L'alternative monétaire Bitcoin : une perspective institutionnaliste[1]

The Bitcoin alternative: an institutionnalist perspective

Odile Lakomski-Laguerre, Université Picardie-Jules Verne, CRIISEA (EA3908)
odile.lakomski@u-picardie.fr
Ludovic Desmedt, Université de Bourgogne, LEDi (UMR 6307)
ludovic.desmedt@u-bourgogne.fr

Résumé

Depuis quelques années, on assiste à l'émergence de monnaies d'un genre nouveau, reposant sur des procédés cryptographiques, gérées en pair à pair selon un consensus distribué. La plus représentative d'entre elles, le Bitcoin, est lancée après la crise financière de 2008 et vient contester un ordre monétaire fondé sur le crédit et le pouvoir bancaire. Ces crypto-monnaies viennent heurter la conception traditionnelle de la monnaie : unitaire, souveraine, territoriale et centralisée. Par conséquent, elles interrogent la théorie et renouvellent le débat sur la nature de la monnaie. Dans ce papier, nous proposons d'analyser le Bitcoin au filtre d'une théorie institutionnaliste de la monnaie. En tant qu'institution sociale, la monnaie est plus qu'une technologie car elle participe à la construction d'un espace marchand s'articulant avec un ordre socio-économique. C'est pourquoi nous mettons en évidence les arguments de la contestation et les racines idéologiques qui sous-tendent le système Bitcoin : décentralisation, anti-étatisme (cryptage) et naturalisation de la monnaie (minage). En mettant en avant la notion centrale de confiance, nous nous intéressons ensuite à la capacité du projet Bitcoin à construire un ordre monétaire, certes alternatif, mais stable.

Mots clés

Bitcoin, système de paiement, monnaie, cryptographie, banque, confiance.

Abstract

Over the past few years, we have witnessed the rise of a new kind of currencies, based on cryptographic processes and managed by peer-to-peer networks. The first and most popular of them, the Bitcoin, was launched after the financial crisis of 2008 and disputes a credit-based monetary order supported by banks. In general, crypto-currencies are challenging the traditional design of the currency as a unitary, territorialized and centralized system. Consequently, they raise theoretical problems and renew the debate on the nature of money. In this paper, we develop an analysis of Bitcoin through an institutionnalist approach. Much more than a pure technology, money is a social institution. Therefore it builds a trade space that must be thought in articulation with a socioeconomic order. This is why we highlight the ideological roots underlying the contesting Bitcoin system: no more centralised hierarchical

[1] Nous remercions les rapporteurs de la revue qui nous ont incités à préciser de nombreux points. Les participants des séminaires dans lesquels ces idées ont été présentées ont également participé à l'amélioration de ce texte. Nous restons responsables des erreurs ou imprécisions.

control over social and economic affairs (encryption) and the naturalization of money (mining). Putting forward the central idea of trust, we test the ability of Bitcoin to build up a new stable monetary order.

Keywords: Bitcoin, payment system, currency, encryption, trust.

Codes JEL
B52 , B25, E42, E51, G38, L14, P1.

Introduction

Le projet Bitcoin voit le jour immédiatement après le déclenchement de la crise financière de 2008, dont l'ampleur a jeté un fort discrédit sur l'industrie bancaire. Comme toute innovation radicale, le caractère disruptif de la technologie qui porte la crypto-monnaie, appuyé par les nouvelles logiques économiques que génère l'expansion d'Internet, apparaît comme une menace potentielle vis-à-vis de l'ordre monétaire existant[2]. Au-delà du seul aspect technique, le système Bitcoin s'affiche clairement comme une alternative au capitalisme contemporain dont la dynamique est portée par une collusion Banques-Gouvernements. Aussi s'inscrit-il dans un mouvement de contestation des pouvoirs politiques et bancaires, qui ont été jugés incapables d'offrir une monnaie de qualité. Les crypto-monnaies constitueraient alors un moyen de "démocratiser la finance" au sein d'espaces alternatifs (transnationaux) et de restituer aux individus ce "bien commun" qu'est la monnaie. Il est donc important de saisir les valeurs et l'idéologie qui sous-tendent le Bitcoin.

L'engouement pour la nouveauté mêlé à la curiosité croissante face à cette monnaie d'un nouveau genre, a donné lieu à un foisonnement impressionnant de travaux, d'analyses, de commentaires et de débats. Or, force est de constater qu'un manque de clarté, si ce n'est une réelle confusion, règnent la plupart du temps dans les études sur le sujet. Cette difficulté tient en grande partie à la diversité des discours (praticiens, théoriciens, medias plus ou moins spécialisés, sites dédiés au Bitcoin, articles académiques etc.) et à la variété d'approches émanant de différents champs disciplinaires intéressés à cet objet (informatique, économie, droit etc.). Mais le constat le plus sévère est à faire au sein de la discipline économique, dans la mesure où la plupart du temps, les commentaires sur le Bitcoin ne s'accompagnent d'aucun éclairage théorique. Est-ce si étonnant, lorsqu'on sait à quel point la monnaie divise les économistes?

Un dernier obstacle à la compréhension du Bitcoin vient aussi de l'incapacité des analystes à s'abstraire de ce qu'ils connaissent déjà : la monnaie bancaire, unitaire et centralisée, garantie en dernier ressort par l'Etat. Or, Internet et les crypto-monnaies remettent en cause cette conception traditionnelle et interrogent la théorie sur sa capacité à les penser. L'objectif central de ce papier consiste à poser les jalons *théoriques* d'une évaluation du Bitcoin comme projet *monétaire*. Le cadre d'analyse que nous privilégions est celui de la monnaie en tant qu'institution sociale. En tant que système de paiement le Bitcoin institue une unité de compte et des règles d'organisation des transactions, de sorte qu'il obéit à des logiques qui lui sont propres. Dans une approche institutionnaliste cependant, l'aspect

[2] Les réactions des Banques Centrales vont de la prohibition pure et simple de cet instrument à la tolérance, voir par exemple : Szczepanski, 2014.

purement fonctionnel de la monnaie doit être dépassé afin de construire une véritable économie politique du Bitcoin. Cela suppose l'étude des formes d'adhésion collective qu'il suscite.

Dans un premier temps, nous discuterons du caractère innovant et alternatif du Bitcoin (système transnational, a-bancaire et décentralisé), en faisant le point sur les vrais enjeux et les faux problèmes qu'il soulève. Nous rappellerons également les caractéristiques de son fonctionnement, en testant, selon la grille de lecture émanant de la théorie des systèmes de paiement, la capacité du Bitcoin à opérer comme monnaie. Dans une deuxième partie, nous analyserons plus précisément les arguments de ses promoteurs[3] en montrant notamment que, contrairement à l'image qu'ils veulent en donner, le Bitcoin n'est pas une technologie neutre. Elle est porteuse d'un ensemble de valeurs et d'une idéologie bien spécifiques qui œuvrent comme une entreprise de "moralisation des marchés" (Fourcade et Healy, 2007). On retrouve bien sûr des valeurs propres au réseau Internet : transparence, décentralisation, accès libre etc. Le Bitcoin plus spécifiquement semble être construit sur la base d'un alliage entre anti-étatisme et néo-métallisme. Maurer et *alii* ont employé le terme de "métallisme digital" (Maurer, Nelms et Swartz, 2013) : dans le vocabulaire des "mineurs" ou dans l'iconographie attachée au système Bitcoin, la référence au métal est omniprésente et contribue à ancrer la monnaie dans un ordre naturel inaliénable. Les promoteurs du Bitcoin suggèrent que les procédés cryptographiques peuvent remplacer les banques comme instances légitimes d'émission de la monnaie. C'est pourquoi, dans un troisième temps, nous nous intéresserons à une notion à nos yeux essentielle : celle de la confiance dans la monnaie. Nous nous référons ainsi aux approches institutionnalistes développées récemment (Aglietta-Orléan, 1998 ; Théret, 2007, 2008) pour tester la capacité du réseau Bitcoin à générer un nouvel ordre monétaire stable.

1. Le Bitcoin, système de paiement électronique de pair à pair

En février 2009, est publiée sur le site P2Pfoundation et sous le nom d'usage de Satoshi Nakamoto[4] (Nakamoto, 2009b), l'annonce d'un travail effectué sur une monnaie de pair à pair, reposant sur des procédés cryptographiques : le Bitcoin. Le code du logiciel expliquant la mise en œuvre du système est détaillé dans un document diffusé en 2009 (Nakamoto, 2009a). La nouveauté du Bitcoin ne réside pas dans son caractère "digital", "virtuel", "électronique" ou "numérique", comme beaucoup de commentateurs semblent le signifier. Faire table rase d'un certain nombre de malentendus nous ramène à la question centrale de la nature de la monnaie. Il est important de distinguer, d'une part les invariants théoriques et, d'autre part, les différentes formes et régulations qu'a pu prendre la monnaie au cours de l'histoire. Si le Bitcoin apparaît bien comme un système de paiement, l'alternative repose dans l'absence d'autorité centrale et dans l'autorégulation de la monnaie cryptographique.

[3] En ce qui concerne la mobilisation des valeurs et de l'idéologie de la communauté Bitcoin, nous nous sommes appuyés pour l'essentiel sur les discours de ses promoteurs, accessibles sur les sites officiels de la crypto-monnaie. Nous sommes bien conscients du fait que l'approche purement théorique de ce papier devra être nécessairement complétée, dans des travaux ultérieurs, par une véritable démarche empirique, afin d'analyser plus finement cette communauté Bitcoin.

[4] Nakamoto est probablement un pseudonyme derrière lequel se cachent une ou plusieurs personnes. Pour les multiples interprétations relatives à l'identité du ou des développeurs du Bitcoin, on peut voir les discussions sur le site P2Pfoundation: p2pfoundation.net/Bitcoin.

1. 1. Quelle innovation?

En insistant de façon récurrente sur une rupture d'ordre "digitale" ou "numérique", les différentes analyses portant sur l'innovation Bitcoin introduisent parfois un malaise intellectuel. A forcer ainsi le trait sur l'idée d'un objet qui ne circule pas *physiquement*, ces commentaires semblent refléter la persistance, encore visible aujourd'hui, d'une conception matérialiste de la monnaie. En effet, dire que le Bitcoin est une monnaie purement numérique laisserait supposer, par effet de contraste, que la monnaie utilisée quotidiennement ne l'est pas, elle. Or, l'informatisation des opérations monétaires que le système bancaire maîtrise depuis le début des années 1970, permet aujourd'hui le stockage et le transfert massif de monnaie par voie électronique (notamment, au moyen du protocole *Secure Sockets Layer*). Autrement dit, presque toute la monnaie est actuellement digitale. Malgré tout, les opérations monétaires ont toujours nécessité des médiations et des supports techniques qui ont pris des formes variées au cours de l'histoire : marchandises précieuses, livres de comptes bancaires, et actuellement informatique et microprocesseurs. En ce sens, toute monnaie est dite "virtuelle", "digitale", "électronique" de façon très générale, à partir du moment où elle suppose une médiation par des ordinateurs (Karlstrom, 2014).

Intéressons-nous maintenant à un second malentendu : toute monnaie électronique n'implique pas nécessairement une innovation *radicale*. Parmi les nouvelles formes monétaires qui se développent très rapidement, certaines relèvent d'une simple évolution dans les techniques de paiement, mais ne remettent pas en cause la nature actuelle de la monnaie. Tant que les transactions monétaires supposent, *in fine*, des transferts d'unités de comptes d'un compte bancaire à un autre, la logique actuelle de la monnaie n'est pas menacée. Avec l'essor du commerce sur Internet, le système *Paypal* a permis en 2000 d'assurer des transferts d'argent sécurisés par courrier électronique. Mais le caractère électronique des flux monétaires supposait toujours un adossement au système bancaire, qui contrôlait le bon déroulement des opérations de compte à compte. Ainsi, en 1988 on estimait à raison que "l'utilisation de l'électronique dans la manière de donner les ordres de paiement ou de transférer des fonds, n'a pas généré, jusqu'à présent, une nouvelle forme de monnaie, à côté de la monnaie fiduciaire (espèces) et de la monnaie scripturale (comptes)" (Ancel, 1988: 305). En revanche, d'autres innovations impliquent un changement plus qualitatif, augurant une modification profonde et irréversible des pratiques monétaires et, par conséquent, de notre façon de penser la monnaie. Il est donc crucial de distinguer clairement les innovations technologiques et les innovations économiques (Gazé, 2003). Depuis les années 1980, les recherches dans le domaine de la cryptographie ont donné lieu à de véritables innovations, qui représentent un défi sérieux à l'ordre monétaire existant et heurtent notre conception théorique actuelle de la monnaie (unitaire, souveraine). Par conséquent, si nous voulons saisir les véritables potentiels, défis et enjeux (qu'ils soient économiques ou sociaux) du Bitcoin, nous devons prendre un certain recul par rapport à la représentation dominante : celle de la monnaie bancaire et centralisée. Car conformément à la logique d'Internet, le Bitcoin est un puissant outil de *désintermédiation*. A l'instar des partages de fichiers numériques (musique, vidéos, etc.), il est fondé sur un réseau de pair à pair (P2P). Son bon fonctionnement ne dépend donc *a priori* d'aucune autorité, mais repose plutôt selon le principe du consensus distribué[5]. Ceci explique notamment les coûts de transactions faibles associés aux paiements

[5] Un système distribué est un système composé de plusieurs entités (ordinateurs par exemple) connectées entre elles par un réseau de communication et qui, ensemble, s'attaquent à un problème : réaliser un calcul ou chercher de l'information (voir notamment Fisher, M.J., Lynch, N.A., Paterson, M.S. (1985) « Impossibility of distributed consensus with one faulty process », *Journal of the Association for Computing Machinery*, vol. 32, n° 2, p.374–

dans la crypto monnaie, principal argument utilisé par les promoteurs pour en vanter les avantages. Ainsi, le Bitcoin augurerait bel et bien l'avènement de nouvelles pratiques monétaires.

Bien que d'un genre nouveau, le Bitcoin se revendique malgré tout comme une monnaie. Aussi est-il important de repérer, derrière la multiplicité des formes empiriques, les *invariants théoriques* de la monnaie : qu'est-ce qui, *par essence*, la définit comme telle? Un examen satisfaisant du Bitcoin comme système monétaire ne saurait donc faire l'abstraction d'une grille de lecture analytique. Mais laquelle? La théorie économique permet d'identifier clairement les fonctions essentielles de la monnaie (unité de compte, instrument d'échange, réserve de valeur), ainsi que les propriétés d'une économie monétaire. En revanche, la question de savoir si les économistes spécifient clairement la *nature* de la monnaie est plus controversée : est-elle une marchandise, un actif sans risque, une institution sociale? Un autre facteur de désaccord concerne la hiérarchie des différentes fonctions de la monnaie : est-elle fondamentalement un instrument d'échange ou une réserve de valeur? Le principal défaut de la plupart des analyses concernant le Bitcoin, vient de ce qu'elles manquent cruellement de clarté, précisément en raison d'un vide théorique qui conduit à mêler et à confondre les différentes clés d'entrée précitées, créant ainsi de faux problèmes. Laissons donc momentanément de côté le caractère contestataire, alternatif ou disruptif du Bitcoin, pour l'appréhender d'abord comme une *monnaie*, puisque telle était sa vocation au départ. Notre analyse s'appuiera alors sur l'hypothèse de la fonction essentielle de la monnaie comme unité de compte. D'une importance primordiale, elle distingue radicalement une économie monétaire d'une économie de troc (Keynes, 1930). En tant qu'unité de compte, la monnaie ne relève pas de forces endogènes au sein du système économique, mais d'un acte hors marché. Elle sert à fixer des grandeurs nominales (prix absolus, en unités de compte) et à enregistrer les transactions ("*record keeping device*", Ostroy et Starr, 1990). C'est par cette fonction d'ailleurs que Schumpeter revendiquait clairement le statut d'institution sociale de la monnaie, l'assimilant à une "comptabilité sociale" dont l'établissement s'avère indispensable au calcul et à la détermination d'un équilibre économique (Schumpeter, 2005).

Plus récemment, l'approche en termes de systèmes de paiement insiste sur l'hypothèse institutionnelle de la monnaie comme unité de compte, sans laquelle aucune économie de marché décentralisée n'est cohérente, ni même réalisable (Cartelier, 1991, 1996). Ces approches, certes différentes, se rejoignent sur l'hypothèse du caractère premier et *abstrait* de l'unité de compte ; la question de la réserve de valeur est alors secondaire pour spécifier le caractère monétaire d'un objet. L'affirmation de cette primauté accordée à l'unité de compte est d'ailleurs clairement revendiquée par la plupart des démarches institutionnalistes (Ingham, 2004, Wray, 2014). Parmi elles, des positions plus radicales voient dans la fixation d'une unité de compte un élément de souveraineté. Dans cette perspective, le courant néo-chartaliste assimile l'unité de compte à l'idée de moyen légal de paiement, permettant à l'Etat de prélever les taxes et les impôts (voir Wray, 2014). Une représentation politique, centralisée et territoriale de la monnaie est étroitement associée à cette conception. La monnaie est alors conçue comme une "créature de la loi" (Knapp, 1905) et la formation d'un espace monétaire détermine conjointement l'existence d'un circuit fiscal et donc, d'un espace public. Echapper à cette souveraineté politique, c'est précisément l'objectif du (ou des) concepteur(s) et des promoteurs du Bitcoin. Si son lancement va de pair avec la définition d'une unité de compte spécifique, en revanche, la conception de cette monnaie est à l'opposé de l'idée de

382 ; voir également Lamport, L., Shostak, R., Pease, M. (1982), « The Byzantine General Problems », *ACM Transactions on Programming Languages and Systems*, vol.4, n°3, p. 382-340). Chaque entité propose une valeur et à la fin du calcul, toutes doivent s'être mises d'accord sur l'une de ces valeurs.

souveraineté politique : le Bitcoin (comme le réseau internet d'ailleurs) est global, a-territorial, indépendant de tout pouvoir central. Il s'agirait donc, *a priori*, d'une vision purement *procédurale* de la monnaie.

Aborder la monnaie comme unité de compte présente un avantage indéniable. Cela évacue définitivement l'idée de considérer l'avènement des monnaies "électroniques" ou "numériques" comme l'aboutissement d'un long processus d'évolution : celui de la dématérialisation progressive de la monnaie[6]. En tant qu'elle est avant tout une unité de compte, la monnaie a toujours été fondamentalement abstraite. Cela signifie qu'elle n'a pas besoin d'être constituée d'un matériau (pourvu d'une valeur intrinsèque) pour fonctionner comme *monnaie*. Néanmoins, comme nous le verrons par la suite, la circulation des signes monétaires n'exclut par pour autant des médiations et des infrastructures concrètes et matérielles.

1. 2. Le Bitcoin est-il une monnaie ? Une analyse en termes de système de paiement

Comme nous l'avons évoqué plus haut, la théorie des systèmes de paiements définit la monnaie comme l'institution minimale d'une économie de marché, décentralisée. Elle est alors pensée comme un ensemble de règles destinées à organiser les échanges et à en assurer le bon déroulement (Cartelier, 1991, 1996). Plus précisément, tout système de paiement peut être caractérisé par : 1/ la fixation d'une unité de compte; 2/ une règle de monnayage qui détermine la manière dont les unités de compte sont mises en circulation; 3/ une procédure de règlement des soldes monétaires (le paiement). Nous proposons de montrer, à la lumière des principes qui viennent d'être exposés, que le Bitcoin présente certaines caractéristiques d'une monnaie, dans la mesure où le lancement de l'unité de compte est bien accompagné d'un ensemble de règles et de méthodes qui assurent la circulation et la gestion de l'unité de compte (régulation de l'offre), ainsi que la bonne marche des transactions et le respect du principe fondamental d'équivalence (dans l'échange).

Notons tout d'abord que sur la plupart des sites officiels dédiés à cette monnaie, le Bitcoin (alors écrit avec une majuscule) est défini comme un système de paiement et comme une unité de compte (le bitcoin, sans majuscule). Cependant, sa conception en fait une monnaie assimilable à de l'argent liquide numérique. Par conséquent, le règlement des soldes ne réclame aucune procédure spécifique, puisque les transactions sont immédiatement dénouées, et la contrainte monétaire est totale. L'émission des bitcoins n'est donc en aucun cas effectuée en contrepartie du crédit[7]. Les mécanismes et les règles qui en organisent le fonctionnement sont le fait d'algorithmes établis par un code source en accès libre (*open source*).

Pour utiliser le système, il est nécessaire de posséder un "porte-monnaie" (*wallet*), qui n'est rien d'autre qu'un nom donné à une suite de symboles, en l'occurrence une suite de chiffres et de lettres. Pour la conserver, tout support convient : la mémoire d'un ordinateur, du

[6] En 2002, un rapport de l'OCDE consacré à l'*Avenir de l'argent* prédisait : "le destin de l'argent est de devenir numérique".

[7] Dans son application purement monétaire, Bitcoin remplace de fait l'argent liquide. Cependant, d'autres applications, notamment financières (crédit, placements financiers, produits dérivés etc.), peuvent être développées grâce à la blockchain. Voir notamment france-bitcoin.net.

papier, une clé USB. Il est possible de détenir plusieurs porte-monnaie, que l'on gère au moyen de logiciels ou d'applications dédiés, sur un ordinateur ou sur un smartphone, ou bien par des sociétés en ligne qui proposent de tels services. A tout porte-monnaie est associée une paire de clés cryptographiques (publique et privée). Chacune des clés d'une paire sert à crypter des messages et à décrypter ceux codés par l'autre clé. La clé publique peut être diffusée, tandis que la clé privée doit être gardée secrète, car c'est elle qui permet de signer et d'authentifier un message[8]. Oublions donc toute référence à la monnaie bancaire actuelle, reposant sur le principe de la comptabilité en partie double (actif-passif) : Bitcoin est une méthode de transferts de données et de droits, sécurisée par la cryptographie asymétrique à double clé[9]. Le paiement revient à transférer une quantité déterminée de bitcoins (disons M) d'un utilisateur A (disons Alice) vers un utilisateur B (Bernard), et la façon de procéder ressemble un peu à l'envoi d'e-mails. Entre autres caractéristiques propres au cash, le Bitcoin respecte l'anonymat des utilisateurs. Ainsi, la cryptographie permet de vérifier l'authenticité des transactions sans révéler l'identité de Bernard ou d'Alice (qui sont en fait des pseudonymes). Pour que la transaction soit validée par le réseau, il suffit de s'assurer que les bitcoins ont bien été envoyés par Alice (pour éviter le problème de la double dépense), et que Alice dispose d'un stock de bitcoins au moins égal à M[10].

Analyser le Bitcoin comme système de paiement nécessite également de se poser la question de l'accès à cette monnaie. Comment obtient-on des bitcoins ? Si nous émettons l'hypothèse d'un raisonnement en circuit fermé et bouclé sur lui-même, alors il serait logique de penser que l'accès aux bitcoins s'effectue en contrepartie d'une vente (de marchandises, de services, de la force de travail) signifiant une contribution à la production (de l'espace marchand correspondant). S'il est possible d'en obtenir en échange de la vente de biens ou services au sein d'un réseau de marchands qui les accepte, en revanche, cette contrepartie est encore extrêmement limitée. De fait, l'accès aux bitcoins s'effectue principalement par la vente de devises officielles sur des plateformes d'échange dédiées, à un cours de marché qui fluctue en fonction de l'offre et de la demande. Dès lors, le bitcoin devient une devise parmi d'autres dans un espace monétaire mondialisé et concurrentiel et il peut, de ce fait, être utilisé comme actif spécifique par tout investisseur motivé par une logique financière d'optimisation de portefeuille. Avec la valorisation phénoménale dont il a fait l'objet depuis sa création, et la volatilité de son cours relativement aux devises officielles, force est de constater que le bitcoin apparaît aujourd'hui bien plus comme un actif spéculatif que comme un instrument au service d'une économie d'échanges et de paiements. Néanmoins, cette distinction essentielle étant faite, nous continuerons à examiner le système Bitcoin comme contestation *monétaire*.

La mise en circulation des bitcoins et le bon déroulement des transactions sont portés par deux procédés : la chaîne de blocs (*Blockchain*) et le minage (*Bitcoin Mining*). Toute transaction doit être traitée, validée et enregistrée dans une sorte de journal public : la chaîne de blocs. Celle-ci est présente dans tous les ordinateurs des utilisateurs du système, et son contenu retrace la totalité des transactions effectuées en bitcoins depuis leur création. Si les transferts monétaires sont anonymes, le contenu de la chaîne de blocs est rendu public et

[8] Par exemple, si A envoie des bitcoins à B, il va signer son message avec sa clé privée. Ainsi, B pourra vérifier, en décryptant le message avec la clé publique diffusée par A, que c'est bien A qui a envoyé le message. Une clé publique est une sorte d'identificateur qui est une suite de symboles du type : *1Lke9VyQHixh8zxteh7mENSr4wsX5N6BeN*. Le titulaire de cet identificateur peut utiliser un pseudonyme (Alice92), qui n'apparaîtra pas dans le registre public. C'est ce qui assure l'anonymat des transactions.

[9] Si la monnaie est *l'une* des applications possibles, la technologie Bitcoin offre d'autres nombreuses potentialités et développements innovants.

[10] Théoriquement, cela renvoie à ce que l'on désigne, à la suite de Clower (1967), sous le terme de "contrainte monétaire".

accessible à l'ensemble du réseau. Il s'agit donc d'une configuration complètement inversée par rapport à la gestion centralisée de la monnaie bancaire. En effet, lorsque les banques enregistrent les transactions individuelles dans les comptes courants, la comptabilité ainsi retracée n'est pas portée à la connaissance du public : l'information est privative. En revanche, chaque titulaire de compte a une identité claire. Au cœur du fonctionnement du réseau, le "minage" (*Bitcoin Mining*) est le mécanisme qui détermine l'émission de nouveaux bitcoins[11]. Il consiste à compléter la chaîne de blocs par l'ajout de nouvelles pages de transactions (des *blocs*). Chaque nouveau bloc est validé par ceux qui contribuent à la gestion et à la surveillance décentralisée des transactions : les "nœuds". Les mineurs sont en concurrence les uns avec les autres. Lorsqu'un bloc est validé par un mineur, l'ensemble des mineurs connectés de pair à pair le compare avec leur propre version de la chaîne de blocs. Si la majorité reconnaît la valeur de ce bloc, il est alors inscrit dans l'historique de toutes les transactions, et le mineur gagnant perçoit une rémunération. Un bloc est généré par le réseau toutes les dix minutes environ, selon un processus de validation qui repose sur l'utilisation d'une fonction de preuve de travail (Nakamoto insiste sur le fait que le Bitcoin est obtenu en échange d'une "*proof of work* ") de type hashcash[12]. Il s'agit d'un problème cryptographique dont la résolution par l'ordinateur valide l'origine et l'authenticité d'une transaction. *Par conséquent, tout nouveau bitcoin émis l'est en contrepartie d'un travail de minage effectué par le réseau*. La contribution des mineurs n'est pas le résultat d'une logique altruiste ; elle est largement motivée par un système d'incitations. Le protocole a été conçu par Nakamoto afin d'éviter que trop peu de nœuds contribuent au fonctionnement du système. Cette activité suppose l'utilisation de ressources (du temps et de l'électricité), sans lesquelles il est impossible de faire tourner les microprocesseurs. Bitcoin ne fait qu'attester un principe central de la monnaie : si l'unité de compte est fondamentalement abstraite, elle n'est pas pour autant désincarnée car les instruments monétaires par lesquels elle est transférée supposent des mécanismes qui, eux, sont bien concrets.

Derrière la "virtualité" des monnaies cryptographiques, un écosystème apparaît donc, qui repose sur des biens tangibles : du matériel informatique (ordinateurs, cartes mémoire, logiciels etc.), de l'énergie électrique et une infrastructure, c'est-à-dire un ensemble de supports permettant de relier entre eux les équipements (câbles, fibres optiques). C'est ce que Maurer et *alii* définissent comme "la matérialité pratique" (*practical materiality*) du Bitcoin (Maurer, Nelms et Swartz, 2013), et qui est révélée à travers divers témoignages de mineurs[13]: acquisition de matériel coûteux et rapidement obsolète (problème de rentabilisation) entraînant une course à l'équipement effrénée et qui semble sans fin ; consommation électrique des ordinateurs qui tournent à plein régime en permanence (générant notamment une production de chaleur qu'il faut contrôler afin d'éviter une surchauffe et un dysfonctionnement des machines, ce qui oblige à prévoir un système de refroidissement). Par conséquent, le minage n'est plus aujourd'hui une activité individuelle : le processus est passé à un stade industriel, avec le regroupement des mineurs en "pools" et la formation de coopératives, *qui inévitablement posent la question d'une centralisation du système obéissant à une logique de mutualisation des ressources*. Nous y reviendrons par la suite.

[11] Voit notamment Bitcoinwiki (https://en.bitcoin.it/wiki/Mining).

[12] "As an alternative to this model, the proof-of-stake (PoS) system was developed (e.g. Nextcoin). This takes into account the number of units of virtual currency owned by each user in the network. It thereby tries to eliminate some of the vulnerabilities of the PoW system, such as the possibility of manipulation through a (temporary) monopoly on mining (the 51% attack) and the high energy consumption", ECB 2015, p.10

[13] Par exemple, "Les confessions d'un mineur de Bitcoins" (http://www.bitcoin.fr/post/Les-confessions-d-un-mineur-de-bitcoin).

L'avantage d'une analyse en termes de systèmes de paiement, c'est qu'elle est applicable à n'importe quelle forme de monnaie. En effet, elle se focalise sur les invariants tels que l'unité de compte et la détermination d'un systèmes de règles et de procédures destinées à la faire circuler et à en assurer la gestion. Nous avons montré quels étaient les modes de régulation propres au Bitcoin, de sorte qu'il fonctionne en tant que monnaie. Mais cela ne nous éclaire en rien sur la nature contestataire et alternative du projet. Car le Bitcoin n'est pas qu'un outil technique destiné à nous faire bénéficier de transactions aux frais réduits. C'est un véritable projet porté par une idéologie bien spécifique, que nous allons maintenant préciser.

2. Derrière la technique : quelle contestation?

Les promoteurs du Bitcoin s'efforcent de le présenter comme une technique neutre : "On ne peut que difficilement trouver une monnaie dans notre histoire qui ait déjà été libre de toute influence politique ou de toute économie nationale. Le Bitcoin est une devise universelle qui est même accessible aux populations non bancarisées. Elle traverse toutes les barrières entre les nations, les politiques et les cultures"[14]. Mais les technologies sont-elles vraiment neutres[15]? Pour saisir le Bitcoin comme projet alternatif, nous devons aller au-delà de l'approche économique des systèmes de paiement, et considérer que la monnaie s'inscrit nécessairement dans un ordre social. A quoi ressemblerait celui porté par la technologie Bitcoin? Derrière l'apparente neutralité du code informatique et des algorithmes, se trouve une logique de contestation : le Bitcoin véhicule ainsi *des valeurs, des normes, et rassemble une communauté porteuse d'un projet politique* : libérer la monnaie de l'Etat et des banques.

2.1. Libérer la monnaie de l'Etat : le Bitcoin entre crypto-anarchistes et défenseurs du marché libre

Au cours des deux dernières décennies, des cryptographes ont cherché à mettre au point une monnaie sécurisée et impossible à tracer. Le Bitcoin est apparu comme l'expérience la plus aboutie de cette série de tentatives. Au début des années 80, David Lee Chaum entamait ses premiers travaux et proposait dès 1985 l'idée d'une monnaie cryptographique dans son article "*Security without identification: Transaction Systems to make Big Brother Obsolete*" (Chaum, 1985). En 1990, Chaum peaufina son modèle et créa la première monnaie cash cryptographique préservant l'anonymat, connue sous le nom de "e-cash". Entre 1998 et 2005, c'est l'informaticien américain Nick Szabo qui développa une monnaie numérique décentralisée appelée "Bit Gold", fondée sur l'idée d'une ressource rare et disponible en quantité limitée à l'instar de la monnaie métallique. En 1998, le cryptographe Wei Dai développa le concept de "B-Money", un système de monnaie électronique distribué et anonyme. S'il y a bien une démarche commune à tous ces projets, c'est l'ambition d'établir un système de paiement libéré de toute influence étatique, intraçable et désintermédié. L'application monétaire participe cependant d'un champ de réflexion beaucoup plus large, qui

[14] http://www.bitcoin.fr/pages/Vices-et-vertus#main.

[15] Un corpus théorique s'est récemment constitué, au sein d'une littérature portant sur les "*science studies*", autour d'une discussion sur ce que Callon appelle la "performativité" des théories économiques (Callon, 1998). Dans la lignée de ces travaux, MacKenzie souligne que l'incorporation des théories n'a pas lieu seulement dans l'esprit des acteurs, mais aussi dans les "algorithmes, les procédures, les routines et les dispositifs matériels" (MacKenzie, 2006: 19).

cherche à assurer, au moyen de protocoles cryptographiques, la confidentialité, l'intégrité et l'authenticité de messages transmis électroniquement.

Alors que la cryptographie peut être mise au service de l'intérêt des gouvernements, certains considèrent qu'elle est aussi et surtout un moyen de se libérer de l'emprise de l'Etat et du contrôle que celui-ci exerce sur les informations relevant de la sphère privée. Les idées exposées par David Chaum notamment, ont été considérées comme les racines techniques du mouvement "*cypherpunk*", mouvement crypto-anarchiste qui s'est manifesté principalement via une liste de diffusion (la plus active entre 1992 et 2001), et dans laquelle on trouvait des hackers, des cryptographes, des défenseurs de la vie privée dont notamment Timothy May, l'auteur du "*Crypto Anarchist Manifesto*". Le contexte historique dans lequel apparaît le Bitcoin ne saurait donc être pleinement restitué sans faire référence à ce mouvement (Jeong, 2013). Ainsi, Julian Assange (créateur de Wikileaks) affirme clairement que le Bitcoin prend racine dans cette mouvance crypto-anarchiste. La "B-Money" de Wei Dai était explicitement associée aux cypherpunks et aux idées de Timothy May ; le Bitcoin est clairement reconnu comme l'héritage intellectuel de la monnaie cryptographique de Dai (Kaplanov, 2012 ; Grinberg, 2011).

Pourtant, S. Nakamoto n'y a jamais fait la moindre référence dans ses différentes publications sur le net, et en 2008, au moment où il diffuse son premier papier, la mailing list des cypherpunks n'est plus active. Cependant, dans les discours officiels de la communauté Bitcoin, nous trouvons des références implicites (ou explicites) à des thèmes tels que : la promotion des libertés individuelles, la défense du marché libre, la revendication d'une devise globale et neutre. On ne peut s'empêcher de penser également à l'influence que les idées ultralibérales de la philosophe et romancière Ayn Rand ont pu avoir au sein de la population américaine[16]. Ce lien n'aurait rien d'étonnant, dans la mesure où, s'il n'est pas nécessairement dominant au sein de la communauté des cryptographes, un fort courant d'idées libertaires associées au principe du marché libre et au respect de la liberté individuelle est néanmoins repérable depuis le début (Karlstrom, 2014). Les préoccupations ne sont pas seulement d'ordre technique (sécurisation des données par le cryptage), mais elles sont aussi philosophiques et politiques : il s'agit de réfléchir aux moyens de contourner le monopole acquis par l'Etat pour le contrôle de l'offre de monnaie et de restituer les pleins pouvoirs d'utilisation de celle-ci à la communauté.

Lorsqu'il lance le Bitcoin néanmoins, le discours de Nakamoto se focalise davantage sur une crise de confiance dans le système bancaire actuel : "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but *the history of fiat currencies is full of breaches of that trust*. Banks must be trusted to hold our money and transfer it electronically, but *they lend it out in waves of credit bubbles with barely a fraction in reserve*"[17] (Nakamoto, 2009a : 1; nous soulignons). Le projet voit ainsi le jour immédiatement après le déclenchement de la crise financière de 2008, et le premier bloc de bitcoins est encodé avec le message suivant : "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"[18]. Si nous nous référons à la première des deux citations précédents (Nakamoto, 2009), c'est le caractère instable et inflationniste d'une monnaie par trop couplée à la finance qui apparaît comme étant le

[16] Auteur de romans comme d'essais, Rand a su coaliser autour d'elle des intellectuels, politiques opposés à "l'esprit du New Deal". En économie, elle aurait été influencée par von Mises.
[17] Satoshi Nakamoto (2009b).
http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562
[18] http://www.newyorker.com/online/blogs/elements/2013/04/the-future-of-bitcoin.html

principal défaut visé. D'un point de vue plus strictement économique, il est difficile de ne pas songer à l'influence du courant libéral autrichien, qui se trouve généralement associé aux mêmes récurrences discursives[19]. Rappelons qu'en plein tournant libéral, F.A. Hayek proposa en 1976 un modèle de free banking fondé sur la concurrence de monnaies privées, de sorte qu'aucune institution centrale (banque centrale ou Etat) ne serait nécessaire à la stabilité monétaire. L'autorégulation de l'offre de monnaie par les mécanismes vertueux de la concurrence et du marché suffirait à contenir les désordres, notamment inflationnistes (Hayek, 1976). L'idée que le système économique puisse reposer sur une multiplicité d'émetteurs et sur l'absence de centralisation (sous forme d'une banque centrale ou de l'unicité du compte), semble désormais trouver un terrain d'application bien concret. En effet, loin de se réduire au seul Bitcoin, l'univers des "crypto-monnaies" compte aujourd'hui une multitude de systèmes de ce type (Litecoin, Peercoin, Namecoin etc.), tous fondés sur des réseaux concurrents (Iwamura, Kitamura et Matsumoto, 2014). Certains travaux interprètent ainsi l'univers concurrentiel des crypto-monnaies dans la perspective d'un processus de sélection naturelle à la Hayek[20]. Plus encore, le fonctionnement des communautés P2P pourrait être pensé à la lumière du concept d'"auto-organisation" et renverrait ainsi à la notion d'"ordre spontané" développé au sein de la tradition autrichienne.

2.2. Le Bitcoin comme "monnaie saine" : naturalisation de la monnaie et retour du métallisme

Ce qui ressort le plus dès l'origine du projet, c'est la volonté affichée d'offrir une monnaie saine et sûre. Aussi le Bitcoin est-il porté par une rhétorique ramenant symboliquement aux régimes monétaires métalliques. La référence aux métaux précieux, plus spécifiquement l'or, est omniprésente à la fois dans la conception même du Bitcoin et dans les discours de la communauté chargée d'en assurer la promotion et la diffusion.

Elle l'est tout d'abord à travers le vocabulaire utilisé. La représentation physique et tangible est affirmée dans le nom même de la monnaie, avec l'utilisation du terme "*coin*". Quant au caractère rare et précieux, il est véhiculé par l'expression d'"or numérique" qui a pu être associée au Bitcoin[21]. De même, le "minage", qui renvoie au processus de validation et d'authentification des transactions, est une référence évidente à la monnaie métallique : "*Bitcoin mining is so called because it resembles the mining of other commodities: it requires exertion and it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground*"[22]. Ainsi, sur Bitcoin.mining, une petite animation explique le processus en montrant une pioche qui frappe des blocs de pierre de plus en plus gros, pour en extraire une pièce (dorée) logée en son centre. La symbolique de la monnaie métallique apparaît également dans une iconographie non moins explicite. La plus populaire consiste sans doute en une série d'images[23] représentant le Bitcoin sous la forme de

[19] L'étude récente de la BCE sur ce sujet reconnaît dans le système Bitcoin l'influence du courant autrichien (BCE, 2012).
[20] Voir par exemple l'analyse que G. Dréan développe dans une série d'articles consacrés au Bitcoin, publiés sur le *blog de l'Institut Turgot*, *think tank* libéral.
[21] C'est de cette façon que le qualifie P. Herlin, par ailleurs grand enthousiaste de cette technologie, dans un entretien accordé au journal *La Tribune* en 2013.
(http://www.latribune.fr/opinions/tribunes/20131106trib000794337/le-bitcoin-c-est-de-l-or-numerique.html)
[22] Bitcoinwiki (https://en.bitcoin.it/wiki/Mining).
[23] Un ingénieur informaticien américain, Mike Caldwell est à l'origine de ces pièces, appelées "Casascius Bitcoins" (combinaison de la contraction de "call a spade a spade" et du suffixe à consonance latine "cius"). Il

pièces métalliques dorées, "frappées" du signe officiel ฿. L'enjeu de toute cette symbolique est double. Il s'agit d'obtenir l'adhésion d'un public d'utilisateurs qui, sans cela, serait sans doute dérouté, voire rebuté, par le caractère abscons de la technologie qui supporte le Bitcoin : la cryptographie, l'informatique, les mathématiques. Au delà de ce premier obstacle, il faut encore faire admettre l'existence possible d'une monnaie qui ne circulerait que dans la mémoire des ordinateurs. Enfin, et c'est là que nous touchons un point central de la rhétorique associée au Bitcoin, la comparaison avec la monnaie métallique doit permettre de capter une clientèle d'utilisateurs et/ou d'investisseurs qui, dans cette période d'instabilité économique, sont à la recherche d'actifs sûrs. Rappelons ce qu'Alan Greenspan, influencé d'ailleurs par Ayn Rand, écrivait bien avant d'accéder à la présidence du Board du Fed : "Under a gold standard, the amount of credit that an economy can support is determined by the economy's tangible assets, since every credit instrument is ultimately a claim on some tangible asset. (…) Gold (…) stands as a protector of property rights" (Greenspan, 1966).

La référence aux métaux précieux est cruciale relativement aux principes d'émission des Bitcoins. Il s'agirait surtout de libérer la monnaie des imperfections liées à une gestion institutionnelle, dénoncée comme étant inflationniste. En période de *quantitative easing* (assouplissement quantitatif) ayant provoqué un gonflement hors normes des bilans des Banques Centrales, ce type d'arguments reçoit donc des échos favorables (voir par exemple Rochard, 2013). Ainsi, la rhétorique portée par la communauté Bitcoin est fondée sur l'idéologie d'une *monnaie saine*, pure de toute manipulation ou défaillance humaine, tandis que l'identification à la monnaie métallique contribuerait à ancrer la monnaie dans un ordre naturel qui seul pourrait en préserver la valeur. Maurer et *alii* évoquent pour leur part un "matérialisme pratique" ou un "métallisme digital"[24] (Maurer, Nelms et Swartz, 2013). La conception du système fait en sorte que le montant total de bitcoins (21 millions au terme de l'émission), ainsi que le taux annuel d'émission, sont déterminés par le programme informatique lui-même. La rareté de la monnaie est donc inscrite dans le "code", présumé infaillible, qui fait office de règle intangible de politique monétaire. L'idée d'une gestion par la règle, plutôt que par une politique discrétionnaire, s'inscrit dans la longue histoire d'un débat désormais bien connu des théoriciens de la monnaie (Fischer, 1988). Dès 1936, Simons affirmait que "relativement à la monnaie, des règles du jeu définies, stables et relevant de la législation sont de la plus haute importance pour la pérennité d'un système fondé sur la liberté et l'entreprise" (Simons, 1936: 339). La règle permet notamment de contenir l'arbitraire d'une politique monétaire lié au jugement d'une autorité. Mais les lois peuvent être changées. L'incertitude relative à la gestion de la monnaie n'est donc pas complètement éliminée. Dans le cas du Bitcoin, les promoteurs espèrent échapper à cet arbitraire en figeant l'émission dans une règle mathématique : 50 BTC sont émis toutes les 10 minutes pendant les 4 premières années du système ; ensuite, le montant est divisé par 2 pour passer à 25 BTC pendant les 4 années suivantes et ainsi de suite, jusqu'à atteindre la plus petite subdivision et donc le nombre maximum de bitcoins aux alentours de 2140.

L'analyse des influences idéologiques et des valeurs portées par le projet Bitcoin nous renseigne sur la nature de la contestation qui est à l'œuvre, au-delà de l'aspect purement

---

souhaitait assurer la promotion du Bitcoin en l'associant à quelque chose de tangible: "No one is going to get this if I can't show them something".
http://www.bloomberg.com/news/2014-09-30/what-s-a-bitcoin-look-like-popular-photograph-has-story.html

[24] Les expressions "métallisme théorique" et "métallisme pratique" ont été introduites par Schumpeter (Schumpeter, 1954). Le métallisme "théorique" enracine la nature et la valeur de la monnaie dans la marchandise (or). Le "métallisme pratique" renvoie à une méthode de gestion de la monnaie, consistant à définir l'unité de compte par rapport à un poids de métal ou à imposer aux banques la convertibilité-or de leurs monnaies (Schumpeter, 2005).

technologique de l'innovation. Il s'agit bien d'une alternative à un ordre existant. Mais pour que le système Bitcoin s'étende et contribue à faire émerger un nouvel ordre monétaire, encore faut-il qu'il rencontre une forme d'adhésion collective. Nous devons maintenant prolonger la réflexion et nous interroger sur les conditions d'un développement continu et pérenne du Bitcoin.

3. Au delà d'une vision procédurale : le Bitcoin comme ordre monétaire cohérent?

Tandis qu'une démarche purement économique se focalisera sur le problème de la valeur de la monnaie, une approche institutionnaliste devrait privilégier la question de sa légitimité et de son acceptabilité inconditionnelle. Cela est d'autant plus crucial que l'accès libre et le caractère public des programmes qui assurent le fonctionnement du Bitcoin, facilitent grandement la conception d'autres monnaies concurrentes calquées sur la même technologie, ou encore la récupération de cette technologie par l'industrie bancaire. La pérennité du Bitcoin comme système de paiement requiert, non seulement la robustesse des procédés techniques, mais aussi l'émergence d'une forme d'adhésion collective à la crypto monnaie. Dans le cadre d'une démarche institutionnaliste et interdisciplinaire, plusieurs auteurs se sont interrogés sur les caractéristiques communes de la monnaie et ont isolé trois formes de confiance (Aglietta, Orléan, 1998 ; Théret 2008) : méthodique, hiérarchique et éthique. L'articulation cohérente de ces trois formes de confiance est alors indispensable à la stabilité d'un ordre monétaire. Munis de cette grille de lecture théorique, nous mettons alors à jour les tensions dans la conception du système Bitcoin.

3.2. Les deux piliers du Bitcoin : transparence et confiance distribuée

La confiance *méthodique* s'ancre dans la répétition des actes d'échange et le constat du bon fonctionnement des pratiques monétaires : elle fonde le caractère routinier des transactions. La confiance *hiérarchique* repose sur un rapport accepté de subordination à une instance supérieure (l'État, la banque centrale), qui va énoncer les règles d'usage de la monnaie, garantir les moyens de paiement et la valeur des signes monétaires, mais aussi protéger les utilisateurs et représenter une voie de recours en cas de non-respect des règles monétaires. La confiance hiérarchique est supérieure à la confiance méthodique, car l'autorité a le pouvoir de changer les règles liées à la monnaie. La confiance *éthique*, quant à elle, renvoie à la doctrine qui anime l'autorité monétaire. Cela signifie que les politiques de la monnaie doivent être conformes à une certaine idée du bien commun, identifiée pour une société donnée.

Pour les promoteurs du Bitcoin, l'idée est de pouvoir se passer de toute autorité supérieure (notamment des banques et de l'Etat) pour faire fonctionner ce système de paiement et en garantir la pérennité. La robustesse des algorithmes, de la cryptographie et du code suffiraient à enraciner cette routine : "What is needed is an electronic payment system based on cryptographic proof *instead of trust*" (Nakamoto, 2009: 1; nous soulignons). Il ne

s'agit pas tant d'évacuer la question de la confiance, qui reste centrale, mais plutôt de remplacer une forme de confiance (celle qui a été façonnée par l'Etat et les banques) par une autre (celle ancrée par la technologie). Rappelons le slogan inscrit sur les "pièces" : "In cryptography we *trust*". La foi dans le code est assurée par les principes de *transparence* et de *confiance distribuée*[25], qui constituent les deux piliers du système Bitcoin : "Remember that the Bitcoin system shares the virtual registry book among all participants, and that everyone can monitor what all others do" (Iwamura et alii, 2014b, p.16). La transparence[26] se traduit par le caractère public de la chaîne de blocs et permet au destinataire de s'assurer de la solvabilité d'un émetteur. Tous les utilisateurs ont connaissance du compte émetteur, du compte destinataire et du montant de chaque transaction. Avec un tel système, le risque de contrefaçon est nul, puisque tout Bitcoin est traçable depuis sa création jusqu'à l'instant présent. Derrière la transparence revendiquée des protocoles de vérification des transactions, se cache néanmoins pour le profane la complexité des arrangements techniques, le caractère abscons du protocole, l'inaccessibilité d'un langage aussi spécifique que celui de la cryptographie et des mathématiques qui la sous-tendent. Il semble évident que pour l'utilisateur lambda, la confiance méthodique ne saurait être réalisée sur la seule base d'une compréhension du fonctionnement du Bitcoin. Le développement et l'adoption massifs d'un tel système supposent donc que les utilisateurs délèguent le contrôle du bon déroulement des transactions, à la communauté de spécialistes chargée de porter le réseau et d'en comprendre tous les rouages.

En attendant, pour les défenseurs du Bitcoin, la transparence serait suffisante pour assurer la confiance méthodique, tout en évacuant la nécessité d'une confiance hiérarchique. Plutôt : c'est le code qui fait alors office d'autorité hiérarchique. Le code, précisément, a été conçu pour assurer la robustesse du réseau[27]. En effet, les caractéristiques de la solution mathématique recherchée lors du minage sont ajustées par le protocole de telle manière que, compte tenu des variations de la puissance de calcul (c'est-à-dire, du nombre de mineurs entrant dans le système), le temps pour la découvrir demeure de 10 minutes en moyenne. Ainsi plus il y a de mineurs et/ou plus ceux-ci ont du matériel de minage puissant, plus la difficulté augmente. Ceci signifie aussi qu'il est d'autant plus difficile pour un attaquant de prendre le contrôle du réseau : lorsque la difficulté augmente, la robustesse du réseau se renforce. Par ailleurs, la sécurité est positivement corrélée à la valeur d'échange des bitcoins par rapport aux devises officielles. Si le cours du bitcoin monte, l'activité de minage devient plus rentable, ce qui doit logiquement attirer de nouveaux mineurs et donc, augmenter la difficulté de ce travail. Comme nous l'avons souligné dans la première partie, le développement du système Bitcoin génère la formation de "pools" de mineurs, voire de véritables "fermes" de minage qui posent "le problème des 51%" : si un groupe de mineur devait accéder à la majorité de la puissance de calcul dans le système, il pourrait remodeler les blocs de validation à son avantage, pour créditer ses partenaires. Cette configuration était survenue le 12 juin 2014 pour Ghash.io, ce qui avait d'ailleurs provoqué une chute du cours du bitcoin en dollars. Ghash.io, dans un courrier à la communauté Bitcoin, s'était alors engagé à ne pas atteindre ces 51%, ce qui aurait eu pour effet la destruction du système lui-même[28].

[25] Le problème du consensus distribué dans les réseaux P2P a été largement étudié en informatique, de même que la question de robustesse de tels systèmes aux pannes.

[26] La transparence est devenue aujourd'hui une sorte de "Graal" pour un internet démocratique, ouvert sur le monde et accessible à tous. L'exemple de Wikileaks montre comment le réseau internet exacerbe un principe qui semble devenir aujourd'hui incontournable.

[27] Attention, il s'agit ici de la robustesse du réseau, dans sa capacité à authentifier les transactions et éviter toute forme de tricherie du type double dépense. Nous ne parlons pas ici des fraudes liées à l'écosystème Bitcoin en général.

[28] Voir https://ghash.io/ghashio_press_release.pdf

De fait, dans les sept heures qui ont suivi cette révélation, les mineurs ont commencé à quitter le pool et la part de Ghash.io s'est retrouvée réduite à 38%. Cette première expérience tendrait à prouver la capacité d'autorégulation du réseau, celui-ci étant censé fonctionner sur la base d'une majorité de nœuds "honnêtes". L'analyse de la confiance hiérarchique supposerait de creuser la question des modes spécifiques de coordination (horizontale, et non verticale) et de la manière dont les réseaux P2P gèrent les situations de crise : peuvent-ils fonctionner durablement selon un mode décentralisé, ou une centralisation est-elle nécessaire, comme cela fut le cas pour la monnaie bancaire[29] ?

Une autre complication cependant vient des fraudes, escroqueries et autres comportements cupides et spéculatifs, qui accompagnent le développement de l'écosystème Bitcoin[30]. Cela est d'autant plus exacerbé, compte tenu de la très forte valorisation, nécessairement programmée par la règle d'émission de la monnaie cryptographique (limitation de l'offre). Récemment, la faillite frauduleuse de la plateforme Mt Gox en février 2014 et le *hacking* récurrent conduisant au vol de portemonnaies, ont jeté du discrédit sur l'univers Bitcoin. Cet aspect plus sombre, qui ébranle la confiance méthodique, est un point constamment souligné par ses détracteurs, notamment par les autorités bancaires (ECB, 2015, p.21). Pour autant, depuis son lancement le réseau a démontré une certaine "résilience" puisqu'il est parvenu à surmonter plusieurs problèmes (hacking de plateformes d'échange, plusieurs versions de la blockchain etc.).

3.3. L'articulation des niveaux de confiance

Pour qu'une monnaie soit "complète", les divers niveaux de confiance doivent être articulés harmonieusement[31]. Dans le cas du Bitcoin, cela signifierait que les utilisateurs de la monnaie ne s'interrogent pas sur les capacités du réseau à faire face à des problèmes majeurs, ou sur la légitimité des valeurs de la communauté qui le porte. Pour éclairer cette idée, reprenons les propos d' A. Orléan, qui rappelle que, même en l'absence de chocs, de tels questionnements peuvent apparaître lorsque les conditions normales de régulation monétaire se révèlent aux yeux des acteurs comme trop partiales, car favorisant les intérêts spécifiques de groupes particuliers (Orléan 2002). Ainsi par exemple, le règne historique du régime de la monnaie métallique au 19ème siècle est apparu, pour la bourgeoisie, comme le signe d'une monnaie au service de la seule aristocratie. Le papier-monnaie et le crédit bancaire sont ainsi apparus comme un moyen de détendre cette contrainte monétaire stricte imposée par l'offre limitée d'or, ces instruments monétaires nouveaux correspondant mieux à l'esprit d'un capitalisme industriel en expansion.

Dans ce cadre d'analyse, la question consiste à savoir si l'évolution du Bitcoin articule correctement les trois niveaux de confiance : la confiance méthodique, la confiance hiérarchique (relative aux règles institutionnelles) et la confiance éthique (mettant en jeu les valeurs de la société) ?

Au plan éthique, on l'a vu, le réseau s'appuie sur des valeurs libertariennes et vise à s'affranchir de l'arbitraire politique en évitant des manipulations abusives de la part du pouvoir étatique. Cette éthique se propose de rompre avec les "réflexes" séculaires de mutations des autorités souveraines : la confiance dans l'instrument de paiement apparaît

[29] Voir Goodhart (1988) ; Aglietta (1992).
[30] On ne développera pas plus ici les utilisations frauduleuses du Bitcoin. Sur ce point : voir le *Focus* de la Banque de France et l'article de Chevalier et Vignolles (2014).
[31] A propos des crises monétaires, voir les études réunies dans Théret (2007).

clairement à ce niveau éthique comme corollaire d'une confiance dans une communauté nouvellement constituée, dans de nouveaux *commons* (voir Rifkin, 2014). Quant au principe de la transparence, considéré comme la valeur centrale d'une nouvelle démocratie que favoriserait l'utilisation massive du Net, la question est plus épineuse. Si l'idéal de transparence peut s'accommoder d'une posture dissidente et contestataire, largement portée par certaines communautés du Web (Wikileaks par exemple), en revanche, elle semble beaucoup moins compatible avec le principe de l'anonymat dont profitent très largement les activités illicites ou criminelles, rendues possibles par le Bitcoin. Un autre souci vient aussi du design même de la monnaie et surtout, de sa règle d'émission. Celle-ci, on l'a bien compris, est conçue de manière à encourager un nombre croissant de mineurs à participer au fonctionnement du réseau et aux vérifications des transactions. En limitant à terme l'offre de monnaie, cette règle organise la rareté du bitcoin et en fait davantage un instrument de réserve de valeur, voire même un actif spéculatif, ces deux usages venant contrarier très fortement son statut de monnaie. Les détenteurs sont ainsi logiquement incités à stocker les bitcoins, plutôt qu'à les dépenser. C'est ce qu'ont montré notamment Ron et Shamir en analysant le graph du Bitcoin (Ron et Shamir, 2012). Ils ont remarqué que 59,7% des unités bitcoins étaient "dormantes". La même étude a permis d'établir que si 97% des comptes possèdent moins de 10 bitcoins, à l'inverse à peine 78 comptes dans le monde concentrent plus de 10 000 bitcoins chacun. D'après Bitcoinica, 1% seulement des acteurs possèdent 50 % des bitcoins. D'autres chercheurs ont identifié les premières transactions importantes et ont découvert qu'elles provenaient toutes d'une transaction initiale, tandis qu'un seul compte (celui de Satoshi Nakamoto en l'occurrence) avait accaparé à peu près 980 000 bitcoins. Dans l'absolu, ceci tend à dénaturer le modèle initial qui était présenté sur un mode coopératif.

Le procédé d'émission (monnayage) qui consiste à récompenser le mineur qui a résolu l'énigme mathématique pose problème. En effet, la complexification croissante des lignes de code à décrypter pour valider les paiements entraîne une course à l'équipement informatique (*hashrate war*)[32], et affecte la rentabilité du minage. Avec une complexité accrue, du matériel de plus en plus coûteux et une éventuelle baisse du cours, on pourrait logiquement se poser la question de la pérennité de l'activité de minage. Au sein des communautés P2P, une sévère critique du modèle Bitcoin commence à se développer par ailleurs. D'une part, la technologie portée par la chaîne de blocs séduit, en tant qu'innovation susceptible de servir de nouvelles formes d'échange. D'autre part, sont pointés un ensemble de défauts liés au *design* même de la monnaie. Notamment, le Bitcoin reproduirait les caractéristiques d'une monnaie "capitaliste" : accumulation, inégalités et concentration des richesses. Au delà des formes politiques d'idéologie, la communauté ayant adopté le Bitcoin semble être traversée par deux systèmes de valeurs finalement antagonistes, qui renverraient à des points de vue différents sur la place de la monnaie cryptographique dans le monde, et sur les conditions de sa diffusion[33]. D'un côté, on trouverait un groupe d'acteurs et d'utilisateurs motivés par une logique entrepreneuriale, passionnés par les avancées technologiques. Dans cette perspective, les promoteurs seraient surtout préoccupés par les usages du Bitcoin comme système de paiement alternatif et par l'extension croissante de la communauté d'échanges qu'il instaurerait. D'un autre côté, avec une vision radicalement différente, une logique d'investisseurs appréhenderait le Bitcoin principalement comme un actif spécifique permettant la réalisation de gains spéculatifs, l'adoption de la crypto-monnaie dans une optique de dépense et de paiement n'étant considérée que comme un effet secondaire. Ce clivage de la communauté Bitcoin est

[32] "By January 2014, the computational power of the network reached 200 petaflops, roughly 800 times the collective power of the top 500 supercomputers on the globe", Swanson, 2014, p.12.
[33] Voir Daniel Krawisz : "The Two Ideologies in Bitcoin", Oct. 4, 2014, http://nakamotoinstitute.org/mempool/the-two-ideologies-in-bitcoin/#selection-7.4-17.19

intéressant, dans la mesure où il révèle des tensions relatives à l'entreprise de légitimation de la monnaie. Alors que les entrepreneurs sont attentifs à l'image (positive) que devrait renvoyer le Bitcoin comme condition de son adoption généralisée, les investisseurs, n'y voyant qu'un actif comme un autre, ferment les yeux sur les activités illicites qu'il abrite, dans la mesure où elles alimentent une demande soutenue nécessaire à sa valorisation.

Conclusion

La contestation Bitcoin montre que l'histoire de la monnaie est traversée par un conflit entre la sphère politique et la sphère privée pour l'appropriation et la gestion de la monnaie (Courbis, Froment, Servet, 1990). Le caractère disruptif de sa technologie tout comme son potentiel d'innovation, font de la monnaie cryptographique un objet d'étude stimulant, bien qu'elle ne soulève pas de débats fondamentalement nouveaux dans l'histoire des idées monétaires. En effet, *in fine*, c'est toujours la question de la nature de la monnaie qui est en suspens : est-elle une marchandise dotée d'une valeur propre, une institution sociale ou une pure créature de la loi ?

Dans ce travail, nous avons opté pour une perspective institutionnaliste : cela supposait, dans une première étape, de considérer l'idée centrale de la monnaie comme unité de compte. Dès lors que ce choix clair est effectué, les confusions (souvent nombreuses dans les analyses) liées au statut du Bitcoin comme monnaie ou comme actif, disparaissent. Le principe de l'unité de compte doit être nécessairement articulé aux règles qui assurent la circulation des "jetons" électroniques, de sorte à constituer une communauté de paiements. Mais puisque le Bitcoin vient contester un ordre existant, il s'agissait aussi de dépasser une vision purement instrumentale pour tenter de construire une économie politique de cette monnaie cryptographique. La seconde étape a donc consisté à mettre en évidence les valeurs et l'idéologie dont est porteur le projet Bitcoin : la crypto-monnaie agrège dans un alliage étonnant crypto-anarchistes, libertariens et métallistes. Dans une perspective institutionnaliste toujours, nous avons insisté sur le principe de la confiance, qui prévaut sur celui de la valeur. La contestation Bitcoin peut perdurer comme alternative à un système monétaire dont la logique de fonctionnement ne correspond plus aux valeurs d'une frange de la société. Il peut aussi, en tant qu'innovation radicale, augurer un nouvel ordre monétaire et donc, économique. C'est ce que les plus enthousiastes ont tendance à croire. Il peut aussi être étouffé ou stoppé net, comme l'ont été historiquement de multiples expériences de systèmes monétaires complémentaires. Les récents scandales Mt Gox, Bitstamp et MyCoin, qui ont occasionné des pertes très importantes aux usagers, montrent bien que la notion de confiance (et de défiance) est fondamentale pour analyser ce système.

Même si ce travail en est encore à un stade exploratoire, le présent article nous a permis de poser quelques jalons théoriques. Au moyen d'une analyse des formes de la confiance, nous avons montré que la cohérence du système Bitcoin en tant que nouvel ordre monétaire pose problème. Premièrement, vient la question du statut central du code dans la confiance méthodique. Mais derrière le code, n'y a t-il pas un concepteur (le mystérieux S. Nakamoto), une communauté ? Outre le réseau en P2P constitué par les nœuds, comment s'organise cette communauté ? Par quels canaux concrets œuvre-t-elle pour la légitimation de sa monnaie ? Il conviendrait alors d'examiner plus avant une telle organisation, pour comprendre son fonctionnement et spécifier les rôles, statuts et positionnements des différents

acteurs qui la composent : mineurs, promoteurs, responsables de sites officiels, utilisateurs etc. Cette démarche plus empirique devrait faire l'objet d'un travail ultérieur. Deuxièmement, la complétude du système Bitcoin au regard d'une articulation cohérente des formes de confiance, pose problème. Car contrairement à la manière dont est défini officiellement le Bitcoin (un système de paiement), les règles de monnayage et la doctrine monétaire sur laquelle il est fondé en font pour l'instant davantage une marchandise dont la valeur en tant qu'actif prédomine. Il n'y a rien d'étonnant alors, dans le fait qu'apparaissent des tensions entre ceux qui voient dans le Bitcoin l'avènement d'une nouvelle monnaie conforme aux valeurs de la communauté Internet, ceux qui craignent l'absence d'une protection par l'Etat, et ceux qui le considèrent comme une source renouvelée de profits.

Bibliographie

Aglietta, M. (1992), « Genèse des banques centrales et légitimité de la monnaie », *Annales E.S.C.*, vol. 47, n°3, p.675-698.

Aglietta, M., Orléan, A. (1998), (sld), *La monnaie souveraine*, Paris, O. Jacob .

Ancel, P. (1988), « La monnaie électronique : régime juridique », dans *Droit et Monnaie, Etats et espace monétaire transnational*, Paris, Litec, p. 302-315.

Banque de France (2013), « Les dangers liés au développement des monnaies virtuelles », *Focus*, décembre.

Callon, M. (1998), « The embeddedness of economic markets in economics », in Callon (ed.), (1998) *The Laws of the Markets*, Oxford, Blackwell, p. 1-57.

Cartelier, J. (1991**)**, « Monnaie et système de paiement: le problème de la formation de l'équilibre », *Revue française d'économie*, vol. 6, n° 3, p. 3-37.

Cartelier, J. (1996), *La monnaie*, Paris, Flammarion, Dominos.

Chaum, D. (1985), « Security without identification: Transaction Systems to make Big Brother Obsolete », *Communications of the ACM*, vol. 28, n° 10.

Chevalier, M., Vignolles, B. (2014), « Le bitcoin : défi à la souveraineté monétaire des états et ressource pour le blanchiment d'argent », *Regards croisés sur l'économie,* n° 14, p. 122-125.

Clower, R. (1967), « A reconsideration of the microfoundations of monetary theory », *Economic Inquiry*, vol. 6, n° 1, p. 1–8.

Courbis, B., Froment, E., Servet, J.-M. (1990), « A propos du concept de monnaie », *Cahiers d'Economie Politique*, vol. 18, n° 18, p. 5-29.

ECB, (2012), *Virtual Currencies Schemes*, pdf sur http://www.ecb.europa.eu.

ECB, (2015), *Virtual Currency Schemes – A Further Analysis*, pdf sur http://www.ecb.europa.eu.

Fischer, S. (1988), « Rules versus Discretion in Monetary Policy », *NBER Working Papers* 2518.

Fourcade, M., Healy, K. (2007), « Moral Views of Market Society », *Annual review of Sociology*, vol. 33, p. 287-311.

Gazé, P. (2003), « Nouveaux moyens de paiements, nouveaux risques ? », *Les Cahiers du Numérique*, vol. 4, n° 1, p. 93-113.

Goodhart, C. (1988), *The Evolution of Central Banks*, Cambridge Mass., MIT Press.

Greenspan, A. (1966), « Gold and economic freedom », *The Objectivist,* repris dans Ayn Rand, *Capitalism: The Unknown Ideal*, 1986, Penguin, New-York, p.101-107

Grinberg, R. (2011), « Bitcoin: An Innovative Alternative Digital Currency », *Hastings Science & Technology Law Journal,* vol. 4, p. 159-207

Hayek, F. (1976), *Denationalisation of Money -The Argument Refined*. *An Analysis of the Theory and Practice of Concurrent Currencies*, Londres, The Institute of Economic Affairs, 3e edition, 1990.

Ingham, G. (2004), *The nature of money*, Cambridge, Polity Press.

Iwamura, M., Kitamura, Y. et Matsumoto, T., (2014a), « Is Bitcoin the only Cryptocurrency in Town? Economics of Cryptocurrency and Friedrich A. Hayek », accessible sur SSRN.

Iwamura, M., Kitamura, Y., Matsumoto, T., & Saito, K. (2014b) « Can we stabilize the price of a Cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with Central Bank money », accessible sur SSRN

Jeong, S. (2013), « The Bitcoin Protocol as Law, and the Politics of a Stateless Currency », accessible sur SSRN.

Kaplanov, N. (2012), « Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against its Regulation », *Temple University Legal Studies Research Paper*.

Karlstrom, H. (2014), « Do Libertarians dream of Electronic Coins? The material Embeddedness of Bitcoin », *Distinktion: Scandinavian Journal of Social Theory*, vol. 15, n°1, p. 23-36

Keynes, J.M. (1930), *A Treatise on Money : the Pure Theory of Money*, 1930 (I), Londres, MacMillan, *The Collected Writings of John Maynard Keynes*, vol. V, 1971

Knapp, G.F. (1905/1924), *The State Theory of Money*, Londres Macmillan.

MacKenzie, D. (2006), *An Engine, not a Camera: How Financial Models shape Markets*, Cambridge Mass., MIT Press.

Maurer, B., Nelms, T. C., & Swartz, L. (2013), « When perhaps the real problem is money itself!: the practical materiality of Bitcoin », *Social Semiotics*, vol. 23, n° 2, p. 261-277.

Nakamoto, S. (2009a)**,** « Bitcoin: A Peer-to-Peer Electronic Cash System », www.bitcoin.org.

Nakamoto, S., (2009b), « Bitcoin open source implementation of P2P currency », 11 février 2009, *P2P foundation*.

O.C.D.E. (2002), « L'avenir de l'argent », Paris.

Orléan, A. (2002), « La monnaie, opérateur de totalisation », Entretien avec André Orléan réalisé par Françoise Bourdarias, *Journal des anthropologues*, n° 90-91, p. 331-352 http://jda.revues.org/2331.

Ostroy, J.M., Starr, R.M. (1990), « The transactions Role of Money », in *Handbook of Monetary Economics*, B. Friedman and F. H. Hahn, eds, Amsterdam, North Holland, p. 3-62.

Rifkin, J., 2014, *The zero marginal cost society*, New York Palgrave MacMillan.

Rochard, P. (2013), « The Bitcoin Central Bank's Perfect Monetary Policy », *The Mises Circle*, 15 décembre.

Ron, D. and Shamir, A. (2012), « Quantitative Analysis of the Full Bitcoin Transaction Graph », https://eprint.iacr.org/2012/584.pdf

Schumpeter, J. (1954), *History of Economic Analysis*, New York: Allen and Unwin; Londres, Routledge, 2006.

Schumpeter, J. (2005), *Théorie de la Monnaie et de la Banque*, 2 vol., Paris, l'Harmattan.

Servet, J.-M. (1988), « La monnaie contre l'État ou la fable du troc », in Philippe Kahn, éd., *Droit et Monnaie*, Paris, Litec, pp. 49-62.

Simons, H. C. (1936) « Rules versus Authorities in Monetary Policy », *Journal of Political Economy*, vol. 44, p. 1-30.

Swanson, T. (2014), *The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin*, Creative commons

Szczepanski, M. (2014), « Bitcoin: Market, economics and regulation », *European Parliamentary Research Service*, november.

Théret, B. (sld), 2007, *La monnaie dévoilée par ses crises*, Paris, Éditions de l'EHESS.

Théret, B. (2008), « Les trois états de la monnaie. Approche interdisciplinaire du fait monétaire », *Revue Economique*, vol. 59, n° 4, p. 813-841.

Wray, L. R. (2014), « From the State Theory of Money to Modern Money Theory: An Alternative to Economic Orthodoxy », *Economics Working Paper Archive*, wp-792, Levy Economics Institute.