Du monnayage au crypto-monnayage

Ludovic Desmedt, Odile Lakomski-Laguerre

Dialogues d'histoire ancienne.
Supplément

Du monnayage au crypto-monnayage

Ludovic Desmedt, Odile Lakomski-Laguerre

Résumé
Récemment, les procédures traditionnelles d'émission et de transfert d'instruments de paiement ont été perturbées par l'irruption des cryptomonnaies. Depuis 10 ans, la prolifération de ces circuits de règlements numériques et alternatifs attire l'attention. Nous revenons dans cet article sur l'assimilation souvent pratiquée entre les cryptomonnaies et les monnaies métalliques : après avoir évoqué les fondements idéologiques et techniques, nous exposons les raisons pour lesquelles la référence aux métaux est omniprésente. Pour finir, nous détaillons les opérations de monnayage, les processus de marquage et la question du seigneuriage.

Abstract
Minting Techniques in Currencies and Cryptocurrencies.
Over the past ten years, the creation of bitcoin and other cryptocurrencies has renewed the debate on the nature of money. This paper discusses the comparison between cryptocurrencies and coins : after describing their ideological and technical foundations, we explain the reasons why the reference to metals is often invoked. We then detail the techniques of minting, the processes of marking, and the question of seigniorage.

Dialogues d'histoire ancienne supplément 20, 2020, 143-156

Du monnayage au crypto-monnayage

Ludovic Desmedt
Université de Bourgogne-Franche Comté – LEDI
ludovic.desmedt@u-bourgogne.fr

Odile Lakomski-Laguerre
Université Picardie Jules Verne, Amiens – CRIISEA
odile.lakomski@u-picardie.fr

> « When I asked a Bitcoin trader about the theory of money underlying his understanding of cryptocurrency, he compared Bitcoin to gold; indeed he suggested that the currency was superior to gold because its supply could be absolutely fixed (at 21 million coins) by the underlying software. »[1]

Bitcoin est un système de signes cryptographiques distribués via internet et affichés comme instruments de paiement. Littéralement « espèces constituées par des unités d'information » (*bits*), l'idée de ce protocole a été rendu public dans un document publié sur internet fin 2008 par un certain Satoshi Nakamoto (un pseudonyme). Selon ce(s) mystérieux concepteur(s) du bitcoin.

> Le problème fondamental de la monnaie conventionnelle est la confiance qu'elle requiert. Il faut faire confiance à la banque centrale pour ne pas dévaluer la monnaie, mais l'histoire des monnaies fiduciaires est remplie de ruptures de cette confiance. Il faut faire confiance aux banques pour détenir notre argent et le transférer par voie électronique, mais elles le prêtent en alimentant des bulles de crédit[2].

Le projet bitcoin se présente donc comme une rupture dans l'histoire monétaire et, si l'on suit le raisonnement, la cryptographie et les réseaux informatiques permettraient à leurs utilisateurs de construire des espaces marchands hors « monnaie

1 Dodd 2017a, p. 10.

2 Nakamoto 2009.

conventionnelle », sans banques, basés sur des relations interindividuelles. Nakamoto a (ont) lui (eux) même(s) « miné » les 50 premiers bitcoins le 3 janvier 2009, puis l'expansion s'est produite de manière virale : 10 ans plus tard, ce projet qui pouvait sembler utopique, s'est concrétisé car on dénombre aujourd'hui plus de 1 500 cryptomonnaies (litecoins, ripple, ethereum, dogecoin…), avec une valeur totale de ces instruments estimée en dollars à plus de 300 milliards[3]. Les protocoles de codage introduisent une nouvelle logique de transfert entre agents : un simple accord entre deux parties (peer-to-peer) suffirait pour opérer des paiements, la cryptographie assurant un niveau de sécurité suffisant. Dans la majorité de ces systèmes, les unités de paiement sont enchaînées en « blocs » (technique de la blockchain) et la vérification/validation continuelle de la communauté des utilisateurs rendrait ces instruments infalsifiables. Il existe donc un protocole de monnayage assurant la sécurité des transferts.

Paradoxalement, alors que des centaines de crypto-monnaies proposent de contourner les circuits traditionnels à l'aide de procédés cryptographiques, l'imagerie et les concepts repris par les zélateurs de ces instruments font abondamment référence aux monnaies anciennes. Sites, blogs, plateformes et écrits soulignent à l'envi le lien avec les moyens de paiement métalliques, tangibles et ancrés dans la nature : on paie en espèces (*coins*), on « frappe » ces instruments, les membres des communautés sont qualifiés de « mineurs », les outils de prospection sont souvent représentés sur les sites de minage… Pour de nombreuses cryptomonnaies, le processus de monnayage est original : le seigneuriage est décentralisé, puisque ce sont les « mineurs » (calculateurs) les plus rapides qui résolvent un défi numérique et obtiennent une rémunération. Au départ, cette rémunération en bitcoins était de 50 unités toutes les 10 minutes, de 12,5 unités désormais. Mais afin d'éviter les accusations de création infinie de moyens de paiement, l'extinction peut être programmée dès l'origine dans le code source : au seuil de 21 millions d'unités de bitcoins créées, la rétribution disparaîtra. Le nombre de *litecoins* a été fixé à 84 millions d'unités, etc. À propos de cette rareté programmée, qui ferait de certaines cryptomonnaies une nouvelle espèce d'« or numérique », certains auteurs évoquent un « métallisme digital »[4]. Si le digital s'ancre (symboliquement) dans le minéral, on exclut le politique. En effet, dans l'imaginaire collectif, la monnaie

[3] La Banque de France préconise depuis mars 2018 l'usage du terme « crypto-actifs », mais nous conservons dans ce texte l'appellation traditionnellement utilisée, traduction du terme *cryptocurrency* anglais. « L'encours des crypto-actifs en circulation atteint environ 330 milliards d'euros fin janvier 2018, comprenant principalement le bitcoin (35 %), l'ether (20 %) et le ripple (10 %). », Banque de France 2018, p. 3.

[4] Maurer, Nelms, Swartz 2013.

métallique aurait l'avantage d'être soustraite à l'arbitraire d'un pouvoir politique très enclin à manipuler les cours (dévaluations ou réévaluations, etc.)[5]. Le sociologue Nigel Dodd précise

> Although it is a virtual currency, the philosophy behind it implies that we must think of money as a thing: an asset whose value must be zealously protected over time[6].

Ainsi, les cryptomonnaies façonnent un alliage étonnant de modernité digitale et d'archaïsmes métallistes, ce qui explique certainement une partie de leur pouvoir d'attraction[7]. L'argumentaire déployé pousse à s'interroger sur les processus de monnayage en général, c'est-à-dire l'opération qui consiste à mettre à disposition des individus des moyens de paiement. Historiquement, la frappe des monnaies supposait un processus de transformation de la matière (métal ou papier) qui nécessitait un travail collectif en atelier. Certes, le rôle de plus en plus accessoire des presses rend le processus de monnayage plus abstrait, mais la dématérialisation n'est pour autant pas accomplie : le monnayage, même digital, réclame d'intenses dépenses, comme nous le verrons.

C'est le rapport ambigu des cryptomonnaies au monde des monnaies métalliques que nous proposons de traiter ici : dans une première section, nous évoquerons les fondements idéologiques et techniques. Nous exposerons ensuite les raisons pour lesquelles la référence aux métaux est omniprésente, puis nous reviendrons plus en détail sur les opérations de monnayage, les processus de marquage et la question du seigneuriage.

Origines et influences

Au cours des trois 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 1980, 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

5 Rappelons ce qu'Alan Greenspan, influencé par les idées ultraliberales d'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.

6 Dodd 2017b, p. 241.

7 Le lancement fin 1997 de *Bitcoingold*, un embranchement (ou fork) de bitcoin prévu pour constituer une « meilleure réserve de valeur », joue sur cette attraction.

Obsolete »[8]. 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 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'État et du contrôle que celui-ci exerce sur les informations relevant de la sphère privée. Les idées exposées par Chaum 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 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[9].

La « B-Money » de Wei Dai était explicitement associée aux cypherpunks et aux idées de Timothy May[10] pourtant, Satoshi 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[11]. Ce lien n'aurait rien

8 Chaum 1985.

9 Jeong 2013.

10 Kaplanov 2012 ; Grinberg 2011.

11 Auteur de romans comme d'essais, Rand a su rassembler autour d'elle des intellectuels et des politiques opposés à « l'esprit du New Deal ». En économie, elle aurait été influencée par von Mises.

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[12]. Les préoccupations ne sont pas seulement d'ordre technique (sécurisation des données par le cryptage), elles sont aussi philosophiques et politiques : il s'agit de réfléchir aux moyens de contourner le monopole acquis par l'État pour le contrôle de l'offre de monnaie et de restituer les pleins pouvoirs d'utilisation de celle-ci à la communauté.

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. 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 État) 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[13]. 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. Certains travaux interprètent ainsi l'univers concurrentiel des crypto-monnaies dans la perspective d'un processus de sélection naturelle à la Hayek. 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 » développée au sein de la tradition autrichienne. 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[14]. En mai 2015, un instrument basé sur la technologie blockchain du nom de « *HayekGold* » a été proposé par la firme Anthem Vault, cet instrument est présenté comme « or digital ». Cette référence n'est pas anodine.

Un retour au métallisme ?

Ce qui ressort dès l'origine du projet, c'est la volonté affichée d'offrir une monnaie « saine » et sûre. La sûreté serait garantie par le codage, mais le Bitcoin est

12 Karlstrom 2014.

13 Hayek 1976.

14 Iwamura *et al.* 2014.

également porté par une rhétorique évoquant le régime monétaire métallique[15]. 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[16]. 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[17].

Ainsi, sur *Bitcoin.mining*, une 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 représentant le Bitcoin sous la forme de 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 algorithmes. Au-delà de ce premier obstacle, il faut encore faire admettre l'existence possible d'une monnaie qui ne circulerait que dans les cartes mémoires 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. Dans le même ordre d'idées, les promoteurs du Bitcoin s'efforcent de présenter cet instrument comme a-politique et a-bancaire :

[15] 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).

[16] C'est de cette façon que le qualifie P. Herlin, par ailleurs très enthousiaste à l'égard de cette technologie, dans un entretien accordé au journal *La Tribune* en 2013.

[17] Bitcoinwiki. Voir : https://en.bitcoin.it/wiki/Mining.

> 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[18].

La référence aux métaux précieux est cruciale relativement aux principes d'émission des Bitcoins : le métal est un actif net, et il comporte une restriction naturelle qui éviterait sa surémission. 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, soient déterminés par le programme informatique lui-même. Ainsi, la rareté de la monnaie est 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[19]. 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[20].

La règle permet notamment de contenir l'arbitraire d'une politique monétaire lié au jugement d'une autorité. Dans le cas du Bitcoin, les promoteurs espèrent échapper à l'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 et ainsi de suite, jusqu'à atteindre la plus petite subdivision et donc le nombre maximum de bitcoins dans quelques décennies.

Selon Nakamoto, si chacun devient vérificateur et appose son sceau sur les transactions, on peut se passer des banques et des États. Encore faut-il éviter la circulation de fausses créances ou l'accumulation de doubles paiements… C'est pourquoi le principe proposé dans le programme initial consiste à créer des unités de paiement enchaînées en « blocs ». La validation continuelle de la communauté des utilisateurs de ces blocs rendrait les bitcoins infalsifiables. Chaque unité transporte donc avec elle la mémoire des transactions (de A à B à C…), mais cette mémoire est cryptée. Ainsi, toute nouvelle transaction (depuis la dernière validation de bloc) est transmise à tous les nœuds de calculs. Si quiconque tente de modifier une seule information à l'intérieur du bloc (et donc de modifier l'historique des transactions passées), l'empreinte n'est plus valable.

18 http://www.bitcoin.fr/pages/Vices-et-vertus#main.

19 Fischer 1988.

20 Simons 1936, p. 3.

La vérification de la circulation entre agents est assurée par un protocole diffusé via un logiciel libre (*open source*).

Derrière l'apparente neutralité du code informatique et des algorithmes se trouve une logique de contestation : les cryptomonnaies véhiculent ainsi des valeurs et rassemblent une communauté porteuse d'un projet politique qui consiste à libérer la monnaie de l'État et des banques. Pour ses partisans, le bitcoin constitue une « insurrection », voire une « révolution » menée sur le terrain des moyens de paiement[21]. L'identification à la monnaie métallique contribuerait à ancrer la monnaie dans un ordre naturel qui seul pourrait en préserver la valeur. Le « matérialisme pratique » ou « métallisme digital »[22] en vogue dans les communautés utilisatrices de *bitcoins, dogecoins, litecoins*… contribue à ancrer ces instruments dans un ordre naturel, ce qui les immuniserait des manipulations humaines :

> the ideology behind Bitcoin is essentially that it removes politics from money altogether – hence the strong parallels between Bitcoiners and goldbugs[23].

Crypto-monnayage, marquage et seigneuriage

La rhétorique portée par la communauté cryptomonétaire est fondée sur l'idéologie d'une monnaie délestée de toute manipulation ou défaillance humaine. En période de *quantitative easing* (assouplissement quantitatif) ayant provoqué un gonflement hors normes des bilans des Banques Centrales, ce type d'arguments reçoit des échos favorables. La gestion institutionnelle et discrétionnaire est dénoncée comme étant inflationniste[24]. Selon Selgin, Bitcoin appartiendrait au monde des monnaies « synthétiques », qui conjugueraient à la fois des aspects de monnaies marchandises et des monnaies décrétées (*fiat*). Depuis longtemps préoccupé par la limitation du pouvoir d'émission des Banques centrales, Selgin estime qu'il n'existe pas de « rareté absolue » des monnaies « synthétiques » mais que leur quantité peut être gérée.

21 Voir Desmedt, Lakomski-Laguerre 2015.

22 Maurer, Nelms, Swartz 2013.

23 Dodd 2017a, p. 3.

24 Voir par exemple Rochard 2013.

		Nonmonetary Use?	
		Yes	**No**
Scarcity	**Absolute**	Commodity	Synthetic Commodity
	Contingent	Coase Durable	Fiat

Figure 1 : Base Money Types. Selgin 2015.

Pour illustrer son propos, cet auteur fait le parallèle avec la monnaie-papier et évoque le montant maximal programmé de beaucoup de cryptomonnaies comme l'équivalent d'une destruction des presses dans le cas des monnaies métalliques ou papier. Ainsi, la « marchandise synthétique » fait figure d'imitation de son modèle historique : « Bitcoin's so-called money system tries to mimic metallic money »[25]. En effet, le plafonnement programmé à l'origine apparaît comme une fiction, car aucune limite naturelle n'interdit la levée de cette restriction et un programmateur pourrait très bien la remettre en cause à un moment particulier. Pourtant, même pour ses utilisateurs, cette « fiction est nécessaire »[26] car le dépassement du plafond saperait la confiance des acteurs du réseau. Mais, répétons-le, aucune limite physique n'existe. Selgin lance l'idée que la concurrence entre cryptomonnaies pourrait éviter la surémission.

Que ce soit avec le métal, le papier ou les virements, deux éléments sont primordiaux pour les opérations de monnayage : l'émission doit se faire à une échelle suffisante (que le territoire soit limité à une ville, une région, une nation ou au-delà) et la sécurisation des moyens de paiement doit être assurée. Ainsi, on attend de l'émetteur qu'il garantisse une diffusion des instruments adéquate aux besoins du commerce, tout en évitant que des agents émettent de « faux droits ». C'est la raison pour laquelle la contrefaçon est un problème de grande envergure, depuis le monnayage métallique jusqu'aux problèmes actuels de cybersécurité. Dans un régime de pièces métalliques (*coins*), la frappe transforme des minerais en disques de taille uniforme, de poids et de teneur métallique certifiés, reconnus et acceptés comme instruments de paiement dans les transactions. L'impression de billets met également à contribution une presse qui transforme une collection de fibres diverses en moyen de paiement légal. L'opération de poinçonnage ou de marquage doit rendre dans les deux cas le faux-monnayage difficile,

25 Weber 2016, p. 19.

26 Voir Dodd 2017a.

coûteux, voire impossible. Or, dans l'univers digital, « la duplication est aisée »[27], c'est pourquoi la création de bitcoins réclame un effort (une « proof of work ») qui donne droit à une rémunération. Le « travail », en l'occurrence consiste à résoudre un défi numérique : le premier « mineur » à avoir résolu ce défi est crédité en bitcoins.

> we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change [...]. The network is robust in its unstructured simplicity[28].

Dans l'univers digital, il y a donc bien poinçonnage et marquage des unités. Chaque unité transporte avec elle la mémoire des transactions sous forme cryptée. On l'a dit, toute nouvelle transaction (depuis la dernière validation de bloc) est transmise à tous les nœuds de calcul sans intervention d'« intermédiaires de confiance » (comme c'est le cas dans les paiements par carte bancaire ou via PayPal). D'un point de vue économique, la qualité de chaque bitcoin peut d'ailleurs représenter *in fine* une faiblesse : puisque chaque unité transporte la mémoire de chaque transaction à laquelle elle a été liée, toutes les unités sont intrinsèquement différentes.

> This quality of bitcoin led some developers to the concept of "colored coins", which would be specially marked bitcoin based on particular ownership or transaction histories, precisely to track their origins and pathways[29].

Cette garantie d'unicité qui leur confèrerait un caractère infalsifiable pose en fait une hypothèque sérieuse : pour éviter d'utiliser des bitcoins ayant été utilisés par certaines adresses proscrites ou inclus dans des transactions illégales, les agents pourraient être amenés à sélectionner entre « bonnes » et « mauvaises » unités[30].

À la suite de Nakamoto et des promoteurs des cryptomonnaies, on soutient souvent que « l'émission décentralisée d'une monnaie virtuelle n'implique aucun revenu de seigneuriage, contrairement à l'émission centralisée d'une monnaie fiduciaire. »[31] Rappelons que le seigneuriage est l'avantage financier qui découle

27 Maurer 2017, p. 219.

28 Nakamoto 2008.

29 Maurer 2017, p. 226-227.

30 « Bitcoins are not alike. Each transaction is a descendant of a unique transaction history, which is readily available in the public blockchain. Therefore, markets participants can, in principle, scrutinize the history and become selective in which transactions they accept; or, with more granularity, how much they value it. The fact that most participants do not differentiate for the time being is hard to justify with economic rationality. », Möser, Böhme, Breuker 2014, p. 12. Sur les processus de marquage et de différenciation des monnaies actuelles, vois les travaux de V. Zelizer.

31 Figuet 2016, p. 328.

de la mise à disposition d'une monnaie. Dans le cas des monnaies et billets émis par les autorités, il est égal au montant émis moins les coûts de fabrication (à ce revenu s'ajoutent les intérêts de refinancement du système bancaire par l'institut d'émission). Dans le cas de la monnaie scripturale (dépôts bancaires sur des comptes), ce sont les banques commerciales qui bénéficient de l'avantage financier du seigneuriage. Les cryptomonnaies, sans seigneur (« acéphales », pour reprendre l'expression de Favier et Takal-Bataille[32]), n'engendreraient logiquement aucun seigneuriage. Cet aspect est contestable : on peut plutôt parler, à la suite de Weber, de « subvention croisée » car l'investissement en matériel et en énergie est non négligeable. Ces fonds investis offrent à certains compétiteurs la puissance de calcul nécessaire, donc la rapidité essentielle pour valider un bloc avant les autres et obtenir une rémunération. Le coût de mise à disposition d'instruments de paiements à la communauté est donc supporté par les mineurs (également utilisateurs) qui doivent rémunérer leurs fournisseurs d'énergie ou d'équipement informatique :

> In the Bitcoin world, costs for payment processing do occur in the form of investment and energy costs for running computers. But the way the system is designed provides for an internal cross-subsidy with seigniorage in money "mining". Each node successful in a bidding contest for processing a transaction is awarded with a certain sum of newly mined bitcoins. Therefore, nodes are willing to process payments with practically no cost charged to customers[33].

Ainsi, la dématérialisation de la monnaie apparaît très largement comme un mythe. Certes, historiquement, la frappe des monnaies supposait un processus de transformation de la matière (métal ou papier) qui nécessitait un travail collectif en atelier. Le rôle de plus en plus accessoire des presses rend le processus de monnayage plus abstrait, mais la dématérialisation n'est pas accomplie : le monnayage, même digital, réclame d'intenses dépenses d'énergie, l'utilisation de logiciels, la production de matériel *hardware*. Le crypto-monnayage est lui aussi dépendant de matières premières sans lesquelles il ne fonctionnerait pas.

Conclusion

> Money is supposed to be a means of buying things. Now, the nation's hottest investment is buying money[34]

32 Favier, Takal-Bataille 2017.

33 Weber 2016, p. 27-28.

34 New York Times, 28 février 2018.

En tout temps, le droit de « battre monnaie » suppose l'exercice d'un pouvoir : lors de cette opération, un des agents profite d'une position privilégiée pour contrôler les émissions au sein d'une communauté.

> Money is created when a stakeholder uses its singular location at the hub of a community to mark the disparate contributions of individuals in a common way[35].

Le pouvoir de celui qui produit la monnaie peut être politique, économique ou technique, il en retire une rente, sous forme de seigneuriage, intérêt ou commission. Ainsi, la diffusion des moyens de paiement suppose le contrôle des réseaux : Hôtels des monnaies maillant un territoire, correspondants bancaires ou plateformes internet. Que ce soit dans l'argumentaire de Nakamoto, ou celui de Matthew Boulton, qui employait la machine à vapeur pour frapper des pièces à la fin du XVIII^e^ siècle, l'on retrouve les mêmes tropismes : l'importance de la mécanisation (le monnayage est la première industrie à produire en masse), l'obsession de la sécurité (symboles et codes ont toujours orné pièces et billets)[36].

Dans ses récents travaux consacrés au phénomène bitcoin, Nigel Dodd[37] discute ce qui selon lui est mis en avant lorsque l'on présente cette cryptomonnaie : le réseau serait « plat » (*flat*), sans hiérarchie. En fait, l'existence d'une équipe de développeurs (*development team*) ou les discussions entre groupes d'experts (*Bitcoin Classic* versus *Bitcoin Core*) relativisent ce premier argument. Dans le projet bitcoin, il existe bien une hiérarchie entre concepteurs-contributeurs et simples utilisateurs, ce que revendique d'ailleurs le site officiel : trois *maintainers* et une quinzaine de *contributors* sont nommément présentés. Que ce soit dans la configuration d'Hôtel des monnaies ou de communautés virtuelles, il existe des différences de statuts irréfragables, car le monnayage suppose d'occuper une position nodale au sein d'un réseau[38].

Trois autres aspects sont discutés par Dodd : selon ses adeptes, le système offrirait des solutions technologiques très fiables aux problèmes de gouvernance monétaire (anti-inflationniste) ; il rendrait superflue la confiance entre échangistes ; enfin Bitcoin serait une « monnaie sans dette », à l'instar de l'or (actif « naturel »). On l'a dit, l'absence de limite physique à l'émission des cryptomonnaies est contestable : la règle

35 Desan 2014, p. 43.

36 « I have executed and perfected such an apparatus or Machinery as will make Coin not only superior in Beauty & Workmanship to that of any Nation in Europe but also so manufactured… that Counterfeiting will be prevented. », Matthew Boulton au Comité du Conseil Privé sur les espèces, décembre 1789.

37 Dodd 2017a et 2017b.

38 Certaines cryptomonnaies sont d'ailleurs centralisées, à l'instar du *ripple*.

de plafonnement peut être modifiée dans le futur ou, pour reprendre l'image souvent utilisée, le stock « d'or virtuel » pourrait être accru par simple décret des développeurs. Ensuite, la confiance est bien présente : elle porte non seulement sur le cryptage (et donc une foi dans l'infaillibilité technique), mais aussi sur le mode de coordination et de gouvernance de la communauté. Par exemple, alors que la décentralisation complète constitue un des piliers de l'écosystème cryptomonétaire, des forces économiques ont amené à une centralisation et une concentration d'un petit nombre d'intermédiaires à différents niveaux. Ce processus pourrait menacer l'adhésion au projet. Enfin, il est clair que les fortes variations des cours indiquent les motivations spéculatives de nombreux utilisateurs : pour beaucoup d'acteurs, les cryptomonnaies représentent bien des crypto-actifs, acquis pour être thésaurisés puis revendus[39].

Bibliographie

Banque de France (2018), « L'émergence du bitcoin et autres crypto-actifs : enjeux, risques et perspectives », *Focus*, 16, p. 1-6.

Chaum D. (1985), « Security without Identification: Transaction Systems to Make Big Brother Obsolete », *Communications of the ACM*, 28/10, p. 1029-1044.

Desan C. (2014), *Making Money: Coin, Currency and the Coming of Capitalism*, Cambridge.

Desmedt L., Lakomski-Laguerre O. (2015), « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la Régulation*, 18, 2e semestre, en ligne [DOI : 10.4000/regulation.11489].

Dodd N. (2017a), « The Social Life of Bitcoin », *Theory, Culture & Society*, en ligne [http://eprints.lse.ac.uk/69229].

Dodd N. (2017b), « Utopian Monies: Complementary Currencies, Bitcoin, and the Social Life of Money », dans N. Bandelj, F. Wherry, V. Zelizer (éds), *Money Talks, Explaining How Money really Works*, Princeton, p. 230-247.

Favier J., Takal-Bataille A. (2017), *Bitcoin, la monnaie acéphale*, Paris.

Figuet J. M. (2016), « Bitcoin et blockchain : quelles opportunités ? », *Revue d'Économie Financière*, 123, p. 325-340.

Fischer S. (1988), « Rules *versus* Discretion in Monetary Policy », *NBER Working Papers*, en ligne [DOI : 10.3386/w2518].

[39] La création d'instruments dérivés sur bitcoin au *Chicago Board Options Exchange* et *Chicago Mercantile Exchange* fin 2017 alimente les attitudes spéculatives.

Greenspan A. (1966), « Gold and Economic Freedom », *The Objectivist* [repris dans A. Rand, *Capitalism: the Unknown Ideal*, 1986, New-York, p. 101-107].

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

Hayek F. (1976), *Denationalisation of Money – The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*, Londres [3e edition, 1990].

Iwamura M., Kitamura Y., Matsumoto T. (2014), « Is Bitcoin the only Cryptocurrency in Town? Economics of Cryptocurrency and Friedrich A. Hayek », *SSRN Electronic Journal* [DOI : 10.2139/ssrn.2405790].

Jeong S. (2013), « The Bitcoin Protocol as Law, and the Politics of a Stateless Currency », *SSRN Electronic Journal* [DOI : 10.2139/ssrn.2294124].

Kaplanov N. (2012), « Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against its Regulation », *Temple University Legal Studies Research Paper*, p. 111-157.

Karlstrom H. (2014), « Do Libertarians Dream of Electronic Coins? The Material Embeddedness of Bitcoin », *Distinktion: Scandinavian Journal of Social Theory*, 15/1, p. 23-36.

Maurer B. (2017), « Blockchains Are a Diamond's Best Friend », dans N. Bandelj, F. Wherry, V. Zelizer (éds), *Money Talks, Explaining How Money really Works*, Princeton, p. 215-229.

Maurer B., Nelms T. C., Swartz L. (2013), « When Perhaps the Real Problem is Money Itself! The Practical Materiality of Bitcoin », *Social Semiotics*, 23/2, p. 261-277.

Möser M. Böhme R., Breuker D., (2014), « Towards Risk Scoring of Bitcoin Transactions » dans *Proceedings of the 1st Workshop on Bitcoin Research in Assocation with Financial Crypto 14*, Barbade, p. 16-32.

Nakamoto S. (2009) « Bitcoin Open Source Implementation of P2P Currency », *P2P foundation* [en ligne].

Nakamoto S. (2008), « Bitcoin: a Peer-to-Peer Electronic Cash System », www.bitcoin.org.

Rochard P. (2013), « The Bitcoin Central Bank's Perfect Monetary Policy », *The Mises Circle* [en ligne : https://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy/].

Selgin G. (2015), « Synthetic Commodity Money », *Journal of Financial Stability*, 17, p. 92-99.

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

Schumpeter J. (1954 [2006]), *History of Economic Analysis*, New York-Londres.

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

Weber B. (2016), « Bitcoin and the Legitimacy Crisis of Money », *Cambridge Journal of Economics*, 40, p. 17-41.

Zelizer V. (2005), *La signification sociale de l'argent*, Paris.