la gouvernance de l'infrastructure du Bitcoin dans sa dimension institutionnelle de construit socio-politique (2.1. La question de la gouvernance de l'infrastructure au prisme des corpus existants), il apparaît qu'une institutionnalisation du Bitcoin est à l'œuvre (2.2. De la gouvernance complexe de l'infrastructure du Bitcoin : une institutionnalisation et ses acteurs). Bien que singulière, c'est bien une forme de gouvernance qui se donne à voir, avec sa définition particulière des rôles et statuts des acteurs, ses modalités propres de résolution des conflits, ses luttes de pouvoir entre parties prenantes pouvant, le cas échéant, déboucher sur des scissions de la communauté (*forks*) (3. Le débat sur la taille des blocs, entre recherche de consensus et émancipation monétaire).

2.1. La question de la gouvernance de l'infrastructure au prisme des corpus existants

- ¹⁴ On peut partir des outils de l'institutionnalisme monétaire pour étudier le Bitcoin afin d'en souligner la dimension institutionnelle et construite. Comme tout autre espace monétaire, le Bitcoin se doit d'entraîner des formes d'adhésion collective (Lakomski-Laguerre & Desmedt 2015 ; Rolland & Slim 2015). Ainsi Lakomski-Laguerre et Desmedt, par exemple, montrent que le Bitcoin correspond bien à une monnaie conçue comme un système de paiement au sens de Cartelier (1996) et Aglietta & Cartelier (1998)¹² : il fonde une unité de compte propre, dont il organise et régule l'émission ; il fournit un cadre de résolution des transactions entre membres (paiement et règlement se dénouant ensemble, aucune procédure spécifique de résolution des dettes n'est requise). Définissant la confiance comme un construit social à trois niveaux (méthodique, hiérarchique et éthique) au sens d'Aglietta et Orléan (1998) et de Théret (2008)¹³, Lakomski-Laguerre et Desmedt dégagent une articulation particulière à l'œuvre dans le Bitcoin : son protocole, qui ambitionne de s'extraire de toute relation verticale et de son pendant de confiance hiérarchique, semble encastrent toutes les confiances dans son code et ses propriétés. Mais se pose alors la question du maintien d'une confiance éthique homogène dans le temps, alors même que la communauté des utilisateurs s'est élargie, en une décennie, bien au-delà des groupes *cypherpunks* et *crypto-anarchistes*, provoquant une dilution de la philosophie libertarienne des origines. Cette confiance éthique pourrait se maintenir à condition que des principes et des valeurs communs continuent d'être partagés au sein de la communauté de paiement évolutive du Bitcoin. Blanc (1998) rappelle qu'une « communauté de paiement » (conceptualisée par Knapp en 1905) qualifie un groupe d'acteurs s'identifiant au système monétaire national et partageant des principes communs de résolution des dettes. Les groupes monétaires sont des sous-ensembles hiérarchiquement insérés dans la communauté de paiement. Ils en respectent les principes mais peuvent aussi refuser d'employer certains instruments monétaires au profit d'autres qui leur sont spécifiques. Il faut souligner ici que la communauté de

paiement du Bitcoin (et des autres cryptomonnaies) n'est pas limitée à l'espace national mais s'étend à un espace défini techniquement.

- 15 La démarche sociologique de De Filippi et Loveluck (2016) complète l'analyse en s'intéressant aux modalités de coordination existantes au sein du Bitcoin. Les auteurs partent de l'idée que ce dernier, comme toute innovation, est une construction sociotechnique au sens de Akrich (1989), c'est-à-dire qu'il combine plusieurs types d'arrangements différents (incluant des normes sociales, des règles et procédures formelles et informelles, des pratiques de marché et des solutions techniques) qui, tous ensemble, constituent à la fois sa gouvernance et ses structures de pouvoir. Or, d'après les auteurs, « les systèmes sociotechniques ne peuvent pas, du fait de leur intégration dans un contexte social et culturel, assurer leur propre autonomie et leur autosuffisance grâce à la seule technologie » (De Filippi & Loveluck 2016, p. 18). Il existerait donc une « superstructure » qui interagirait avec l'infrastructure afin de répondre à trois problématiques critiques : (i) définir et protéger les frontières de sa communauté ; (ii) établir des incitations à la participation des membres et leur reconnaître des statuts (iii) pacifier les conflits (Auray, 2012). La superstructure est perçue par De Filippi et Loveluck comme scindée en deux groupes distincts : celui des nœuds passifs (utilisateurs) et actifs (mineurs) et celui de quelques développeurs (*core developers*) en mesure d'apporter des modifications directes à l'infrastructure du Bitcoin. Ces deux groupes ont leurs propres frontières et leurs propres mécanismes de coordination (incitation, protection, résolution de conflits). Toutefois, d'après les auteurs, les « crises » de gouvernance du Bitcoin seraient la marque des difficultés d'établissement d'une structure de gouvernance apte à jouer le rôle d'interface équilibrant ces différentes dimensions (De Filippi & Loveluck 2016).
- 16 La grille d'analyse de De Filippi et Loveluck (2016) est précieuse, car elle pose très clairement les différents enjeux liés à la gouvernance d'un tel protocole. Toutefois, la conclusion des auteurs consistant à dire que la superstructure du Bitcoin est « technocratique » du fait que seuls quelques développeurs ont la main sur l'infrastructure nous paraît erronée. D'abord, parce que le groupe de développeurs est plus hétérogène que ce qu'en perçoivent De Filippi et Loveluck. Il est hétérogène en intérêts, en valeurs et en représentations. Il connaît, de plus, des recompositions. Ensuite, parce que ce groupe doit convaincre les autres membres actifs du réseau, qui peuvent le cas échéant refuser les éventuelles mises à jour. Les mineurs (par les récompenses qu'ils obtiennent), et plus généralement les nœuds complets, sont les plus intéressés par une éventuelle modification du protocole. C'est donc eux qu'il faut convaincre. Les débats sur la mise à l'échelle du protocole (l'enjeux de « scalabilité »), communément qualifiés de débats sur la taille des blocs, entamés en 2015 et qui se poursuivent avec une intensité redoublée jusqu'à nos jours, témoignent du caractère non « technocratique » de la superstructure du Bitcoin.

2.2. De la gouvernance complexe de l'infrastructure du Bitcoin : une institutionnalisation et ses acteurs

- 17 Comme toute gouvernance, celle du Bitcoin est censée définir et réaliser les objectifs collectifs, gérer les conflits, contrôler les relations de pouvoir et apparaître légitime aux yeux des autres parties prenantes. Le Bitcoin repose, comme on l'a vu, sur un protocole bien défini, qui dispose de ses propres modalités techniques de résolution des conflits. Un

« conflit » au niveau de l'infrastructure technique correspond à l'émergence sur le réseau de deux blocs alternatifs, valides l'un et l'autre, et créant deux versions concurrentes de la chaîne de blocs. Le protocole du Bitcoin dispose alors d'une stratégie automatique de choix en faveur de la chaîne de blocs la plus lourde en calculs et dont les blocs respectent les règles reconnues par la majorité des nœuds. En cela, faire évoluer le protocole semble impossible en l'absence d'un consensus fort au sein de la communauté. Bien que le Bitcoin soit un projet *open source*, le développement et la maintenance de l'infrastructure technique du Bitcoin dépendent, ultimement, d'un nombre restreint de développeurs hautement qualifiés. Mais, s'ils font bien partie de la gouvernance de l'infrastructure (comme précisé par De Filippi & Loveluck 2016), il ne faudrait pas croire qu'ils ont tout pouvoir. En effet, si dans la pratique ce sont bien ces derniers qui ont la main sur le protocole, il faut encore qu'ils arrivent à convaincre les autres groupes de la communauté du bien-fondé de leurs décisions. Rien ne garantit que les mineurs et les autres nœuds complets, par exemple, accepteront la nouvelle version logicielle et ses nouvelles propriétés. Cela implique des débats et la recherche d'un consensus plus ou moins difficile à atteindre selon l'ampleur des modifications envisagées. Certaines améliorations sont mineures, impliquant de nouvelles fonctionnalités sans remettre en cause les règles de consensus suivies par les mineurs, tandis que d'autres sont plus importantes et peuvent affecter lesdites règles de consensus débouchant alors sur des *soft forks* ou des *hard forks* qui n'entraînent pas les mêmes implications (voir Annexe 1). Le Bitcoin se présente alors comme un véritable écosystème¹⁴ reposant sur des acteurs distincts à rôle spécifique (développeurs, mineurs, nœuds complets, utilisateurs, services marchands) (2.2.1. Acteurs et groupes composant la superstructure : une communauté de paiement hétérogène) et des procédures, règles et médias qui encadrent et donnent forme au consensus structurant la gouvernance de l'infrastructure (B).

2.2.1. Acteurs et groupes composant la superstructure : une communauté de paiement hétérogène

- 18 En tant que protocole sans confiance (« *trustless* »), le Bitcoin n'appartient à aucune organisation formelle. Aucune entité n'a le pouvoir d'imposer directement aux autres membres ses règles de consensus puisque celles-ci sont intégrées dans le code logiciel choisi par les membres du réseau. La dimension hautement technocratique soulignée par De Filippi et Loveluck (2016) résulte en partie d'une erreur d'appréciation des frontières des groupes composant la communauté. Il convient donc de bien définir les parties prenantes en présence.
- 19 Le groupe des développeurs du Bitcoin est responsable du contrôle et de l'amélioration du protocole. D'après De Filippi et Loveluck (2016), la structure organisationnelle de ce groupe serait « autocratique-mécanistique », c'est-à-dire que les décisions y seraient prises de manière très centralisée (par opposition à une organisation « organique-démocratique »). De fait, depuis sa mise en place en 2009 et jusqu'à son retrait en 2011, c'est Satoshi Nakamoto, « le » fondateur, qui avait la charge du projet. En « dictateur philosophique », il a conçu les règles originelles du protocole, fut le mineur du « genesis block »¹⁵, et si d'autres l'ont rapidement épaulé, il détenait seul l'accès au répertoire originel de dépôt des codes¹⁶. En se retirant, Satoshi Nakamoto a pris le soin de transférer le contrôle sur le code source du Bitcoin à Gavin Andresen, l'un des contributeurs principaux durant ces premières années. Ce dernier a élargi les droits sur le code source du répertoire Bitcoin.org à un petit groupe de développeurs connu sous le nom de «

bitcoin core ». Mais ce groupe connaît des recompositions durant lesquelles d'anciens membres peuvent se voir retirer leurs droits tandis que de nouveaux peuvent en être dotés. Alors que le groupe formé en 2011 comprenait Jeff Garzik, Gregory Maxwell, Wladimir van der Laan, Pieter Wuille et Mike Hearn, celui détenant les droits d'accès du dépôt Github Bitcoin Core au début de 2018 était composé de Jonas Schnelli, Pieter Wuille, Wladimir van der Laan et Marco Falke. Ces recompositions sont la plupart du temps le résultat d'oppositions (parfois violentes) sur des projets aux vues et philosophies différentes. Une hiérarchie existe au sein de ce groupe de développeurs. On y distingue : les responsables du répertoire qui sont chargés de fusionner les demandes émergentes, les responsables principaux (en charge du cycle de publication, de la fusion globale, de la modération et de la nomination de nouveaux responsables) et les autres développeurs. Tous les acteurs du Bitcoin peuvent proposer des modifications à condition de respecter les procédures ouvertes¹⁷. Les développeurs du code du protocole lui-même cohabitent aussi avec (voire sont eux-mêmes) des développeurs d'applications et logiciels reposant sur le protocole (services de paiement, bourses, marchands, etc.), les compétences techniques n'étant pas les mêmes. En définitive, le groupe des développeurs apparaît hétérogène (des intérêts antagonistes peuvent y voir le jour) et mouvant (recompositions régulières au fil des débats et propositions). Enfin, ce groupe ne peut imposer aucune modification des règles de consensus sans l'adhésion des mineurs, des nœuds complets et des utilisateurs. Ces derniers disposent de l'équivalent d'un droit de veto car ils sont libres de ne pas retenir les modifications réalisées. Par conséquent, pour rendre légitime leur proposition de modification, les développeurs sont dans l'obligation de trouver des relais chez les autres membres de la communauté. Sans un minimum de confiance éthique (jugement de valeur sur ce qu'induisent les modifications) et hiérarchique (confiance dans le projet et dans les compétences des personnes qui le portent), il ne peut y avoir aucune modification, car la majorité des nœuds peut tout refuser.

- 20 Les nœuds structurant le réseau comprennent les mineurs et plus largement les nœuds complets. Les mineurs, comme on l'a vu, sont responsables du minage qui est le cœur de la « décentralisation », de la « démocratie » et de la sécurité du protocole. Chaque mineur est incité à ajouter de la capacité de calcul afin d'augmenter ses chances de rémunération, ce qui se traduit corrélativement par une augmentation de la sécurité. Toutefois, l'activité de minage s'est industrialisée, conduisant à une course à la machine la plus puissante et provoquant une certaine centralisation. Alors que de simples ordinateurs de bureau suffisaient pour miner il y a encore quelques années, il faut désormais des équipements spécifiques dédiés permettant d'optimiser la quantité de calculs par énergie consommée¹⁸. En se professionnalisant, l'activité de minage se concentre, ce qui contribue à ériger des barrières à l'entrée pour les nouveaux mineurs. Des *pools*¹⁹ de mineurs se sont constitués, permettant à ces derniers de mutualiser leur puissance de calcul et d'augmenter ainsi leurs chances dans la course à la résolution des blocs. Le groupe des mineurs n'est pas non plus homogène. On trouve en son sein deux grandes catégories : les *hashers*, amateurs ou professionnels, qui mettent leur puissance de calcul à disposition d'un *pool* de minage qui les rémunère au prorata de leur participation ; et les *opérateurs de pools* qui génèrent le processus de minage, choisissent la version logicielle qu'ils utilisent et rémunèrent leurs *hashers*. Les opérateurs de pools disposent d'un grand pouvoir. Intéressés au protocole, se trouvant dans une position oligopolistique²⁰, ils seraient en mesure d'imposer leurs intérêts en proposant des modifications du protocole. Ils doivent toutefois eux-mêmes composer avec les *hashers* qui leur fournissent leurs capacités de calcul et qui peuvent, en cas de désaccord, quitter un pool pour en rejoindre un autre. Les mineurs (opérateurs de

pool et *hashers*) doivent également tenir compte des intérêts et du pouvoir d'influence des fabricants de matériels de minage. Peu de firmes proposent des ASIC. Bitmain, entreprise chinoise, est le leader sur le marché. En plus de fabriquer des composants, cette entreprise détient des pools et des mineurs. Ainsi, Bitmain et son PDG ont pris activement part aux négociations concernant les évolutions logicielles. Bitmain est également soupçonné d'avoir utilisé dans ses pools un processus technique permettant de miner plus rapidement (« Asic-Boost »²¹).

- 21 Enfin, les mineurs sont les acteurs actifs du réseau, mais ils ne sont pas les seuls et les nœuds complets doivent être considérés (Loop 2014 ; Maderia 2017 ; Janssen 2017). Ces nœuds complets permettent aux membres du réseau qui les possèdent de vérifier que les nouveaux blocs respectent bien les conditions de consensus reconnues par tous. Vecteurs de sécurité, individuelle et collective, ils permettent aux nouveaux blocs de se diffuser rapidement et de manière homogène dans le réseau. Ils deviennent un outil de vote et de blocage contre des blocs qui imposeraient de nouvelles propriétés aux transactions, puisque ces blocs ne seraient pas suffisamment diffusés pour pouvoir devenir l'historique consensuel sur lequel les autres mineurs travailleront.
- 22 De fait, tous les autres acteurs de la communauté (utilisateurs, marchands, fournisseurs de services, fonds d'investissement, etc.) seront actifs s'ils maintiennent eux-mêmes leurs propres nœuds complets. Tous ceux qui utilisent des services reposant sur les nœuds complets d'autres acteurs sont alors inactifs en ce sens qu'ils délèguent la définition de la validité des blocs à d'autres, en qui ils ont confiance. C'est le cas, par exemple, des utilisateurs de portefeuilles légers (dits SPV pour *Simplified Payment Verifications*)²² ne reposant pas sur un nœud complet propre. Mais là encore, un utilisateur inactif pourrait « activement » changer de fournisseur de services pour sanctionner un choix qu'il désapprouverait.
- 23 Il est important de comprendre les frontières de cette communauté comme les possibilités stratégiques ouvertes par chacun des statuts qui la composent. Cette gouvernance de l'infrastructure repose sur une balance de pouvoirs (personne n'en est totalement privé) et pose le problème de l'obtention d'un consensus large, traversant toutes ces strates communautaires. En pratique, a émergé un cadre institutionnel permettant à l'ensemble de cette communauté de rechercher de tels consensus par la mise en place de procédures de discussion et de résolution des conflits, même si tous ne sont pas pacifiés.

2.2.2. La mise en place d'institutions d'expression des désaccords

- 24 Un « conflit » au niveau de la superstructure ne peut pas être résolu par les mécanismes de résolution des conflits à l'œuvre dans l'infrastructure, dans la mesure où il n'est pas technique, mais socio-économique. Or, pour préserver la légitimité des règles automatiques de l'infrastructure, il est vital pour le Bitcoin de se doter d'une superstructure capable de réaliser une coordination sociale. Il s'agit d'institutionnaliser des procédures permettant de faire émerger un consensus autour de propositions de modification du protocole. Ces procédures vont de la normalisation des propositions à leur discussion *via* des canaux spécifiques, en passant par leur vote par signalement en vue d'implémentation.
- 25 L'instauration d'un mécanisme d'arbitrage s'avère essentielle en cas de divergence d'opinions relatives aux modifications à apporter à l'infrastructure du Bitcoin. Ce

mécanisme peut être soit interne, soit externe à la superstructure. L'exemple des Propositions d'Amélioration du Bitcoin (ou *BIPs* pour *Bitcoin Improvement Proposals*), lancées en 2011 suivant la proposition d'un développeur²³, va dans ce sens²⁴. Les *BIPs* correspondent à une recherche de consensus entre toutes les parties prenantes du Bitcoin. Toute modification de l'infrastructure proposée par un développeur doit, au préalable, être diffusée à l'ensemble de la communauté via le répertoire GitHub²⁵, et ce afin de recueillir la discussion la plus large possible. Les *BIPs* doivent donner des informations techniques concises sur la modification, ses propriétés et sa mise en application. Ce mécanisme d'arbitrage permet, en l'absence d'une structure formalisée dans le protocole lui-même, de proposer de nouvelles fonctionnalités, de faire remonter les avis et problèmes de la communauté, tout en documentant la prise de décision qui a conduit au code du Bitcoin reconnu par la grande majorité. Il est un outil de proposition, d'évaluation par les pairs, de débats, d'amendement et de consignation à vue dans la plus grande transparence. Les *BIPs* relèvent, dans leurs constructions et leurs pratiques, d'une forme instituée de résolution des conflits, permettant de déplacer les problèmes sur un champ procédural ordonné et de limiter ainsi la survenue de conflits personnels, voire d'attaques *ad hominem* (les développeurs peuvent y intervenir sous pseudonyme).

- 26 Une autre procédure est fournie par l'usage des réseaux sociaux, utilisés comme des supports de la superstructure pour donner forme aux débats. Sur GitHub, le débat a lieu entre développeurs. Des *BIPs* alternatives, voire opposées, y sont discutées. De nombreuses autres plateformes²⁶ hébergent les débats entre toutes les parties prenantes, et pas seulement les développeurs. Elles constituent autant de relais politiques à l'expression des vues des groupes sociaux composant la communauté Bitcoin. Émergent alors des hiérarchies entre les intervenants, des faiseurs d'opinions, des jeux de pouvoir, des attaques (*trolling*, achat de *retweet*, compte multiple, etc.). Sur certaines plateformes, des modérateurs peuvent exercer une forme de censure à l'encontre de participants défendant des arguments différents... Mais l'usage qui est fait des réseaux sociaux relève bien d'une forme instituée d'expression des groupes sociaux co-décisionnaires.
- 27 Une autre procédure est donnée par les rencontres physiques qui ont pu être organisées entre les différentes parties prenantes²⁷. Elles servent autant à la discussion de projets différents qu'à la construction même des communautés qui les portent, forgeant des représentations communes. Dans l'espace public, si les personnes/entités participantes sont identifiées, des attaques plus importantes peuvent être constatées (attaques informatiques, dénonciation policière fallacieuse, etc.).
- 28 Enfin, une procédure qui s'apparente à un vote permet aux nœuds de signaler leurs soutien ou non à une modification qui aurait été ainsi débattue. Cette procédure, mise en place par la *BIP 9*²⁸, permet de définir un laps de temps (exprimé en nombre de blocs) après lequel une mise à jour sera enclenchée à condition qu'elle ait reçu le soutien de suffisamment de nœuds (un *quorum* étant défini dans la proposition *BIP*).
- 29 Toutes ces procédures agissent comme des formes instituées de gouvernance. Elles se renouvellent au gré des besoins. Des intérêts divergents s'y manifestent, des visions opposées y sont débattues et des projets différents y rentrent en concurrence. Il existe donc bien une dimension politique du Bitcoin qui ne peut être réduite à son seul protocole. À ce titre, les débats sur la taille des blocs en constituent une bonne illustration, car ils attestent du fait que le Bitcoin n'échappe pas à son contexte socio-économique.

3. Le débat sur la taille des blocs, entre recherche de consensus et émancipation monétaire

- 30 Une superstructure doit être en mesure de définir des objectifs collectifs et de les réaliser, de gérer et de trouver des solutions pacifiques aux conflits, de contrôler les relations de pouvoir et d'asseoir la légitimité des règles qu'elle crée ou modifie. La présence de conflits de différentes formes, entraînant des consensus lents, ne relève pas d'une gouvernance défailante, voire pathologique. Avec le succès grandissant du Bitcoin, le nombre d'utilisateurs a grossi, ainsi que les intérêts économiques qui en soutiennent l'usage. Des visions différentes se sont développées et les conflits qui en résultent traduisent la socialisation en cours d'une communauté. L'objet du conflit est bien un élément de dissociation, mais il est aussi un élément de résolution, même si cela doit passer par la séparation des parties : la nécessité du conflit est son surpassement, afin de maintenir l'unité, forgeant ainsi les identités (Simmel 1908 ; Duhaime 2001). Loin de révéler une « crise » de la gouvernance de l'infrastructure (comme le suggèrent De Filippi & Loveluck 2016), le désaccord sur la mise à l'échelle constitue, d'après nous, l'expression d'une gouvernance singulière définissant une communauté, ses valeurs et ses pratiques.
- 31 Pour des raisons variées (sécurité, stabilité du système, décentralisation), la taille des blocs a été initialement fixée à 1 Mo (Mégaoctet). Or ce choix limite de fait la quantité de transactions que la chaîne de blocs peut recevoir sur un temps déterminé. À mesure que le Bitcoin devenait populaire et que le nombre de transactions augmentait, l'idée est apparue d'accroître la capacité de traitement des blocs. Mais les différentes modifications, qu'elles portent sur l'optimisation des transactions au sein de bloc inchangé, ou sur l'augmentation de la taille du bloc pour qu'il contienne plus de transactions, induisent toutes des coûts et bénéfices différents. En dernière instance, elles renvoient aux représentations que les acteurs se font du Bitcoin comme de ce qu'ils entendent par « bonne monnaie » (débat sur la primauté de la fonction réserve de valeur ou de moyen d'échange). Une augmentation de la taille des blocs rendrait plus coûteux le maintien des nœuds complets (la base de données croîtrait plus vite et nécessiterait plus d'espace) et se payerait au prix d'une centralisation accrue. Naîtrait alors un risque qu'une entité, ou un groupe, atteigne plus de 51 % de la puissance de minage et puisse théoriquement falsifier les blocs ou censurer certaines transactions (ce qui conduirait irrémédiablement à l'effondrement des trois niveaux de confiance)²⁹. *A contrario*, maintenir les blocs petits permet de conserver un plus grand nombre de nœuds complets et autorise un contrôle plus large par la communauté.
- 32 En 2015, des débats très intenses ont eu lieu sur les forums et réseaux sociaux dédiés. Des conférences se sont tenues sur le sujet et des divisions sont apparues jusqu'au sein du groupe des *core developers*. Hearn évoque une situation de « guerre civile ouverte » entre les rangs des développeurs (Hearn 2016). En août 2015, en l'absence de tout consensus, deux *core developers* (Gavin Andresen et Mike Hearn) lançaient le Bitcoin XT, une nouvelle version du Bitcoin avec des blocs allant jusqu'à une capacité théorique de 8 Mo. Ce projet alternatif a provoqué un *Hard fork*. Deux (ou plus) logiciels alternatifs sont proposés alors aux utilisateurs. L'adoption ou non par ces derniers déterminera quelle branche du projet s'imposera ou bien si elles s'imposeront toutes les deux et évolueront comme deux branches alternatives. Le Bitcoin XT ne s'est finalement pas imposé auprès des mineurs et des utilisateurs et a été abandonné le 23 janvier 2016. Mais il a suscité de telles

controverses et attaques personnelles que Mike Hearn a préféré se retirer de la superstructure de Bitcoin. Depuis, d'autres propositions de *fork* offrant des tailles variables de blocs ont vu le jour (Bitcoin Unlimited, Bitcoin Classic, BitPay Core). Et les derniers épisodes en date (Bitcoin Cash³⁰, SegWit³¹ et SegWit2X³²) ont donné lieu, en 2017, à la mise en place de SegWit sur le protocole Bitcoin, à la naissance du Bitcoin Cash comme nouvelle crypto-monnaie, et à l'abandon de SegWit2X par ses promoteurs.

- 33 De tels conflits mettent aux prises des acteurs aux stratégies, contraintes et représentations souvent antagonistes. Ils peuvent même se dénouer dans des séparations. Les *forks*, moyens techniques d'évolutions du code *open source*, deviennent désormais le moyen politique de l'émancipation de nouvelles communautés monétaires. Ces dernières se regroupent ainsi derrière un projet qui porte leurs valeurs et intérêts. Ce faisant, elles s'émancipent d'anciennes communautés auxquelles elles appartenaient, mais avec lesquelles elles ne partagent plus l'essentiel. Ces *forks* volontaires deviennent le moyen ultime de la gouvernance du Bitcoin. La plupart du temps, ils ne sont pas pacifiés³³, mais leur fonction n'est pas la pacification. Les forks ont pour rôle essentiel le maintien d'un réseau autonome par la constitution d'une communauté qui croit au projet et y participe. Une gouvernance de l'infrastructure est bien à l'œuvre, et à la manière de Hirschman (1995), des procédures de prise de parole (*voice*) fondées en loyauté sont ouvertes. Si les personnes porteuses d'un projet de modification n'arrivent pas à fédérer la majorité de la communauté autour de celui-ci, elles peuvent toujours faire le choix de l'*exit*, et créer leur propre monnaie autour d'une communauté plus homogène en valeurs. Dans ce cas, deux communautés apparaissent et chaque membre de la communauté originelle (possesseur d'unité monétaire au moment du *fork*) se voit doté des mêmes soldes dans chacune des deux chaînes. Cela laisse à chacun le choix de ce qu'il veut en faire et celui de définir son appartenance ou non à ces communautés.
- 34 L'apparente inertie de cette gouvernance, au sens où il apparaît en pratique difficile d'imposer des modifications techniques importantes est, pour de nombreux promoteurs du Bitcoin, sa plus belle réussite. Pour eux, il serait un pas de plus vers une société *crypto-anarchiste*, en faisant la démonstration qu'un système résilient aux pressions, coopératif, partageant le pouvoir et l'information, peut rester pérenne, fiable et viable. Les propriétés tant vantées d'immutabilité du Bitcoin, bien que cela soit largement discutable en théorie et en pratique (Walch 2017), se paient au prix d'une évolution lente. L'adoption massive ou non du Bitcoin constituera l'indicateur ultime de la réussite ou non de son système de gouvernance.

Conclusion

- 35 Contrairement au récit de certains de ses promoteurs, le Bitcoin est une construction profondément politique et sociale. Il requiert par conséquent des formes d'institutions sociales (internes et/ou externes), plus ou moins formelles, en mesure de préserver la légitimité d'ensemble du système. La pratique des *forks* à répétition montre comment la superstructure actuelle gère les évolutions : de manière conservatrice. Elle permet en cela le maintien d'une forme de *statu quo* défendant la vision d'un Bitcoin comme non censurable, propriété qui ferait pour ses promoteurs sa valeur première. Avoir imaginé qu'une infrastructure technique pouvait se maintenir par elle-même, sans aucune intervention de tiers extérieurs était une erreur. Plutôt que d'avoir une gouvernance, le Bitcoin est une gouvernance dans son ensemble. Cette gouvernance combine une

superstructure socio-économique et une infrastructure technique. La superstructure s'est constituée progressivement en faisant émerger des formes instituées de résolution des conflits (BIPs, réseaux sociaux, rencontres, votes) permettant des évolutions consensuelles du protocole. Les *forks* eux-mêmes apparaissent non pas comme un révélateur de crise, mais bien comme un élément constitutif de la gouvernance singulière du Bitcoin. D'ailleurs, ils s'inscrivent parfaitement dans la définition d'un code *open source* dont la caractéristique est sa capacité à être dupliqué et modifié en fonction des besoins et des usages !

- 36 Les crypto-monnaies ayant vu le jour depuis 2009 ont dessiné d'autres modalités de gouvernance. Elles peuvent être une source d'inspiration car elles articulent à leur manière les trois niveaux de confiance. Des systèmes hybrides à algorithme de *Proof Of Stake*, comme le Dash par exemple, offrent des prestations monétaires supérieures au bitcoin (anonymat et rapidité) et disposent de procédures de gouvernance collective incorporées dans leur architecture (budgets communs, finançant les propositions votées par des *masternodes*, acteurs à statut spécifique). Chaque communauté spécifique associée à sa crypto-monnaie est porteuse de valeurs et de représentations propres.
- 37 Les pionniers du Bitcoin ont cherché à se libérer d'une monnaie vectrice d'oppression, de contrôle et de domination. Ils ont conçu le Bitcoin comme le plus pur outil de l'émancipation. Ce dernier apparaît comme une voie de défétichisation de la monnaie, pointant sa construction institutionnelle et politique. Si le projet Bitcoin voulait à l'origine remplacer la discrétion par la règle, il a finalement bien plus souligné la construction institutionnelle et collective de celle-ci.
- 38 Loin d'être une manière de dépolitiser la monnaie, le Bitcoin et les crypto-monnaies semblent plus à même de la re-politiser en questionnant directement toutes les dimensions de la monnaie en tant que système de paiement, dont chaque règle et paramètre constitutifs peuvent et se doit d'être discuté collectivement. Le Bitcoin est ainsi, comme toute monnaie, une institution. Il est un ensemble organisé de structures matérielles et de parties prenantes définies, régies et gouvernées par des règles fondées en représentation.

BIBLIOGRAPHIE

Aglietta Michel & Jean Cartelier (1998), « Ordre monétaire des économies de marché », in M. Aglietta & A. Orléan (dir.), *La Monnaie souveraine*, Paris, Odile Jacob, p. 129-157.

Aglietta Michel & André Orléan (dir.) (1998), *La Monnaie souveraine*, Paris, Odile Jacob.

Aglietta Michel, Ould Ahmed Pepita & Jean-François Ponsot (2014), « La monnaie, la valeur et la règle », *Revue de la régulation* [En ligne], 16 | 2e semestre / Autumn 2014, mis en ligne le 19 décembre 2014, consulté le 29 mars 2018. URL : <http://journals.openedition.org/regulation/10998> ; DOI : 10.4000/regulation.10998

Akrich Madeleine (1989), « La construction d'un système socio-technique – Esquisse pour une anthropologie des techniques », *Anthropologie et Sociétés*, vol. 13, n° 2, p. 31-54.

- Ali Robleh, Barrdear John, Clews Roger & James Southgate (2013), « The economics of digital currencies », *Bank of England Quarterly Bulletin*, Q3, n° 1, p. 38-47.
- Böhme Rainer, Christin Nicolas, Edelman Benjamin & Tyler Moore (2015), « Bitcoin: Economics, Technology, and Governance », *Journal of Economic Perspectives*, vol. 29, n° 2, p. 213-238.
- Blanc Jérôme (1998), « Les monnaies parallèles. Évaluation du phénomène et enjeux théoriques », *Revue d'économie financière*, Revue d'économie financière, numéro 49, septembre, p. 81-102.
- Cartelier Jean (1996), *La Monnaie*, Paris, Flammarion, coll. « Dominos ».
- Chaum David (1985), « Security without Identification Card Computers to make Big Brother Obsolete », *Communications of the ACM*, vol. 28, n° 10, October, p. 1030-1044.
- Dai Wei (1998), « b-money »; <http://www.weidai.com/bmoney.txt> (consulté le 29/03/2018).
- Danezis George & Sarah Meiklejohn (2015), *Centrally Banked Cryptocurrencies*, p. 1-15; <https://arxiv.org/abs/1505.06895> (consulté le 29/03/2018).
- De Filippi Primavera & Benjamin Loveluck (2016), « The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure », *Internet Policy Review*, vol. 5, n° 3, September.
- De Filippi Primavera (2014), « Bitcoin: a regulatory nightmare to a libertarian dream », *Internet Policy Review*, vol. 3, n° 2, May.
- Delahaye Jean-Paul (2014), « La cryptographie réinvente la monnaie », *Les nouvelles d'Archimède*, n° 66, p. 13-15.
- Desmedt Ludovic & Odile Lakowski-Laguerre (2015), « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, [En ligne], 18 | 2e semestre / Autumn 2015, mis en ligne le 20 décembre 2015, consulté le 29 mars 2018. URL: <http://journals.openedition.org/regulation/11489>; DOI: 10.4000/regulation.11489
- Dodd Nigel (2007), « On Simmel's Pure Concept of Money: A Response to Ingham », *European Journal of Sociology*, vol. 48, n° 2, p. 273-294.
- Dodd Nigel (2014), *The social Life of Money*, Princeton, NJ, Princeton University Press.
- Drean Gérard [2013], « Au-delà du Bitcoin : l'avenir des monnaies et systèmes de paiement », Note de synthèse ; <http://blog.turgot.org/index.php?post/Drean-bitcoin-fin>, 28/11/2017
- European Central Bank (2012), *Virtual Currency Schemes*, ECB, October.
- European Central Bank (2015), *Virtual Currency Schemes – a further analysis*, ECB, February.
- Hayek Friedrich A. (1976), *Choice in Currency: A Way to Stop Inflation*, The Institute of Economic Affairs, vol. 4, n° 1, p. 1-24.
- Hearn Mike (2016), « The resolution of the Bitcoin experiment »; <https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.o84p91oy2> (consulté le 29/03/2018).
- Hirschman Albert (1995), *Défection et prise de parole, Théorie et applications*, Paris, Fayard, coll. « L'espace du politique ».
- Hughes Éric (1993), *A Cypherpunk's Manifesto*, 9 mars ; <http://www.activism.net/cypherpunk/manifesto.html> (consulté le 29/03/2018).
- Janssen Olivier (2017), « Why “non-mining full nodes” are a terrible idea », *Medium blog post*, 22 August; <https://medium.com/@olivierjanss/why-non-mining-full-nodes-are-a-terrible-idea-ad3c49f7a7b6> (consulté le 29/03/2018).

- Karame Ghassan, Androulaki Elli & Srdjan Capkun (2012), « Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin », *IACR Cryptology ePrint Archive*; <https://eprint.iacr.org/2012/248.pdf> (consulté le 29/03/2018).
- Koning J.P. (2017), « Fedcoin: A Central Bank-issued Cryptocurrency », *R3 Reports*; https://www.r3.com/wp-content/uploads/2017/06/fedcoin_central-bank_R3.pdf (consulté le 29/03/2018).
- Loop Jameson (2014), « Bitcoin Nodes: How Many is Enough? Should we be worried about the declining number of nodes? », Medium, Blog Post, 7 June; <https://medium.com/@lopp/bitcoin-nodes-how-many-is-enough-9b8e8f6fd2cf> (consulté le 29/03/2018).
- Madeira Antonio (2017), « 6 Reasons To Run A Bitcoin Full Node », *Bitcoinist article*, 18 March; <http://bitcoinist.com/6-reasons-run-bitcoin-full-node/> (consulté le 29/03/2018).
- MAY Timothy C. (1992), *The Crypto Anarchist Manifesto*, November; <http://www.activism.net/cypherpunk/crypto-anarchy.html> (consulté le 29/03/2018).
- Meiklejohn Sarah *et al.* (2013), « A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. », *IMC'13 Proceedings of the 2013 conference on Internet measurement*, Pages 127-140; Barcelona, Spain; October 23 - 25, 2013 Cette conférence de 2013 à donner lieu à a publication de l'article : Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M. & Savage S. (2016), « A fistful of Bitcoins: Characterizing payments among men with no names. », *Communications of the ACM*, 59(4), 86-93. DOI: 10.1145/2896384
- Menger Carl (1976) [1871], *Principles of Economics*, Ludwig Von Mises Institute.
- North Peter (2007), *Money and Liberation. The Micropolitics of Alternative Currency Movements*, Minneapolis, MN, University of Minnesota Press.
- Nakamoto Satoshi (2008), « *Bitcoin: A Peer-to-Peer Electronic Cash System* »; <https://bitcoin.org/bitcoin.pdf> (consulté le 29/03/2018).
- Orlean André (2005), « L'utopie individualiste d'une économie sans monnaie », *Communications*, n° 78, « L'idéal prométhéen », p. 235-244.
- Raskin Max & David Yermack (2016), « Digital Currencies, decentralized ledgers, and the future of central banking », *National Bureau of Economic Research*, p. 1-18.
- Rolland Maël & Assen Slim (2015), « Le Bitcoin, une monnaie sans banques », *CEMI-EHESS Working Paper WP 2015-05*, 22 mai.
- Simmel Georg (2009) [1900], *Philosophie de l'argent*, trad. S. Cornille et P. Ivernel, Paris, Puf, coll. « Quadrige ».
- Simmel Georg (1999) [1908], « Le conflit » – Chap. 4 de *Sociologie. Études sur les formes de socialisation*, Paris, Puf.
- Theret Bruno (2008), « Les trois états de la monnaie. Approche interdisciplinaire du fait monétaire », *Revue économique*, vol. 59, n° 4, p. 813-841.
- Von Mises Ludwig (1981, 5th Revised edition) [1912], *The Theory of Money and Credit*, Liberty Fund Inc.
- Walch Angela (2017), « The Path of the Blockchain Lexicon (and the Law) », *Review of Banking and Financial Law*, n° 36, p. 713-766.
- Wray Randall L. (2010), « Alternative Approaches to Money », *Theoretical Inquiries in Law*, vol. 11, n° 1, p. 29-49.

Yermack David (2013), « Is bitcoin a real currency? An economic appraisal », *National Bureau of Economic Research*, p. 1-22; <http://www.nber.org/papers/w19747.pdf> (consulté le 29/03/2018).

NOTES

1. Citation originale : « *We have proposed a system for electronic transactions without relying on trust* ».
2. Comme indiqué par Böhm *et al.*, la littérature aurait retenu cette dénomination dans le but d'établir une distinction nette entre les deux notions (Böhme *et al.* 2015).
3. « *Trustless* ». Cette réflexion est au cœur de la construction du Bitcoin qui doit pouvoir permettre l'échange sans qu'aucune confiance ne soit accordée aux membres du réseau. Nous verrons que l'infrastructure technique est censée garantir qu'aucun membre du réseau, même le plus mal intentionné, ne peut déroger aux règles de consensus imposées par le protocole.
4. Le terme « *cypherpunk* », connu depuis les années 1990, entre dans l'*Oxford dictionaries* en 2006. Il désigne une « personne qui utilise le cryptage lorsqu'elle accède à un réseau informatique dans le but d'assurer la confidentialité et se protéger, en particulier des autorités gouvernementales » (Voir Hughes 1993).
5. Le terme « crypto-anarchiste » désigne une personne appartenant à un groupe qui refuse toute forme d'autorité centrale et qui s'appuie sur l'usage des nouvelles technologies pour définir une nouvelle forme de gouvernance, de confiance et d'identité (voir May 1992).
6. Parmi les fondateurs de ces courants, on trouve David Chaum, John Gilmore, Timothy C. May et Eric Hughes (liste non exhaustive).
7. Dans une société devenue entièrement crypto-anarchiste, « le gouvernement n'est pas temporairement détruit, mais devient inutile et interdit de manière permanente. C'est la communauté dans laquelle la menace de la violence est inexistante car la violence n'existe pas, et la violence n'existe pas parce que ses participants ne peuvent pas être identifiés par leurs vrais noms et leurs adresses. » (Dai 1998)
8. <https://coinmarketcap.com/> (consulté le 13/04/2018).
9. Un bloc est une concaténation des transactions par *hashage* cryptographique. En termes moins techniques, il correspond à une fonction cryptographique qui, appliquée aux données brutes entrantes, les encrypte sous la forme d'une empreinte numérique partielle mais suffisante pour retrouver la donnée initiale.
10. Voir : <https://blockchain.info/fr> (consulté le 29/03/2018).
11. Cette difficulté s'ajuste en fonction de la capacité moyenne du réseau, le but étant de maintenir un rythme moyen d'environ dix minutes entre deux blocs émis quelquesoit l'évolution de la puissance totale du réseau. Voir : <http://www.bitcoinblockhalf.com> (consulté le 29/03/2018).
12. La monnaie comme système de paiement est une hypothèse développée d'abord par Cartelier (1996) puis Aglietta & Cartelier (1998). La monnaie y est dès le départ pensée comme une institution minimale permettant une économie de marché décentralisée, puisqu'elle est un ensemble de règles rendant possible la coordination économique. Un système de paiement se définit selon la présence (i) d'une unité de compte nominale, première dans l'ordre économique (ce que reconnaissent nombre de courants institutionnalistes – voir Wray 2010) puisque c'est sur elle que repose toute forme

d'évaluation économique ; (ii) d'un monnayage définissant les conditions d'accès aux moyens de paiement ; (iii) de règles de résolution des soldes entre individus.

13. Trois dimensions de la confiance sont proposées par Aglietta & Orléan (1998) et par Thérét (2008). C'est à travers la multitude des variations potentielles de ces trois dimensions et de leur articulation qu'il est permis de déceler la nature et de mesurer la force de la confiance collective à la source de la monnaie. Les auteurs distinguent : (i) une confiance méthodique, correspondant aux mimétismes des comportements individuels, de l'ordre d'une croyance routinière dans l'acceptation collective de ce médium ; (ii) une confiance hiérarchique, reposant sur une relation de subordination à une instance supérieure (État, Banque centrale) qui établit les règles d'usage de la monnaie, en garantit les moyens de paiement et protège les utilisateurs ; (iii) une confiance éthique, mettant en branle l'autorité du système normatif (normes et valeurs) porté par les autorités monétaires.

14. Il est un écosystème au sens où il repose sur des logiciels compatibles entre eux, mais issus d'architectures, de codes source et de langages de programmation différents.

L'écosystème Bitcoin fait partie de l'écosystème plus large des protocoles à registre distribué, dont il est le précurseur. Enfin, suivant cette logique d'emboîtement, il est contenu lui-même dans l'écosystème monétaire de nos économies, auquel il se connecte, là encore, *via* des acteurs spécifiques : bourses, services de paiement, portefeuille, etc.

15. Ce bloc originel a un statut particulier puisqu'il apparaît le premier. Il est celui qui permet l'émission des premières unités de bitcoin, et sur lequel va se bâtir la chaîne de blocs (voir https://en.bitcoin.it/wiki/Genesis_block (consulté le 29/03/2018)).

16. Les codes *open source* sont mis en ligne et accessibles *via* différentes plateformes. Github, par exemple, est une plateforme très utilisée car elle héberge répertoires et logiciels, offre des outils de gestion de version, permet des discussions et contrôle l'accès. Si le code est librement téléchargeable, l'accès au répertoire relève quant à lui du/des développeurs qui en ont l'accès (« commit right »), ce qui permet d'en certifier la source. Rien n'empêche un développeur de développer un nouveau répertoire en repartant d'un ancien code *open source*.

17. La procédure est explicitée sur le site suivant : <https://bitcoincore.org/en/contribute/> (consultation du 24/11/2017). On peut y constater le nombre de développeurs participant au répertoire, les recompositions à l'œuvre, l'intensité de l'activité de chacun. En définitive, une centaine de développeurs y ont contribué. Voir <https://github.com/bitcoin/bitcoin/graphs/contributors> (consulté le 29/03/2018).

18. Les ASIC (Application Specific Integrated Circuit) permettent une augmentation importante de la puissance de hash et contrairement aux logiciels, ils introduisent une concurrence technologique et des brevets pouvant induire une centralisation. Pour une comparaison des composants et de leur puissance, voir https://en.bitcoin.it/wiki/Mining_hardware_comparison (consulté le 29/03/2018).

19. Certains de ces pools ont adopté des architectures centralisées tandis que d'autres travaillent en P2P décentralisé.

20. En novembre 2017, les six plus grands pools représentaient à eux seuls près de 78 % de la capacité totale de calcul du réseau. Voir <https://blockchain.info/pools> (consultation du 24/11/2017)

21. Un tel processus a fait l'objet d'un brevet et met en péril la distribution homogène de la puissance (risque d'attaque à 51%) puisqu'il offre un pouvoir de monopole à celui qui le vend et en use. Voir <https://bitcoinmagazine.com/articles/halong-mining-first-bitcoin-mining-hardware-producer-implement-overt-asicboost/>. Certains membres de la

communauté, dont les porteurs du brevet, ont réagi *via* l'établissement de la « Blockchain Defensive Patent License », créant une licence commune ouverte à tout membre de l'organisation. Voir <https://blockchaindpl.org/> (consultation du 13/04/2018)

22. Portefeuilles qui, pour rester pratiques et légers (sur téléphone portable par exemple) ne maintiennent pas leur propre version dupliquée de la chaîne de blocs.

23. Le premier *BIP* (*BIP* 0001) fut déposé par le développeur Amir Taaki. Voir <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki> (consulté le 29/03/2018).

24. <https://bitcoin.fr/proposition-damelioration-de-bitcoin/> (consulté le 29/03/2018). Il existe des *BIPs* standards, des *BIPs* informationnelles et des *BIPs* de processus.

25. <https://github.com/bitcoin/bips> (consulté le 29/03/2018).

26. Reddit, Bitcointalk ou encore twitter.

27. Mise en place en 2016 de la Satoshi Round Table, dont les participants sont les grands noms de la communauté Bitcoin. Liste disponible sur <https://news.bitcoin.com/satoshi-round-table-participants-agree-sign-pledge-respectful-dialogue/> (consulté le 29/03/2018) ; événement de type scaling bitcoin ; conférence, etc.

28. <https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki> (consulté le 29/03/2018).

29. La confiance méthodique serait rompue, puisque les transactions peuvent être censurées par l'entité détenant le pouvoir d'émission des nouveaux blocs. La confiance éthique et hiérarchique en serait de fait remise en question.

30. Bitcoin Cash est né le 1^{er} août 2017, de la volonté d'une partie de la communauté, dont Jihan Yu (PDG de Bitmain) et Roger Ver (investisseur pionnier), de ne pas adhérer au projet SegWit. Bitcoin Cash correspond à un *hard fork* et propose un bloc à 8 Mo.

31. SegWit, activé le 1^{er} août 2017, correspond à un *soft fork*. Il propose une modification de script des transactions afin d'optimiser les blocs pour qu'ils puissent contenir plus de transactions. SegWit rend inopérant l'avantage qu'obtenait Bitmain *via* son AsicBoost.

32. SewWit2X a été abandonné par ses promoteurs. Il correspondait à un *soft fork* prévoyant en plus de l'implémentation de Segwit, un passage à des blocs à 2 Mo. Voir, <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-March/013921.html> (consulté le 29/03/2018).

33. Aux discussions s'ajoutent souvent les insultes sur les réseaux sociaux, voire les attaques informatiques coûteuses.

RÉSUMÉS

Le Bitcoin, cryptomonnaie apparue en 2009, repose sur une infrastructure technique censée offrir « un nouvel espace de liberté » selon l'expression de ses concepteurs. Cette infrastructure, s'appuyant sur un protocole décentralisé, une chaîne de blocs et le minage, a été pensée pour permettre l'interaction directe des individus sans aucun recours à un tiers. Cet article s'attache à montrer que la gouvernance *par* l'infrastructure du Bitcoin conduit, comme elle contraint, à l'émergence d'une gouvernance *de* l'infrastructure socialement située. Problèmes et solutions prennent alors place hors du champ de la technique, au sein d'espaces de débats et de prise de

décision socialement construits et organisés. Contre l'attente de ses concepteurs, le Bitcoin relève désormais d'une gouvernance « duale », à la fois technique et sociale.

The Bitcoin, a cryptocurrency which appeared in 2009, is based on a technical infrastructure supposed to propose “a new space of freedom” according to its creators. This technical infrastructure, based on a decentralized protocol, a Blockchain and a process of mining, was designed to allow direct interaction of individuals without any intervention of a third party. This article aims to show that the governance by the infrastructure of Bitcoin both helps and hinders the emergence of a governance of the infrastructure. Problems and solutions then take their place far from the field of technology within socially constructed and organized forums for debate and decision-making. Despite the expectations of its creators, the Bitcoin is now based on a technical and social “dual” governance.

INDEX

Keywords : monetary systems, innovations, Bitcoin, institutions

Mots-clés : systèmes monétaires, innovation, Bitcoin, institutions

AUTEURS

MAËL ROLLAND

Professeur en économie en Lycée, chercheur au CEMI à l'EHESS, roland.mael@hotmail.fr

ASSEN SLIM

Inalco, Essca, chercheur au CREE à l'INALCO, membre associé au CEMI à l'EHESS, assen.slim@inalco.fr