



HAL
open science

Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique

Pierre-Henri Faure

► To cite this version:

Pierre-Henri Faure. Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique. 2016. hal-01337694

HAL Id: hal-01337694

<https://hal.science/hal-01337694>

Preprint submitted on 27 Jun 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Le bitcoin peut-il être assimilé à une monnaie ?

Un examen à partir des différentes grilles de lecture de la science économique

Pierre-Henri Faure

LAREFI Working Paper N°2016-07

2016

<http://lare-efi.u-bordeaux4.fr>

LAREFI

Université Montesquieu-Bordeaux IV
Bâtiment Recherche Economie – 1^{er} étage
Avenue Léon Duglît – 33 608 Pessac

PEPS « Monnaies virtuelles »

LAREFI – LABORATOIRE D'ANALYSE ET DE RECHERCHE EN ECONOMIE ET FINANCES INTERNATIONALES

AUTHORS

Pierre-Henri Faure, LAREFI, Université Montesquieu Bordeaux IV

NOTICES

LAREFI Working Papers contain preliminary material and research results. They have been peer reviewed. They are circulated in order to stimulate discussion and critical comment; any opinions expressed are only those of the author(s).

Copyright LAREFI. All rights reserved. Sections of this material may be reproduced for personal and not-for-profit use without the express written permission of but with acknowledgment to LAREFI. To reproduce the material contained herein for profit or commercial use requires express written permission. To obtain permission, contact LAREFI at cyril.mesmer@u-bordeaux4.fr.

PEPS « Monnaies virtuelles »

Le bitcoin peut-il être assimilé à une monnaie ?

Un examen à partir des différentes grilles de lecture de la science économique

Pierre-Henri Faure

Larefi — Université de Bordeaux

pierre-henri.faure@u-bordeaux.fr

Juin 2016

Résumé

La multiplication sur Internet des nouveaux instruments de paiement virtuels recourant à la cryptographie interpelle aujourd'hui les économistes sur leur conception de la monnaie, en même temps qu'elle remet en question l'organisation pyramidale du système bancaire. Leur émission privée et leur circulation dans des réseaux pair-à-pair, au sein desquels n'existe plus aucun tiers de confiance désigné, contestent en effet l'ordre monétaire fondé sur le crédit et les banques centrales. Le présent papier s'intéresse au bitcoin, le plus emblématique de ces instruments virtuels, et traite la question de savoir s'il peut être réellement considéré comme une monnaie au sens où l'entendent les économistes. Il apparaît en première analyse qu'il ne remplit que très imparfaitement les trois fonctions qui lui sont habituellement dévolues et qu'il s'apparente surtout à un actif financier. Le bitcoin est ensuite étudié à partir de l'approche réaliste en privilégiant le point de vue de l'école économique autrichienne, compte tenu du soubassement intellectuel des idées défendues par ses promoteurs ; dans ce cadre, deux points sont plus particulièrement abordés : sa compatibilité avec le théorème de régression puis la comparaison des projets actuels avec la proposition hayékienne de dénationalisation des monnaies. Le cas du bitcoin est enfin examiné dans la perspective du paradigme hétérodoxe qui combine la conception institutionnaliste et la pensée post-keynésienne. En conclusion, s'il peut être vu comme une sorte de mise à l'épreuve des thèses autrichiennes, son caractère totalement exogène et son incapacité à satisfaire les différentes formes de confiance qui sont indispensables à la légitimation de la monnaie conduisent à lui refuser ce qualificatif dans la grille de lecture institutionnaliste.

Mots-clés : bitcoin, cryptomonnaie, école autrichienne, institutionnalisme, post-keynésianisme

Classification JEL : B25, B52, B53, E42, 033

PEPS « Monnaies virtuelles »

« Il se pourrait bien qu'il y ait moins de banques centrales à l'avenir, et leur disparition ne peut être écartée. Les sociétés ont fonctionné sans banques centrales par le passé. Elles pourraient le faire à nouveau dans le futur. »

Mervyn King, *Challenges for Monetary Policy: New and Old*,
extrait d'un discours donné à Jackson Hole le 27 août 1999

Apparue en janvier 2009, la monnaie virtuelle bitcoin a su susciter, en l'espace de quelques années seulement, un véritable engouement auprès de nombreux internautes, pour des raisons qui tiennent à la fois du contexte et de la technologie. Le contexte d'abord, puisque le projet de son mystérieux créateur, qui se cache derrière le pseudonyme de Satoshi Nakamoto, s'inscrit clairement en réaction aux turbulences de 2007 et 2008, qui ont jeté, par leur ampleur, un discrédit quasi total sur les pratiques des banques et plus largement le monde de la finance. Ce discrédit s'est alors traduit par la volonté de contourner le système bancaire au moyen d'une monnaie sur laquelle celui-ci n'aurait aucun contrôle. La technologie ensuite, parce le protocole à l'origine du bitcoin est révolutionnaire et permet la concrétisation de cette volonté à travers un modèle de règlement des transactions radicalement différent de celui associé aux monnaies officielles, car entièrement décentralisé, indépendant de toute autorité et néanmoins sécurisé grâce aux progrès de la cryptographie mathématique. Le bitcoin se présente ainsi comme une monnaie mondiale qui n'est rattachée à aucun État et où le tiers de confiance n'est autre que la communauté de ses utilisateurs. Il attire aussi bien les *geeks* passionnés par l'informatique et les nouvelles technologies que ceux qui se réclament des mouvances anarchiste et libertarienne et qui voient dans cette invention l'occasion de contester la puissance publique ou la finance mondiale. L'engouement pour ce type de monnaie s'est en outre trouvé grandement favorisé par le choix de mettre librement à disposition le code source du logiciel, de sorte que les programmeurs peuvent le reprendre et le modifier dans le sens qu'ils souhaitent, d'où la multiplication très rapide des devises dématérialisées sur Internet, chacune possédant ses propres spécificités et répondant à des besoins ou des goûts particuliers¹.

Le bitcoin est pourtant loin d'avoir bonne presse, car son utilisation est souvent associée au Darknet, le côté obscur de la toile. L'anonymat des transactions permis par la cryptographie se révèle en effet propice aux actions frauduleuses², et le recours à la monnaie virtuelle fait désormais partie des techniques de blanchiment d'argent employées par les trafiquants. L'absence de cadre légal fait également peur, et de nombreux pays ont déjà formulé des mises en garde sur les risques

1 On compterait aujourd'hui plus d'un millier de monnaies virtuelles, mais ce chiffre est à relativiser, car beaucoup demeurent on ne peut plus confidentielles. Le bitcoin est de très loin la plus connue de toutes, avec une part de marché évaluée à plus de 90 % fin 2015. Sa capitalisation est également la plus élevée (plus de 9 milliards de dollars au début du mois de juin 2016).

2 Ainsi, l'un des tout premiers sites à avoir accepté le bitcoin comme moyen de paiement, Silk Road, permettait à ses utilisateurs d'acheter ou de vendre des armes, des stupéfiants et d'autres produits et services illicites, ce qui lui avait valu d'être surnommé « l'eBay de la drogue » avant sa fermeture par le FBI.

PEPS « Monnaies virtuelles »

entraînés par sa détention (Banque de France [2013]), tandis que d'autres, comme la Thaïlande, la Chine, la Russie ou encore l'Islande, ont purement et simplement décidé de l'interdire. Les différentes affaires ayant émaillé la jeune histoire du bitcoin ne l'ont toutefois pas empêché de voir son cours progresser contre les devises officielles dans des proportions considérables, mais au prix d'une volatilité absolument hors norme, ce qui fait dire à beaucoup que cette monnaie virtuelle ne serait en fin de compte qu'une bulle spéculative d'un nouveau genre.

Si le bitcoin intéresse de plus en plus les économistes, comme en témoigne le nombre croissant d'articles qui lui sont consacrés, c'est cependant surtout parce qu'il remet radicalement en cause leur conception de la monnaie et qu'il propose un modèle cherchant à se passer des banques. L'extrait du discours de Mervyn King en épigraphe, discours prononcé à une époque où les travaux sur les monnaies cryptographiques n'en étaient encore qu'à leurs débuts, revêtirait-il un caractère prophétique ? Sans grande surprise, les économistes se montrent assez dubitatifs à propos du bitcoin, quand ils n'émettent pas un avis carrément négatif. Ainsi, l'ancien gouverneur de la Réserve fédérale américaine, Ben Bernanke, a estimé en novembre dernier qu'il a « *de sérieux problèmes* » en raison de son cours hautement volatil, après avoir pourtant écrit dans une lettre adressée à un comité du Sénat en septembre 2013 qu'il pourrait « *présenter des promesses de long terme* » et « *promouvoir un système de paiement plus rapide, sûr et efficace* », même s'il existe des risques « *liés à l'application de la loi et aux questions de supervision* ». Paul Krugman, de son côté, se montre beaucoup plus radical dans son jugement et le compare volontiers au diable, tandis que Nouriel Roubini n'y voit qu'un jeu de Ponzi et une base pour des activités illégales.

Pour paradoxal que cela puisse paraître, si la technologie derrière le bitcoin est réellement novatrice, son soubassement intellectuel sur le plan économique réside dans des thèses monétaires plutôt anciennes, plus précisément dans les idées développées au sein de l'école autrichienne par Ludwig von Mises et Friedrich August Hayek³. Le fait que la dernière crise financière semble avoir fourni des arguments en faveur de leur théorie des cycles économiques, qui met en avant le rôle de la politique monétaire, n'y est peut-être pas étranger. Le rapprochement avec ce courant de pensée s'explique aussi par le caractère totalement privé des monnaies virtuelles, qui évoque fatalement la célèbre proposition de Hayek [1976] pour obtenir la stabilité monétaire après l'éclatement du système de Bretton Woods, à savoir l'abolition du monopole d'émission de billets des banques centrales et le passage à la concurrence entre des monnaies privées. Si elle fut accueillie avec incrédulité à l'époque, cette proposition retrouve une certaine acuité à l'ère actuelle du numérique. Faudrait-il alors voir dans le bitcoin une possible solution aux désordres monétaires et financiers ?

Ce papier présente une réflexion sur la nature même de cet objet purement numérique. Possède-t-il toutes les qualités attendues d'une monnaie, ou s'agit-il plutôt d'une nouvelle forme d'actif financier obéissant à une logique spéculative ? Tenter de répondre à cette question demande de préciser au préalable comment fonctionne le bitcoin et de souligner les points de rupture par rapport à notre conception courante du système bancaire. Se pose ensuite le problème du choix de la grille de lecture économique. L'approche fonctionnelle traditionnellement retenue pour définir la monnaie nous permettra dans un premier temps de faire ressortir certaines limites du bitcoin, notamment à cause de sa très grande volatilité. L'influence des thèses de l'école de Vienne qui transparaît dans sa conception nous conduira ensuite à l'analyser sous l'angle du théorème de régression de Mises et sous celui du projet hayékien de dénationalisation de la monnaie. Le paradigme hétérodoxe dans lequel on peut inclure l'approche institutionnaliste et la théorie post-keynésienne sera enfin mobilisé pour traiter cette question, ce qui nous amènera à conclure que le

3 L'influence de ce courant de pensée est d'ailleurs mentionnée dans une étude de la Banque centrale européenne (BCE [2012]).

PEPS « Monnaies virtuelles »

bitcoin ne saurait être appréhendé en l'état comme une monnaie à part entière, car il est détaché de la notion de bien public et n'est pas au service de l'économie réelle.

1. Bitcoin, une révolution conceptuelle et technologique

Le recours aux grilles de lecture fournies par la science économique pour étudier le bitcoin, et plus particulièrement la possibilité que celui-ci constitue à terme une monnaie qui remplirait les mêmes fonctions que les devises nationales, et qui entrerait du coup en concurrence directe avec elles, demande au préalable de voir ses spécificités quant à son mode de création et la façon dont il circule⁴.

Il convient en préambule d'apporter quelques clarifications sur le choix des termes. Parler simplement de monnaie « électronique » ou « digitale » pour désigner le bitcoin et ses variantes, et les distinguer des monnaies traditionnelles comme le dollar ou l'euro, est insuffisant et ne nous renseigne guère, étant donné que ces dernières existent également sous cette forme, qui est la version moderne de la monnaie scripturale, forme devenue dominante avec l'informatisation des opérations de paiement puis la généralisation de l'usage des appareils connectés⁵. Le bitcoin n'est, de ce point de vue, que la dernière étape du processus de dématérialisation de la monnaie. S'il s'agit de faire ressortir les différences entre les monnaies, l'expression de « monnaie virtuelle » serait peut-être déjà un peu plus appropriée, vu que le bitcoin n'a aucun support physique et n'existe que sous la forme digitale⁶, à la différence des devises nationales qui ont conservé leurs formes fiduciaire (billets) et métallique (pièces). Cependant, compte tenu de la technologie utilisée, le vocable « cryptomonnaie » semble finalement le moins sujet à confusion, puisqu'il renvoie à la cryptographie asymétrique, qui est le procédé de codage des transactions dont se sert le système pour garantir leur sécurité⁷.

Le principal changement du point de vue économique ne réside pas tant dans le caractère intégralement virtuel des unités monétaires que dans l'algorithme cryptographique employé pour les créer et assurer ensuite leur circulation entre les agents. Cet algorithme introduit en effet une double rupture, au niveau du fonctionnement du système de paiement d'une part, qui devient totalement décentralisé en reprenant le principe des réseaux pair-à-pair (*peer-to-peer*, ou P2P), et au niveau de la conception même de la monnaie d'autre part, puisque celle-ci cesse d'être une créance pour s'apparenter à une valeur boursière. Il s'ensuit que la banque centrale et les établissements de second rang n'auraient plus aucun rôle à jouer.

Sur le plan purement technique, Bitcoin est d'abord un réseau, au même titre qu'Internet, utilisant un langage informatique ouvert et libre de droits. Ce réseau, qui constitue un système monétaire complet, n'exige aucune entité centrale pour l'exécution de certaines fonctions ; les participants à ce réseau assurent eux-mêmes toutes les fonctions et aucun d'entre eux ne dispose d'un avantage particulier sur les autres. Il suffit pour y entrer de télécharger un logiciel libre qui va permettre à la fois de se créer un compte, de réaliser des achats et de vérifier la validité des

4 L'orthographe du terme et l'emploi de l'article permettent de distinguer l'unité monétaire (le bitcoin, noté BTC) du système définissant les modalités de son émission et de son utilisation pour effectuer des transactions (Bitcoin).

5 À titre d'exemple, la masse monétaire en France est aujourd'hui à plus de 90 % sous une forme scripturale.

6 Étymologiquement, le terme est la combinaison de bit (en informatique, l'unité de mesure de base de l'information) et de *coin* (pièce en anglais). Certains sites comme Alitin Mint ou Titan Bitcoin proposent bien à la vente des pièces métalliques en édition limitée incorporant une certaine valeur en bitcoin, mais ce support, qui s'adresse en priorité aux collectionneurs et aux numismates, ne représente qu'une partie infime de la valeur totale des bitcoins en circulation à l'heure actuelle.

7 Un autre terme également rencontré dans la littérature est « cybermonnaie ». On emploiera indifféremment les deux ici.

PEPS « Monnaies virtuelles »

transactions effectuées par l'ensemble des participants. À la différence du système bancaire traditionnel, il n'y a plus de tiers de confiance, ou plutôt c'est le réseau lui-même qui tient désormais ce rôle, grâce à la *blockchain* (littéralement, la « chaîne de blocs »). En fait, c'est cette chaîne qui est véritablement l'innovation majeure ici, le système Bitcoin n'étant que l'une de ses possibles applications. On peut se représenter cette chaîne comme l'équivalent d'un grand-livre comptable (*ledger*) dans lequel toutes les transactions sont traitées, validées et enregistrées. Chaque bloc correspond en quelque sorte à une page de ce grand-livre : dès qu'un bloc de transactions est validé par les utilisateurs du réseau, il est automatiquement ajouté à la chaîne, d'où son appellation.

La cryptographie à double clé garantit en principe la sécurité des transactions⁸. Une fois les bitcoins achetés sur une plate-forme d'échange et placés dans le porte-monnaie (*wallet*) installé sur l'ordinateur, les transactions peuvent être effectuées à l'aide de deux clés⁹, qui sont les « adresses » de l'acheteur et du vendeur : l'adresse de l'acheteur, générée par son porte-monnaie, est la clé privée, l'équivalent d'un mot de passe qui permet de s'authentifier et de dépenser ses bitcoins, et l'adresse du vendeur la clé publique, qui correspond *grosso modo* à un numéro de compte bancaire. Le transfert de bitcoins d'un compte à un autre ressemble ainsi un peu à un échange de courriels. Toutes les transactions sont vérifiées par les nœuds du réseau (c'est-à-dire les ordinateurs connectés) et enregistrées de façon irréversible dans la *blockchain*. N'importe qui peut consulter librement et sans aucune restriction ce registre pour voir l'historique de toutes les transactions. Bitcoin substitue ainsi une vérification consensuelle fondée sur la communauté des utilisateurs au système classique du tiers de confiance. Pour autant, les identités réelles ne sont pas directement visibles dans la mesure où les transactions se font d'adresse à adresse et non de personne à personne. En ce sens, on peut aussi parler d'un quasi-anonymat de Bitcoin¹⁰.

Ce mode de fonctionnement introduit un bouleversement radical par rapport au système bancaire ordinaire, qui exige de déclarer son identité pour ouvrir un compte, mais qui ne porte pas à la connaissance des autres les opérations exécutées à partir de ce compte. Ce renversement fait dire aux plus enthousiastes que la *blockchain* est une technologie potentiellement révolutionnaire, car elle laisse entrevoir un changement de paradigme organisationnel en rendant possible une gouvernance totalement décentralisée et donc la fin des structures hiérarchiques. En permettant de transférer de la valeur de façon sécurisée sans nécessiter le recours à un tiers de confiance, ce sont les banques dans leurs fonctions d'intermédiaires et de garantes du bon déroulement des opérations qui se trouvent remises en question.

Mais le bouleversement ne s'arrête pas là. La seconde rupture amenée par la *blockchain* concerne le processus de production des unités monétaires. En effet, alors que la création monétaire traditionnelle est laissée à la discrétion des banques, l'émission de nouveaux bitcoins est réalisée par des acteurs privés mettant leur équipement informatique à la disposition du réseau pour confirmer les transactions en attente de validation. Leur travail de vérification de la chaîne de blocs s'appelle le « minage » (*Bitcoin mining*), d'où leur surnom de « mineurs ». Ces transactions doivent

8 Il est vrai que la réputation de la cyberdevise en matière de sécurité, malgré les techniques cryptographiques complexes qui sont employées, a été entachée par la faillite en 2014 de la première plate-forme mondiale d'échange, MtGox, après sa déclaration d'une perte de près de 500 millions de dollars consécutive à un piratage externe. L'enquête s'est toutefois orientée par la suite vers la thèse d'une fraude interne mise sur pied par le patron de la société, Mark Karpelès. Ce dernier a depuis été mis en examen au Japon pour détournement de fonds et falsification d'informations.

9 Ces clés sont des successions de chiffres et de lettres. Techniquement, il s'agit de chaînes de 256 bits, codées sous forme de 64 caractères hexadécimaux (0-9, a-f).

10 L'anonymat absolu est toujours difficile à garantir. Il est par exemple théoriquement possible de relier l'adresse envoyant des bitcoins à une identité réelle par l'intermédiaire de l'adresse IP de l'ordinateur.

PEPS « Monnaies virtuelles »

être incluses dans un bloc respectant des règles cryptographiques très strictes¹¹. De nouveaux bitcoins sont alors générés par un algorithme pour récompenser la contribution des mineurs au fonctionnement du système. La rémunération des mineurs, outre le fait qu'elle est destinée à assurer la pérennité de Bitcoin en maintenant l'incitation à poursuivre le travail de validation des blocs, est le seul et unique moyen de créer de nouveaux bitcoins¹². Il s'agit donc d'une création monétaire *ex nihilo*, au même titre que celle des banques quand elles accordent des prêts. Il existe toutefois une différence fondamentale quant à la nature de la monnaie. En effet, si celle-ci est une créance dans le système bancaire traditionnel, il n'en va plus de même avec les bitcoins nouvellement émis. Ces bitcoins s'apparenteraient plutôt à des actions — d'un genre certes très particulier, vu que leur émetteur est un réseau informatique —, dans la mesure où leur valeur va normalement dépendre de la perception par les utilisateurs de la valeur de ce réseau en tant que système de paiement, de la même façon que la valeur intrinsèque d'une action ordinaire doit refléter la valeur de la société qui l'a émise. Ce passage de « l'argent-dette » à « l'argent-valeur » (Fontan [2014]) correspond à une transformation profonde de la nature de la monnaie.

Les mineurs se trouvent en fait en concurrence entre eux pour valider les blocs et acquérir les nouveaux bitcoins, car leur rémunération est proportionnelle à la puissance de calcul qu'ils apportent dans le réseau. Le traitement cryptographique permettant la validation des blocs est fondé sur le principe de la preuve de travail (*proof of work*), qui demande de résoudre un problème mathématique complexe nécessitant des milliards de calculs par seconde. Comme le système a été calibré pour que le temps moyen de minage d'un bloc soit d'une dizaine de minutes, le réseau s'adapte en permanence à la puissance de calcul disponible. La difficulté de ce problème est ainsi automatiquement ajustée à la hausse lorsque le nombre de mineurs détecté par le réseau augmente¹³. Si un mineur isolé pouvait gagner de nouvelles unités dans les premiers temps de l'aventure, le nombre beaucoup plus élevé de participants fait que cela n'est désormais plus du tout possible, d'où la constitution de coopératives de mineurs (*mining pools*) qui répartissent les gains entre leurs membres quand l'un d'entre eux parvient à valider un bloc¹⁴.

Il importe de noter que le principe du minage présente des analogies avec l'extraction d'or¹⁵. L'algorithme créant les nouvelles unités imite en effet, à travers les mathématiques, l'exploitation d'un gisement qui s'épuise peu à peu. À l'instar de cette exploitation, le rendement est décroissant, puisque l'ajout de blocs supplémentaires dans la chaîne devient de plus en plus coûteux pour les mineurs avec l'accroissement de la concurrence et de la puissance de calcul requise. Comme pour

11 Bitcoin recueille toutes les transactions faites dans un laps de temps donné dans un bloc. Le minage consiste à intégrer ce bloc à la chaîne et à vérifier que celle-ci n'a pas été altérée. Pour ce faire, quand un bloc est créé, les mineurs le traitent en prenant l'information qui y est contenue et le transforment en une séquence de chiffres et de lettres que l'on appelle un *hash*. Ce *hash* est ensuite stocké avec le bloc à la fin de la *blockchain*. Chaque *hash* est calculé à partir de celui associé au bloc précédent de façon à empêcher que les blocs ne soient trafiqués.

12 Il s'ensuit que les gains du seigneurage (la différence entre la valeur de la monnaie créée et le coût de cette création) sont perçus dans ce système par des acteurs privés, alors qu'il s'agissait historiquement d'un droit du souverain. Le bitcoin se différencie également des monnaies locales complémentaires qui ne sont pas créées *ex nihilo*, mais qui sont gagées par des dépôts équivalents à la valeur mise en circulation.

13 La difficulté de minage mesure à quel point il est difficile de générer un bloc comparativement au premier bloc créé en 2009 par Satoshi Nakamoto. À titre d'illustration, pour une difficulté de minage initialement fixée à 0, la difficulté au début du mois de juin 2016 était évaluée à près de 200 milliards (l'évolution de cette difficulté est observable sur la page <http://bitcoindifficulty.com>). Aujourd'hui, la seule méthode de minage potentiellement rentable requiert de nouvelles machines spécialement conçues pour cette activité.

14 La difficulté croissante du minage a également conduit à l'apparition de sociétés de *cloud mining* qui vendent de la puissance de calcul à leurs clients.

15 On parle d'ailleurs souvent de « l'or numérique » pour qualifier le bitcoin. La terminologie qui lui est associée est assez révélatrice, le choix du mot « minage » pour désigner la production des nouvelles unités n'étant pas le fruit du hasard.

PEPS « Monnaies virtuelles »

l'or, la production se voit imposer une limite, car le système est conçu pour que la quantité de bitcoins nouvellement émis soit divisée de moitié tous les 4 ans et que le stock ne dépasse jamais les 21 millions d'unités. Ainsi, l'activité de minage, initialement rétribuée 50 BTC, puis 25 BTC en 2012, ne sera plus payée que 12,5 BTC à partir de juillet 2016, puis 6,25 BTC en 2020, et ainsi de suite. Le nombre total de bitcoins en circulation, qui se rapproche actuellement des 16 millions, devrait normalement dépasser les 20 millions en 2025 et atteindre son maximum de 21 millions en 2140.

Au total, la technologie de la *blockchain* présente clairement un potentiel disruptif en matière de gouvernance et fait du bitcoin quelque chose d'à part. Du point de vue de l'analyse économique, la proximité avec l'or, le mode de création qui rompt le lien avec la puissance publique, la mise en avant récurrente des valeurs libertariennes, mais aussi la critique du système bancaire dans le contexte actuel et la volonté de proposer une monnaie saine, qui ne pourrait faire l'objet d'aucune manipulation de la part des autorités, sont autant d'éléments qui évoquent les thèses de l'école autrichienne. En particulier, cet instrument virtuel et ses nombreuses variantes pourraient désormais offrir la possibilité d'une mise à l'épreuve de la proposition d'un régime de libre concurrence monétaire formulée par Hayek [1976]. Si l'idée d'instaurer un tel régime n'a guère rencontré de succès à l'époque, son auteur lui-même la jugeant utopique, le développement de l'informatique conduit 40 ans plus tard à la reconsidérer sous un jour nouveau et à lui redonner une place dans les débats actuels.

2. Une première interprétation du statut du bitcoin à partir des trois fonctions de la monnaie

La question la plus fréquemment posée au sujet du bitcoin a trait à la détermination exacte de sa nature : s'agit-il d'une véritable monnaie, comparable au dollar ou à l'euro ? Pour ses utilisateurs, une telle question n'a même pas lieu d'être puisque le bitcoin permet d'acheter des biens et des services ; pour les économistes, il convient de se montrer beaucoup plus nuancé, car un moyen de paiement ne suffit pas à définir une monnaie.

Cette question peut d'abord recevoir une réponse d'ordre juridique. Le bitcoin ne saurait être considéré comme une monnaie comparable à une devise nationale pour la simple raison qu'il n'a pas cours légal, c'est-à-dire qu'un commerçant en France peut parfaitement refuser d'être payé avec des bitcoins si tel est son désir, alors qu'il est obligé d'accepter des euros pour ne pas contrevenir aux dispositions de l'article R642-3 du Code pénal. Si le bitcoin est une monnaie, il ne peut donc l'être que « du fait des usages », à la différence des monnaies « du fait de la loi ». Son pouvoir libératoire dans les transactions étant limité, il ne peut s'agir au mieux que d'une monnaie complémentaire. L'État ne considère d'ailleurs pas le bitcoin comme une monnaie concurrente de l'euro vu que l'article R642-2 du Code pénal interdit « *le fait d'accepter, de détenir ou d'utiliser tout signe monétaire non autorisé ayant pour objet de remplacer les pièces de monnaie ou les billets de banque ayant cours légal en France.* » Le bitcoin ne satisfait pas non plus la définition de la monnaie électronique donnée par l'article L315-1 du Code monétaire et financier puisqu'il n'est pas créé à l'occasion de l'octroi d'un crédit et ne constitue pas une créance sur son émetteur, ainsi qu'on l'a vu dans la section précédente. Cette première réponse a le mérite de la clarté, mais ne dit cependant rien sur les caractéristiques intrinsèques du bitcoin et sur son potentiel en tant qu'actif monétaire.

PEPS « Monnaies virtuelles »

Pour tenter de le percevoir, il faut se tourner vers la science économique. Il est de tradition dans les manuels de présenter la monnaie à partir des trois fonctions qu'elle exerce — et qui furent identifiées dès l'Antiquité par Aristote — de façon à souligner la rupture avec le troc :

- exprimer la valeur de tous les biens et services dans une unité de mesure commune pour simplifier le système des prix (fonction d'unité de compte) ;
- constituer la contrepartie de n'importe quelle marchandise pour résoudre le problème de la double coïncidence des besoins (fonction d'intermédiaire des échanges) ;
- représenter un pouvoir d'achat pour permettre à son détenteur d'étaler dans le temps les transactions sur biens et services (fonction de réserve de valeur).

La monnaie doit par ailleurs avoir des caractéristiques physiques qui facilitent la réalisation de ces fonctions. Elle doit être inaltérable, fongible, parfaitement divisible, facile à stocker et à transporter. Idéalement, elle devrait aussi être impossible à contrefaire. Les cryptodevises, par nature intangibles, respectent à première vue toutes ces contraintes¹⁶. Leur nature particulière est de plus souvent présentée comme un avantage pour leur adoption par rapport aux instruments d'échange matériels. Ce point semble toutefois discutable. Gertchev [2013] fait notamment remarquer que le degré d'universalité des monnaies virtuelles se trouve précisément affaibli par leur intangibilité dans le sens où leur diffusion présuppose l'acceptation par tous de la même technologie. Or, le développement de la technologie au sein d'une société n'est jamais uniforme, ne serait-ce simplement que parce que les revenus et les préférences individuelles diffèrent, de sorte que ce sont les monnaies avec un support physique qui conservent le plus haut degré d'universalité de son point de vue.

Si l'on met de côté cette opposition entre monnaie matérielle et monnaie virtuelle, le bitcoin est bien, aux yeux de ses promoteurs, l'équivalent numérique de l'argent liquide puisqu'il remplit les trois fonctions mentionnées plus haut : on trouve en effet sur Internet des sites où les prix sont exprimés en bitcoin et qui acceptent le bitcoin comme moyen de paiement, et il existe pour stocker ses clés privées en vue d'achats futurs une grande variété de *wallets* avec des fonctionnalités plus ou moins étendues. Cette simple constatation est cependant loin de suffire. Le bitcoin échappe forcément à la définition traditionnelle de la monnaie quand on considère son statut d'équivalent général qui lui permet d'acheter n'importe quelle marchandise à l'intérieur d'un territoire donné. Un actif qui permet d'acquérir une partie seulement des marchandises disponibles dans une économie, comme c'est encore le cas du bitcoin, n'est qu'un moyen de paiement et pas de la monnaie au sens strict du terme¹⁷. Le bitcoin ne possède pas la liquidité absolue qui est la marque même de la monnaie.

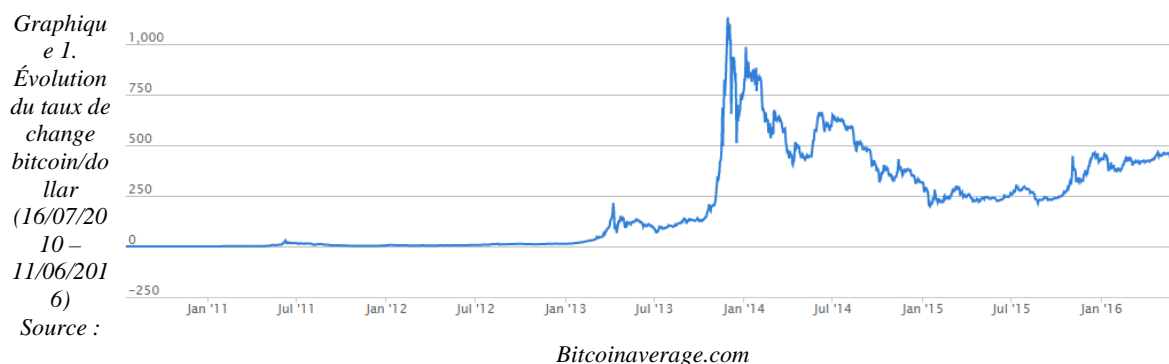
Cela ne signifie pas *a priori* qu'il en sera toujours ainsi ; la technologie et les comportements évoluent, et il n'est pas interdit d'envisager que toutes les marchandises pourraient être payées dans un futur plus ou moins éloigné avec un moyen de ce genre. L'impossibilité à l'heure actuelle de considérer le bitcoin comme une monnaie au sens strict ne résulte cependant pas seulement de ce qu'il n'est pas un équivalent général. Il présente d'autres particularités qui l'empêchent de remplir correctement les trois fonctions que l'on attend d'une monnaie. Ces

16 La question de la fongibilité du bitcoin fait toutefois débat, en particulier aux États-Unis depuis la décision prise par l'administration fiscale en mars 2014 de ne pas le considérer comme une monnaie, mais comme un actif financier et de taxer les plus-values réalisées sur les transactions qui devront donc être déclarées. Compte tenu de la très forte variabilité du cours du bitcoin depuis son lancement, chaque unité peut être différenciée fiscalement. La personne ayant par exemple payé son premier bitcoin 5 \$ le 30 avril 2012 puis son second bitcoin 761 \$ le 22 novembre 2013 aurait aujourd'hui tout intérêt à utiliser ce dernier dans une transaction. Comme ces deux unités bitcoin ne sont plus équivalentes, à la différence de deux billets de 100 \$, il n'est plus possible de parler de monnaie.

17 Il en est exactement de même des tickets restaurant ou des bons d'achat qui ne donnent accès qu'à un registre limité de biens et de services.

PEPS « Monnaies virtuelles »

fonctions étant liées, les difficultés rencontrées au niveau de l'une d'entre elles ne peuvent que compliquer la réalisation des deux autres. En particulier, si un actif n'est pas perçu par les agents comme une réserve de valeur suffisamment sûre, ceux-ci seront logiquement peu enclins à l'accepter comme moyen de paiement, ce qui limitera sa circulation dans l'économie, et donc du coup les raisons de s'en servir comme unité de compte.



L'une des principales caractéristiques du bitcoin est la volatilité extrêmement grande de son prix. Le graphique 1 retrace l'évolution de son cours vis-à-vis du dollar entre juillet 2010 et juin 2016. Après une phase de hausse significative pendant le premier semestre 2013, consécutive à la crise chypriote marquée par la fermeture des banques et la crainte d'une taxation des dépôts, le cours s'est littéralement envolé durant la seconde moitié de l'année, en raison notamment de l'intérêt massif porté par les Chinois, pour dépasser la barre des 1000 \$. Il a ensuite perdu en 2014, après la décision des autorités chinoises de mettre fin aux opérations en bitcoin et la faillite de MtGox, plus de la moitié de sa valeur pour enfin se stabiliser l'an dernier et connaît depuis une nouvelle phase de croissance qui le porte au début de ce mois de juin 2016 aux environs de 590 \$, soit une progression en un an de près de 157 % ! Du point de vue financier, le bitcoin est inclassable et n'apparaît corrélé à aucune catégorie d'actifs. Sa volatilité a été de 142 % pour la seule année 2013 (Yermack [2013]), ce qui est sans commune mesure avec les ordres de grandeur habituels pour les taux de change des devises officielles (aux alentours de 10 %) ou pour la plupart des actions cotées (entre 20 et 30 %). Entre mai 2012 et mai 2014, les volatilités mensuelle et quotidienne du bitcoin ont été respectivement de 265 % et 200 %, et la parité bitcoin/dollar a été 40 fois plus volatile que la parité euro/dollar.

Le cours du bitcoin est tellement variable sur des périodes courtes qu'il lui est impossible de jouer le rôle de réserve de valeur. Les agents économiques ne peuvent pas être incités à conserver des bitcoins et à les utiliser pour leurs transactions s'ils n'ont aucune idée précise de ce qu'ils pourront acheter dans un avenir proche avec ce qu'ils possèdent aujourd'hui. En réalité, la détention de bitcoins obéit fondamentalement à une logique spéculative, ce qui fait de lui un actif financier et non un actif monétaire¹⁸. Même si certains sites, à l'instar de Magnr, offrent depuis peu la rémunération d'un taux d'intérêt contre la mise en dépôt de bitcoins, la plupart des individus qui achètent aujourd'hui des bitcoins sur les plates-formes de change le font avant tout parce qu'ils

18 Certains sites le reconnaissent d'ailleurs très ouvertement. On peut par exemple lire sur la page du site français Bitcoin qui explique le rôle des places de marché (<https://bitcoin.fr/obtenir-des-bitcoins/#plateformes>) : « Quelle que soit la place de change choisie, rappelez-vous que le bitcoin est très volatil, que c'est un placement spéculatif et qu'il ne faut y investir que ce qu'on peut se permettre de perdre. » La même page précise plus bas : « Vendre des biens contre des bitcoins n'est pas une chose facile, rares sont les acheteurs qui possèdent des bitcoins et sont disposés à les dépenser. Les sites spécialisés dans ce genre de transaction sont donc rares. »

PEPS « Monnaies virtuelles »

parient sur la hausse du cours sur la longue période¹⁹. C'est typiquement le comportement observé dans le cas d'une bulle spéculative. Ceci n'est guère surprenant compte tenu des caractéristiques très particulières du bitcoin : n'étant adossée à rien, et en l'absence de consensus sur ce qui pourrait constituer sa valeur fondamentale, si tant est qu'il soit possible de parvenir à un consensus dans ce cas, sa valeur actuelle ne peut être que très dépendante des anticipations sur sa valeur future.

Mais la spéculation ne découle pas uniquement de la pure virtualité de cet instrument quand on se rappelle que l'algorithme utilisé par les mineurs est fondé sur une règle de création des nouvelles unités à un rythme décroissant et que le programme a fixé une limite absolue de 21 millions de bitcoins dans le monde. En d'autres termes, sa rareté étant garantie par les mathématiques, le bitcoin a été créé dès le départ pour être un actif spéculatif. Si la demande globale de bitcoins progresse encore, son cours ne pourra que monter à cause de l'inélasticité de l'offre, ce qui soutiendra mécaniquement la demande, d'autant que l'absence de toute référence au réel favorise le mimétisme, et la dynamique haussière s'en trouvera renforcée. À l'inverse des monnaies traditionnelles, qui sont inflationnistes du fait de l'action des banques centrales qui ont le pouvoir d'en créer à volonté, le bitcoin est une monnaie déflationniste²⁰.

Le problème du point de vue des fonctions de la monnaie est que le caractère spéculatif du bitcoin ne peut que limiter son rôle d'intermédiaire des échanges. En effet, les possesseurs de bitcoins devraient logiquement être de moins en moins incités à les dépenser s'ils voient leur portefeuille prendre de plus en plus de valeur ; dans ce cas, les achats de la vie quotidienne pouvant toujours être effectués avec les monnaies nationales, la circulation de bitcoins entre les individus ralentira, et il deviendra de plus en plus difficile d'en trouver en contrepartie de la vente d'un bien ou d'un service. La fameuse loi de Gresham, selon laquelle la mauvaise monnaie chasse la bonne, trouve avec Bitcoin une nouvelle illustration : lorsqu'un agent économique a le choix entre deux monnaies, il conserve celle qui a le plus de valeur et utilise l'autre pour ses transactions courantes. C'est sans doute là le grand paradoxe du bitcoin : alors qu'il est présenté comme une monnaie à part entière par ses promoteurs et la communauté de ses utilisateurs, sa forte médiatisation risque fort dans les années qui viennent de compliquer la réalisation des fonctions qu'il est censé exercer ; si une monnaie inflationniste peut se trouver remise en cause parce qu'elle achète de moins en moins de choses du fait de son abondance, une monnaie déflationniste ne se montrera guère plus utile aux agents si elle est thésaurisée et retirée du circuit économique.

Le succès d'une monnaie dépend certes de ce qu'elle permet d'acheter, mais aussi du nombre de personnes qui s'en servent dans leurs transactions quotidiennes. Sur ce point, les données disponibles pour essayer de se faire une idée plus précise de l'importance du bitcoin en tant que moyen d'échange doivent être prises avec prudence, dans la mesure où tous les possesseurs d'un portefeuille n'utilisent pas forcément les bitcoins qui y sont déposés pour leurs achats courants, outre le fait que le nombre de ces portefeuilles n'est pas un indicateur vraiment fiable du nombre réel d'utilisateurs, puisqu'il est possible pour un même individu d'en avoir autant qu'il le souhaite. Les réponses à un sondage effectué sur Internet en février 2014 par l'agence d'études Waykup montrent d'ailleurs que la première motivation de la détention de la devise virtuelle serait l'investissement et la spéculation²¹, bien loin devant l'anonymat des transactions, ce qui va dans le sens des conclusions de Ron et Shamir [2013] qui estiment le taux de thésaurisation à près de 80 %. L'importance de cette cryptodevise en tant que moyen de paiement est donc encore aujourd'hui des

19 Aït-Kacimi [2014] estime ainsi que 70 % des achats de bitcoins seraient effectués à des fins spéculatives.

20 Comme le font remarquer Lakowski-Laguerre et Desmedt [2015], la volonté de créer une monnaie enfin débarrassée du problème traditionnel qu'est l'érosion de son pouvoir d'achat et la défiance à l'égard du système bancaire actuel transparaissent clairement dans Satoshi Nakamoto [2009].

21 Dans le même ordre d'idées, l'un des fondateurs du site de gestion de portefeuille Coinbase évaluait à la même époque l'activité en rapport avec la spéculation à 80 % environ (Yermack [2013]).

PEPS « Monnaies virtuelles »

plus modestes, malgré la forte progression du nombre de commerces en ligne qui l'acceptent²², et le volume des transactions en bitcoin reste insignifiant quand on le compare aux volumes des transactions libellées en dollar et en euro²³. Même si le nombre de ses utilisateurs actifs devrait continuer d'augmenter dans les années qui viennent²⁴, Bitcoin est encore très loin de la taille critique à partir de laquelle les externalités de réseau pourraient accélérer significativement le rythme de son adoption par les autres agents économiques pour en faire un véritable instrument d'échange, parce que le coût d'utilisation de la cryptodevise (sur le plan de l'acquisition de la technologie, notamment) serait devenu inférieur au coût de transaction associé à l'emploi d'une autre monnaie. S'il y a un effet d'entraînement aujourd'hui, celui-ci s'explique davantage par la montée rapide de son cours, et donc l'espoir d'une plus-value future, que par la hausse du nombre de transactions sur biens et services.

Le bitcoin, enfin, se heurte à plusieurs obstacles pour devenir une véritable unité de compte. Il est vrai que l'on peut trouver sur des sites de vente en ligne les prix des produits exprimés en bitcoin, mais ces prix sont également donnés en monnaie nationale. Le risque de change particulièrement important implique une actualisation beaucoup plus fréquente des prix en bitcoin par rapport aux prix en dollar ou en euro²⁵, d'où des coûts de réétiquetage (*menu costs*) plus élevés pour la cryptodevise, mais aussi un coût psychologique pour le consommateur face à ces rapides fluctuations de valeur qui n'existe pas en temps normal avec les monnaies traditionnelles. Cette volatilité fait que le bitcoin ne se prête pas naturellement au rôle d'étalon des valeurs²⁶. En particulier, l'acceptation de voir son salaire libellé en bitcoin ne va pas de soi puisqu'elle entre en conflit avec l'exigence de prévisibilité de la rémunération²⁷. Il s'ensuit dans ces conditions que le bitcoin ne peut être au mieux qu'une monnaie complémentaire avec une fonction d'unité de compte restreinte. Les agents économiques, tant qu'ils percevront leur salaire dans la monnaie nationale officielle, raisonneront d'abord sur la base de cette monnaie pour prendre leurs décisions de consommation et d'investissement.

Au-delà de la question de la volatilité, il existe, dans une perspective de long terme, un autre argument lié au salaire qui amène à douter de la capacité du bitcoin à pouvoir jouer ce rôle. Si le bitcoin devenait l'unité de compte de tous les biens et services disponibles dans l'économie, les salaires seraient eux aussi exprimés dans cette unité. La croissance impliquant à terme une chute

22 D'après le service de paiement BitPay, ce nombre aurait dépassé les 100 000 l'an dernier.

23 Le nombre moyen de transactions quotidiennes (disponible à la page <https://blockchain.info/fr/charts>) tourne actuellement autour de 200 000. Ce nombre est encore plus faible si l'on exclut les chaînes longues qui peuvent résulter des tentatives de blanchiment. McCallum [2015] indique un volume de transactions par minute fin 2013 qui ne représentait même pas les quatre millièmes des transactions en dollar en comptant uniquement celles effectuées avec une carte Visa. Le nombre de transactions avec cette cryptomonnaie apparaît également dérisoire au regard des quelque 274 millions de paiements quotidiens par carte bancaire dans l'Union européenne (Dupré *et al.* [2015]).

24 Une étude prospective récente estime que ce nombre, qui était évalué à 1,3 million en 2014, devrait passer à 4,7 millions à la fin de cette décennie (Holden [2015]).

25 À titre d'illustration, Lo et Wang [2014] mentionnent une révision des prix en bitcoin toutes les 10 minutes sur le site Overstock et une actualisation toutes les 15 minutes sur TigerDirect.

26 Yermack [2013] suggère qu'une autre raison pour douter de la capacité du bitcoin à être un bon étalon des valeurs réside tout simplement dans le fait que l'expression des prix dans cette unité n'est pas standard. Le bitcoin étant divisible jusqu'à la huitième décimale (le satoshi correspondant à la plus petite unité possible), certains produits sont vendus à des prix qui peuvent paraître déroutants de prime abord. Ainsi, au moment de l'écriture de ces lignes, une livre de fondant au chocolat sur le site BitDazzle valait 19 \$ ou 0,07096 BTC. Un changement d'unité peut certes donner un prix plus lisible, mais l'inconvénient est alors la multiplication des sous-unités qui vient compliquer la comparaison des prix.

27 Il existe pourtant aujourd'hui des expériences pilotes de paiement du salaire en monnaie virtuelle. Bitwage et Paybits permettent par exemple aux entreprises de verser aux salariés qui le souhaitent une partie de leur rémunération en bitcoin.

PEPS « Monnaies virtuelles »

généralisée des prix compte tenu de la quantité fixe de monnaie dans ce système, les salaires devraient donc également diminuer. Est-ce envisageable vu la rigidité fréquemment observée des salaires nominaux à la baisse ? Il s'ensuivrait dans ce cas une hausse du coût réel du travail pour les entreprises. La combinaison d'un accroissement des coûts de production et d'une réduction de la demande agrégée, si les agents pensent que la chute des prix va se poursuivre, est l'un des arguments les plus fréquemment employés à l'encontre du bitcoin à cause de ses conséquences macro-économiques. Ses défenseurs tendent pourtant le plus souvent à l'ignorer purement et simplement en arguant du fait que la déflation n'est pas une mauvaise chose, voire un mythe, reprenant ainsi à leur compte la thèse extrême de Rothbard [1995].

Cette première lecture du potentiel du bitcoin sur la base des fonctions qui sont traditionnellement assignées à la monnaie nous amène finalement à donner une réponse négative. Le bitcoin n'est pas encore un équivalent général de tous les biens et services. Mais son principal problème, dans l'optique de la réalisation de ces fonctions, vient de sa volatilité. En dépit d'un recul par rapport aux années précédentes²⁸, celle-ci demeure trop importante pour lui permettre de constituer une unité de compte fiable et une réserve de valeur suffisamment sûre.

Cette réponse doit cependant être nuancée en rappelant que ces fonctions n'ont pas toujours été historiquement remplies par le même actif²⁹. Leur séparation a notamment été mise en évidence par Polanyi [1968] avec sa distinction classique entre une monnaie « pour tous les usages » (*all-purpose money*) et une monnaie « à usage spécifique » (*special-purpose money*). L'approche polanyienne, qui relève de l'anthropologie économique, s'efforce de rendre compte des transformations institutionnelles ayant progressivement conduit à la concentration des différentes fonctions de la monnaie sur un même support. Les sociétés anciennes, contrairement à l'idée toujours dominante qui présente le troc comme une sorte d'état originel³⁰, associaient à chaque usage des objets distincts. Ces objets étaient des monnaies « monofonctionnelles » et ne servaient donc pas nécessairement à l'échange, certains ayant seulement une fonction d'étalon tandis que d'autres étaient utilisés pour le paiement³¹. Ce n'est qu'avec le développement de l'organisation marchande que sont apparues les monnaies « multifonctionnelles », qui correspondent aux monnaies d'État que nous utilisons aujourd'hui. Pour autant, les monnaies à usage spécifique n'ont pas disparu dans les sociétés modernes : pour Blanc [2006], les monnaies affectées, comme les bons d'achat prépayés, ou les monnaies locales, destinées à n'être utilisées que dans une zone géographique bien délimitée, peuvent être assimilées à ces formes monétaires particulières étant donné que leur validité est restreinte d'une façon ou d'une autre, dans le temps, l'espace ou encore du point de vue des biens et des services auxquels elles donnent accès.

Il semble possible de prolonger ce raisonnement et d'utiliser la grille de lecture polanyienne pour intégrer le bitcoin et ses variantes dans l'ensemble des monnaies à usage spécifique. Être un moyen de paiement alternatif est en effet pour beaucoup d'entre elles leur principale fonction, si ce n'est la seule. Par ailleurs, certaines cryptomonnaies ont un caractère social beaucoup plus affirmé que d'autres parce qu'elles ne sont pas conçues à la base pour acheter des marchandises, mais pour

28 Elle a tout de même été de 65 % en 2015.

29 Un exemple classique est le cas de la France sous l'Ancien Régime : la fonction de moyen de paiement était remplie par des pièces d'or et d'argent, tandis que l'unité de compte était la livre tournois, qui ne correspondait à aucune monnaie en circulation et qui fut remplacée par le franc en 1795.

30 Cette « fable du troc » est l'un des fondements de l'approche hétérodoxe de la monnaie qui sera abordée plus loin dans ce papier.

31 Comme l'explique Servet [1993], Polanyi établit dans son œuvre une distinction entre la fonction de paiement et la fonction d'échange, la première précédant historiquement la seconde. Le paiement correspond primitivement à l'acquittement d'obligations qui ne sont pas de nature économique, mais de l'ordre du cérémoniel, tandis que l'échange renvoie à l'acquisition d'objets destinés à la satisfaction d'un besoin sur un marché qui crée un prix. Ces deux fonctions vont par la suite se confondre avec la généralisation des échanges marchands.

PEPS « Monnaies virtuelles »

effectuer des micropaiements, plus particulièrement sur les réseaux sociaux³². Cette fonction précise peut se voir comme la version moderne du concept de paiement au sens de Polanyi puisqu'elle n'obéit pas à une logique marchande et ne vise pas la satisfaction d'un besoin matériel.

Les formes monétaires ne sont en rien immuables, et l'idée que les nouvelles technologies entraînent à terme la déconcentration des fonctions de la monnaie et la multiplication des supports de paiement a déjà été envisagée avant l'apparition du bitcoin (Cowen et Kroszner [1994]). Le développement très rapide des cryptodevises auquel on assiste depuis plusieurs années et les transformations majeures qu'elles laissent entrevoir accélèrent aujourd'hui clairement cette réflexion. Ce sont également les théories monétaires qui se trouvent interrogées sur leur capacité à intégrer le bitcoin et ses multiples déclinaisons dans leur schéma explicatif. La structuration de la pensée monétaire autour des approches réaliste et institutionnaliste rencontre avec le bitcoin un défi inédit : s'il s'agit effectivement d'une monnaie, peut-on pour autant l'appréhender comme un bien ou une institution ?

3. L'approche réaliste de la monnaie appliquée au cas du bitcoin : le retour de l'école économique autrichienne

Énumérer les trois fonctions habituellement dévolues à la monnaie pour la définir est commode, mais insuffisant pour appréhender toute sa complexité. Les avis des économistes diffèrent radicalement dès qu'il s'agit de les situer les unes par rapport aux autres du point de vue de leur importance respective, à tel point que le débat sur la nature de la monnaie est certainement l'un de ceux où les clivages théoriques apparaissent les plus marqués. Au risque de simplifier quelque peu, l'étude de la monnaie se structure autour de deux conceptions très différentes, pour ne pas dire opposées, qui renvoient en partie à la ligne de séparation schumpétérienne entre l'analyse *réelle* des phénomènes économiques et leur analyse *monétaire*.

L'approche la plus ancienne, qui demeure largement dominante aujourd'hui, conçoit avant tout la monnaie comme l'instrument qui permet de résoudre les problèmes inhérents au troc. Parce que la monnaie est destinée à faciliter les transactions entre les individus, sa fonction essentielle est d'être l'intermédiaire des échanges, ce qui lui confère alors aussi le rôle d'unité de compte. D'après cette conception, qualifiée de « réaliste », ou de « métalliste » dans sa formulation la plus ancienne, la monnaie est à l'origine un bien sélectionné parmi d'autres pour sa forte négociabilité. La vision dite « institutionnaliste » de la monnaie, quant à elle, réfute l'idée que cette dernière ne serait qu'un instrument choisi à l'initiative du secteur privé en raison de son côté pratique et l'associe à l'émergence progressive de la vie sociale et à l'existence d'une représentation du pouvoir ; elle doit se comprendre comme une règle sociale qui se définit d'abord par sa fonction d'unité de compte, son imposition par le pouvoir favorisant sa circulation et la conduisant *de facto* à être le moyen de paiement.

Cette section adopte le point de vue réaliste, en prenant plus précisément appui sur les thèses monétaires développées au sein de l'école autrichienne. Pas simplement parce que l'œuvre de Menger, le fondateur de cette école, constitue la référence classique pour appréhender la monnaie à partir de sa fonction d'intermédiaire des échanges. Plus fondamentalement, le biais intrinsèquement

32 On peut citer parmi elles le dogecoin (la plus ancienne de ce type), le neucoin, le reddcoin ou encore le sendcoin. Ces micropaiements sont souvent désignés sous l'expression de « pourboires sociaux » (*social tipping*).

PEPS « Monnaies virtuelles »

déflationniste de Bitcoin, la volonté manifeste de retrouver les vertus de l'étalon-or, la défiance à l'égard des monnaies de papier qui voient leur pouvoir d'achat s'éroder continuellement, les critiques à l'encontre d'un système bancaire à réserves fractionnaires, qui trouvent une résonance dans le contexte de crise et le surendettement, mais aussi et peut-être surtout le contournement grâce à la *blockchain* de la puissance publique dans le processus de création monétaire sont autant d'éléments qui ne peuvent que faire penser à ce courant.

3.1. Le bitcoin enfreint-il le théorème de régression ?

Si, à l'instar de Tucker, les libertariens les plus enthousiastes voient dans chaque satoshi « *un peu de Menger, Mises, Hayek, Rothbard et Kirzner* »³³, il convient de se montrer plus nuancé quand on songe au caractère déroutant que revêt la cryptodevise aux yeux de bon nombre d'économistes rattachés à l'école autrichienne et aux divergences d'analyse qui existent en son sein. La plus grande difficulté concerne la qualification qu'il convient de donner au bitcoin et donc, dans cette grille de lecture, la manière d'interpréter le théorème de régression de Mises [1912]³⁴, censé expliquer l'origine de toute monnaie.

Dans l'approche réaliste, la fonction centrale de la monnaie est d'être l'instrument des échanges. La monnaie émerge comme la solution aux problèmes du troc à l'issue d'un processus d'apprentissage des acteurs privés pour améliorer leur bien-être personnel grâce à un accès beaucoup plus rapide aux biens désirés, apprentissage au cours duquel les différents objets présentant une valeur d'échange ont été comparés dans leur degré d'acceptabilité dans les transactions et rejetés l'un après l'autre jusqu'à la sélection finale de celui offrant la plus grande capacité d'écoulement (*Absatzfähigkeit*), c'est-à-dire la plus grande liquidité (Menger [1892]). L'objet en question devient alors la monnaie du fait de son adoption à une large échelle et continuera d'être demandé, même s'il perd par la suite toute utilité directe, pour pouvoir acquérir les autres marchandises. La monnaie peut ainsi se définir comme « *le moyen d'échange généralement accepté et communément utilisé* » (Mises [1949]). La critique traditionnellement adressée à cette conception porte sur la circularité du raisonnement, puisque la monnaie a de la valeur en tant que moyen de règlement précisément parce qu'elle sert à régler les transactions. En d'autres termes, si la monnaie est utile parce qu'elle représente une valeur, comment affirmer dans le même temps que sa valeur découle des services qu'elle rend ? Le théorème de régression brise cette circularité et résout du coup le problème de l'indétermination de la valeur de la monnaie : l'acceptation d'un bien comme moyen de règlement à un instant t implique la constatation de son pouvoir d'achat en $t-1$, de même que son acceptation en $t-1$ a été conditionnée par l'observation de son pouvoir d'achat en $t-2$, et ainsi de suite jusqu'au tout premier paiement sous la forme de ce bien, qui n'a pu être effectué que parce que son usage était valorisé par les agents économiques pour ses qualités intrinsèques. En conséquence, d'après ce théorème, toute monnaie tire sa valeur d'une utilisation concrète qui n'est pas originellement liée à l'échange.

C'est précisément là que se situe le problème des cryptodevises aux yeux de certains auteurs (Shostak [2013], LeRoux [2014]). Leur immatérialité s'avère incompatible avec leur idée d'une

33 Voir la page <https://fee.org/articles/the-austrian-influences-on-bitcoin/>. De manière générale, on ne compte plus aujourd'hui les sites Internet consacrés à Bitcoin qui se réfèrent à l'école autrichienne. Leur pensée en la matière est finalement assez bien résumée dans ce titre d'un article d'Allen Scott (<https://news.bitcoin.com/austrian-school-economists-bitcoin/>) : « *Les économistes de l'école autrichienne étaient des bitcoiners, c'est juste qu'ils ne le savaient pas encore.* »

34 Ce théorème prolonge l'analyse de Menger pour expliquer l'apparition d'un moyen de règlement puis sa transformation en monnaie.

PEPS « Monnaies virtuelles »

monnaie ne pouvant se concevoir autrement que comme le résultat d'un long processus de sélection parmi une grande variété de biens échangeables³⁵. Leur lecture du théorème de régression est que le bitcoin ne peut pas devenir une monnaie parce qu'il ne possédait aucune valeur d'usage direct avant son émergence en tant que moyen de paiement. La connaissance du pouvoir d'achat antérieur de la monnaie est essentielle ici. Or, n'ayant aucun prix au départ, parce que nullement demandé, le bitcoin ne peut satisfaire le théorème de régression. Il est au mieux ce que Mises appelait un « *moyen d'échange secondaire* » ou Rothbard une « *quasi-monnaie* ». Ainsi, pour Shostak [2013], « *le bitcoin n'est pas une vraie monnaie, mais seulement une nouvelle manière de fonctionner avec la monnaie qui existe.* » Sa conclusion générale sur les monnaies virtuelles est sans appel : « *La monnaie électronique ne remplacera jamais la monnaie fiduciaire. C'est une illusion liée à l'incompréhension de la nature et de la fonction de la monnaie, et de la manière dont les monnaies émergent.* »

Ce jugement ne fait toutefois pas l'unanimité, et l'argumentation de ce dernier auteur pour réfuter la nature monétaire du bitcoin a été sévèrement critiquée (Krawisz [2013]), notamment la condition de tangibilité impliquant que seule une marchandise physique pouvant être évaluée du point de vue de son utilité intrinsèque serait susceptible de se transformer en monnaie. Pour Graf [2013], le caractère purement numérique des bitcoins importe peu, leur valeur initiale avant le développement de la fonction d'intermédiaire des échanges pouvant être trouvée, suivant le profil de leur détenteur, dans le plaisir d'un jeu informatique pour *geek*, ou à un niveau symbolique dans la satisfaction de manifester un certain mode de pensée et l'appartenance à une communauté revendiquant l'idéologie libertarienne. Dans la même veine, Tucker [2014] défend l'idée que la valeur non monétaire des bitcoins résiderait tout simplement dans la perception des avantages apportés par la *blockchain* elle-même, avec la rapidité et la sécurité des opérations et la faiblesse des coûts de transaction. Le bitcoin serait dans cette optique une monnaie dont la valeur découlerait du système de paiement qui lui est associé. Dans tous les cas, la valeur d'usage direct ayant conduit à l'établissement de la valeur d'échange sur le marché ne peut être que d'ordre purement mental. L'historique du prix du bitcoin montre que celui-ci n'a eu aucune valeur d'échange pendant plusieurs mois après son lancement³⁶ ; pourtant, les premiers mineurs ont forcément dû lui accorder une certaine valeur d'usage puisqu'ils ont utilisé leur équipement informatique afin d'en obtenir. Dire que le bitcoin ne peut pas constituer une monnaie parce qu'il n'a rien d'un objet traditionnel apparaît finalement contradictoire avec le subjectivisme de l'école autrichienne. En effet, pour Hayek [1943], « *dans les sciences sociales les choses sont ce que les gens croient qu'elles sont. La monnaie est la monnaie, un mot est un mot, un produit de beauté est un produit de beauté, si et parce que quelqu'un pense qu'ils le sont.* » Il paraît donc impossible, si l'on adhère à cette conception, d'affirmer qu'une chose dématérialisée ne pourra jamais devenir une monnaie.

Un autre type d'argument en faveur de la cryptodevise consiste à renverser le raisonnement à la manière de Šurda [2014] : vu que tout moyen de règlement est, d'après le théorème de régression, une marchandise au départ, et comme il est indéniable que le bitcoin sert aujourd'hui à régler des transactions, le caractère *a priori* apodictique de ce théorème implique que le bitcoin a bien dû être perçu d'abord comme une marchandise ; soutenir que le bitcoin ne peut pas satisfaire le théorème de Mises reviendrait dès lors à remettre celui-ci en cause, ce qui n'a pas de sens dans la logique autrichienne. Mais on se heurte dans ce cas à l'écueil du dogmatisme et on retombe sur le

35 D'où la critique de Rothbard [1992] au sujet de la privatisation de l'offre de monnaie envisagée par Hayek [1976], proposition jugée totalement irréaliste.

36 La sortie de la version 0.1 du logiciel Bitcoin a été annoncée par Satoshi Nakamoto le 9 janvier 2009 et le premier taux de change contre le dollar a été publié le 5 octobre de la même année, le bitcoin valant alors environ un millième de dollar.

PEPS « Monnaies virtuelles »

problème de la circularité du raisonnement : le bitcoin doit respecter le théorème de régression simplement parce que le théorème est toujours vrai et qu'il affirme qu'il le doit.

Une autre réponse consiste enfin à dire qu'il n'y a pas de débat tout simplement parce que la question de savoir si le théorème de régression s'applique aux monnaies virtuelles est sans objet. Davidson et Block [2015] estiment que le théorème de Mises a été mal interprété : il ne dit pas que tout bien remplissant les fonctions d'une monnaie doit d'abord avoir été désiré pour lui-même et non pour son utilité dans l'échange, mais simplement qu'un moyen d'échange peut apparaître, même s'il ne possède aucune valeur d'usage direct, du moment qu'il existe déjà un système de prix, ou même la mémoire d'un tel système, pour permettre aux agents économiques d'évaluer son pouvoir d'achat et de le comparer avec celui des autres actifs, d'où l'acceptation du billet de banque en tant que moyen de règlement malgré son absence de valeur intrinsèque. En d'autres termes, dans une perspective historique, seule la première marchandise à avoir été utilisée comme intermédiaire général des échanges a dû avoir une valeur d'usage et être initialement demandée pour ses propriétés intrinsèques dans ce qui était alors une économie de troc pur, quand il n'existait encore aucun système de prix absolu.

3.2. Or numérique et concurrence entre les cybermonnaies

Si l'on admet que le bitcoin peut être considéré comme une monnaie dans le sens où son existence ne soulève aucune contradiction avec le théorème de régression, la logique économique dans laquelle s'inscrit sa création et ses caractéristiques semblent à première vue faire de lui le candidat idéal du point de vue de l'école autrichienne.

Le projet Bitcoin a clairement pour but de mettre sur pied un système de paiement parfaitement sécurisé, capable de fonctionner sans États ni banques centrales. En cela, il se situe dans le prolongement direct des expériences datant de la fin des années 1990, comme la *b-money* imaginée par Wei Dai pour valider des accords contractuels dans l'anonymat ou le *bit gold* de Nick Szabo. Leur volonté commune de libérer par la cryptographie les individus de toute influence étatique sur le plan monétaire et de préserver leur vie privée prend racine dans les idées du mouvement *cypherpunk*³⁷, apparu avec l'émergence d'Internet, à la confluence des thématiques anarchistes, du libertarianisme et des problématiques soulevées par le développement rapide des nouvelles technologies de l'information et de la communication³⁸. Sur le plan purement économique, que le projet Bitcoin ait vu le jour très peu de temps après le krach boursier de septembre 2008 n'est sans doute pas un hasard. Cet extrait de Satoshi Nakamoto [2009] est particulièrement instructif sur les références sous-jacentes : « *Le problème fondamental avec la monnaie conventionnelle réside dans la confiance requise pour son bon fonctionnement. Il faut faire confiance à la banque centrale pour qu'elle n'altère pas sa valeur, 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 électroniquement, mais elles le prêtent en masse dans des bulles de crédit en conservant à peine une fraction en réserve.* » La défiance manifeste dans ces trois phrases à l'égard des banques centrales, du papier-monnaie à cours forcé et du système bancaire à réserves fractionnaires renvoie clairement au courant libéral autrichien et à sa théorie des cycles économiques, développée par Mises puis Hayek, et revenue au premier plan en 2008.

37 Le terme *cypherpunk* est un jeu de mots combinant l'univers cyberpunk et l'utilisation des techniques de chiffrement (*cipher* en anglais).

38 On rencontre d'ailleurs souvent le mot « cryptoanarchie » dans les nombreux articles consacrés aux monnaies virtuelles.

PEPS « Monnaies virtuelles »

En effet, ce courant, qui s'appuie sur la distinction originelle de Wicksell entre le taux d'intérêt « monétaire », fixé sur le marché des fonds prêtables, et le taux d'intérêt « naturel », mesuré par la productivité marginale du capital à l'équilibre de plein emploi, situe l'origine des crises dans la création monétaire excessive et l'écart que celle-ci induit entre ces deux taux. Il présente donc aussi en cela une filiation avec la *currency school* qui souligne la responsabilité majeure des banques centrales, à travers leur action sur le crédit, dans l'existence et la récurrence des cycles économiques. Leurs politiques expansionnistes et la possibilité pour les banques de second rang de prêter plus d'argent qu'elles n'en ont en dépôt alimentent les bulles spéculatives et déforment les structures des prix et de la production en conduisant les entreprises à réaliser des investissements injustifiés qui ne répondent pas aux préférences intertemporelles des consommateurs. Lorsque les crédits ne peuvent plus être octroyés au même rythme qu'auparavant, l'expansion se transforme en récession. Si les auteurs autrichiens ont ainsi toujours vu l'origine du mal dans l'offre de monnaie incontrôlée, leur solution pour retrouver la stabilité a cependant évolué au cours du temps. Le grand intérêt du bitcoin aux yeux de ses partisans est qu'il permettrait d'envisager aussi bien le retour à un système comparable à l'étalon-or que le développement d'un régime de concurrence entre des monnaies privées.

La première voie, défendue par Mises et Rothbard, mais également Hayek au début de sa carrière, consiste à lier la valeur des devises à l'or pour discipliner la création monétaire, les réserves de métal des banques centrales devant assurer la couverture totale des billets émis. Les plus fervents partisans des monnaies virtuelles estiment possible le passage à terme à un régime d'étalon-bitcoin dans lequel tous les échanges se feraient au moyen du bitcoin ou seraient garantis par celui-ci. Dans la mesure où l'algorithme de création des nouveaux bitcoins vise justement à imiter l'exploitation des gisements aurifères, il ne serait plus possible de manipuler la quantité de monnaie disponible. Weber [2016] avance que la marge de manœuvre des banques centrales dans la fixation de leur taux directeur serait même moindre que ce qu'elle était sous l'étalon-or du fait de la disparition des coûts d'arbitrage pour les opérations internationales.

La quantité fixe de monnaie dans le système de l'étalon-bitcoin et le biais déflationniste de ce dernier ne sont pas perçus comme des problèmes par ses partisans. Ainsi, le site Internet Bitcoin, dans sa foire aux questions³⁹, estime d'une part que la limite indépassable de 21 millions d'unités n'est pas contraignante, sachant que le bitcoin peut être divisé jusqu'à la huitième décimale, et d'autre part que la possibilité d'une spirale déflationniste et d'une récession économique à cause du comportement d'attente des agents privés ne semble « pas toujours avérée ». Le lien avec les idées de l'école autrichienne apparaît ici clairement. L'une des critiques récurrentes adressées au système de l'étalon-or est que la quantité du métal précieux est insuffisante pour servir de monnaie, ce à quoi les économistes autrichiens répondent que n'importe quelle quantité de monnaie convient du moment que les prix peuvent se fixer librement sur le marché⁴⁰. Sur le second point, on retrouve les positions de Rothbard ou Hülsmann, pour lesquels la déflation n'exerce aucun effet dépressif dès lors que les prix de vente et les coûts de production baissent simultanément, de sorte que les marges des entreprises ne s'en trouvent pas affectées. Ces deux auteurs ne voient dans la lecture keynésienne du phénomène qu'un mythe, les agents ne reportant pas indéfiniment leurs achats. De façon plus générale, dans la conception autrichienne, la déflation est parfaitement naturelle dans un système de marchés libres et ne traduit que le progrès technique et les gains de productivité⁴¹.

39 Voir la page <https://bitcoin.org/fr/faq#general>.

40 Citons à ce sujet Mises [1949] : « La quantité de monnaie disponible dans l'économie est toujours suffisante pour permettre à chacun tout ce que la monnaie fait et peut faire. »

41 On trouvera dans Bagus [2003] une comparaison des positions des principaux représentants de l'école autrichienne sur la question de la déflation. Il en ressort que l'opinion de Rothbard en la matière se distingue assez nettement de

PEPS « Monnaies virtuelles »

L'expérience de l'étalon-or entre 1880 et 1914, durant laquelle la croissance associée à la première mondialisation a coïncidé avec des tendances déflationnistes, constitue donc un cadre de référence qu'il s'agirait de retrouver grâce aux cyberdevises.

La seconde voie pour en finir avec les désordres monétaires a été proposée par Hayek au milieu des années 1970. Elle consiste à abolir le monopole de la banque centrale pour l'émission de billets et à permettre aux établissements bancaires d'émettre eux-mêmes leur propre monnaie. Ces nouvelles monnaies, qui porteraient des noms différents pour identifier leur émetteur, pourraient être utilisées par les agents économiques pour régler leurs transactions et être librement converties à leur demande. Cette idée, qui apparaît encore aujourd'hui résolument novatrice sur le plan de la théorie monétaire, est sur le fond cohérente avec les fondements de la pensée hayékienne, qui pose la concurrence comme un « processus de découverte » dont la finalité est l'émergence des éléments les plus efficaces. Si la concurrence dans le secteur des biens et services est par nature toujours bonne, pourquoi en irait-il autrement dans le domaine monétaire ? La monnaie étant un bien comme un autre, la régulation par le marché devrait être élargie à la sphère monétaire. Chaque banque émettant sa propre monnaie serait en effet contrainte, par le mécanisme de la concurrence, à gérer sa quantité de façon à répondre au mieux aux intérêts de ses détenteurs, donc à ne pas abuser de la possibilité qui lui est octroyée, puisque celle qui se lancerait dans une émission excessive verrait la valeur et l'acceptabilité de sa monnaie décliner ; en l'absence de toute inflexion de sa politique, une telle banque serait vouée à terme à disparaître. Ainsi, la concurrence entre les monnaies et la détermination de leur taux de change par le marché inverseraient la loi de Gresham, puisque les bonnes monnaies chasseraient alors les mauvaises. Cette concurrence est pour Hayek la meilleure façon de réinscrire le système monétaire dans la logique de l'ordre spontané, interrompue par la généralisation du monopole étatique, et d'échapper ce faisant aux conséquences désastreuses de l'inflation, perçue comme une véritable menace pour la démocratie.

En rompant avec le principe tenu pour acquis que la gestion monétaire doit être du ressort des autorités, cette proposition a soulevé à l'époque l'incrédulité de la plupart des économistes, ou pour le moins beaucoup de scepticisme quant à sa faisabilité, y compris à l'intérieur du camp autrichien. Mais l'univers concurrentiel des cyberdevises semble désormais offrir un terrain concret d'application, d'autant que la technologie qui leur est associée, en supprimant les intermédiaires et en rendant possible leur utilisation à l'échelle mondiale, résout le problème initialement attendu de l'augmentation des coûts de transaction due à la multiplicité des monnaies en circulation⁴². Il est certes encore trop tôt pour vraiment évaluer la capacité des devises virtuelles à faire émerger un régime comparable à celui imaginé il y a 40 ans par Hayek, d'autant que les quelques épisodes historiques de *free banking* aux 18^e et 19^e siècles ne permettent guère de trancher la question de la supériorité des monnaies privées sur les monnaies d'État et qu'ils se sont déroulés dans des conditions différentes de celles qu'il envisageait⁴³. Si l'expérience de l'Écosse entre 1717 et 1845,

celle des autres auteurs de ce courant, qui auraient tendance à devenir interventionnistes face à une contraction de la masse monétaire.

42 La très grande faiblesse des frais de transaction avec Bitcoin, évalués à moins de 1 % quand les commissions prélevées par les intermédiaires financiers avec les autres systèmes de télépaiement se situent à l'heure actuelle entre 2 % et 10 %, est l'un de ses avantages régulièrement mis en avant par ses utilisateurs. La banque Goldman Sachs a calculé en 2013 que les économies de frais de transaction découlant de la généralisation de l'usage de cette cryptomonnaie pourraient avoisiner les 210 milliards de dollars par an.

43 Hayek lui-même était extrêmement critique à l'égard des premiers défenseurs de l'émission de monnaies privées, puisqu'il les considérait comme une « bande d'excentriques avec un fort penchant pour l'inflation ». En effet, ceux-ci voyaient dans le monopole de l'État non pas la source de la surabondance de l'offre de monnaie, mais bien au contraire le facteur explicatif de son insuffisance.

PEPS « Monnaies virtuelles »

peut-être la plus connue en la matière, semble avoir montré que l'offre de monnaies concurrentes n'est pas nécessairement inflationniste, d'autres essais se sont révélés être des échecs patents⁴⁴.

On peut néanmoins tenter d'esquisser une réponse à partir des conditions identifiées par Hayek [1976] pour qu'une monnaie privée puisse faire l'objet d'une demande durable de la part des agents. Il faut naturellement que ces derniers s'attendent à ce que cette monnaie conserve son pouvoir d'achat dans le temps. Dans le cas du bitcoin, l'algorithme intangible qui organise sa rareté remplit cette condition, mais il implique aussi une inélasticité totale de l'offre de monnaie. Cette caractéristique est-elle compatible avec le mode de régulation auquel pensait Hayek ? Si une monnaie se dépréciant constamment doit être d'après ce dernier vite abandonnée par les agents, une monnaie avec la tendance contraire ne se révélera pas nécessairement plus attractive. Pour Hayek, à la différence d'une banque centrale dont la situation de monopole lui permet de ne pas craindre la dépréciation de ce qu'elle émet, il est dans l'intérêt même de la banque privée de conférer à sa monnaie la valeur la plus stable possible : cette stabilité est la condition de sa survie, et c'est précisément la concurrence avec les autres établissements privés qui constitue la meilleure incitation à fournir cette stabilité. Certes, rien *a priori* n'empêche dans son schéma les émetteurs privés d'adopter des stratégies différentes selon la clientèle visée, étant donné que les agents avec une capacité de financement rechercheront les monnaies qui s'apprécient alors que les emprunteurs rechercheront celles qui tendent à se déprécier, mais la confrontation des intérêts individuels devrait quand même aboutir d'après lui à une préférence collective pour les monnaies avec un cours stable. La raison tient au fait que c'est essentiellement dans leur fonction de mesure de la valeur que les monnaies devraient être comparées, et cette fonction « *devrait susciter une préférence générale pour une monnaie stable* », car « *la conservation de la valeur des capitaux et le contrôle des coûts ne sont possibles que si les comptes sont tenus dans une unité qui d'une certaine façon reste d'une stabilité tolérable* » ; ainsi, chaque émetteur privé devrait s'engager à « *assurer l'invariance du prix agrégé en termes de sa propre monnaie d'un ensemble particulier de marchandises* » (Hayek [1976], cité dans Tutin [1989]). Le problème dans le cas du bitcoin est qu'il n'y a rien pour assurer cette régulation, c'est-à-dire pour limiter la pression à la hausse sur son cours vis-à-vis des autres devises. La volonté manifeste de contourner de la banque centrale et son émission entièrement privée, si elles permettent bien sûr un rapprochement du point de vue de la philosophie générale, ne doivent donc pas occulter les différences qui subsistent avec le projet hayékien d'origine.

Certains chercheurs, conscients de cette limite, se sont intéressés aux révisions qui pourraient être apportées au protocole Bitcoin pour introduire la possibilité d'un ajustement de la quantité disponible en réaction à une variation du cours du change (Ametrano [2014], Iwamura *et al.* [2014]). Ces modifications pourraient prendre la forme de règles contingentes à l'état de l'économie ou de normes prévoyant une croissance régulière du stock de monnaie qui serait calée sur celle du revenu dans la longue période, à l'instar de la règle du $k\%$ de Friedman [1968]. La force des cybermonnaies est que l'ajout de telles modifications ne soulève pas de difficultés particulières, du moins sur le plan purement technique⁴⁵. En fait, dans la mesure où une monnaie virtuelle est

44 L'expérience du *free banking* durant le 19^e siècle fut notamment marquée aux États-Unis par l'apparition de nombreux établissements véreux, symboles de la « finance sauvage » (*wildcat banking*), qui lésèrent beaucoup de déposants, et des taux élevés de faillite bancaire. En Australie, elle conduisit à une bulle financière dont l'éclatement entraîna dans les années 1890 une contraction de l'activité plus forte que celle qui suivit le krach de 1929.

45 Ces modifications correspondent techniquement à des programmes d'embranchement (des « fourches », ou *forks*). Le protocole Bitcoin permet aussi bien une évolution radicale (*hard fork*) qu'une évolution plus graduelle (*soft fork*), le premier type d'évolution impliquant l'apparition d'une nouvelle version du programme qui n'est pas compatible avec les autres versions, alors que le second type permet aux nœuds du réseau d'utiliser encore les versions précédentes pour pouvoir valider les nouvelles transactions. Une adaptation de l'offre d'une cybermonnaie à sa demande renvoie au premier type. Cependant, l'adaptabilité de Bitcoin ne semble peut-être pas aussi grande dans

PEPS « Monnaies virtuelles »

indissociable de l'algorithme déterminant son émission et le mode de rémunération des mineurs, tout changement dans le protocole de construction de la *blockchain* signifie automatiquement la création d'une nouvelle monnaie. Les cryptodevises peuvent donc suivre autant de règles que ce qu'il est possible d'en imaginer, et leurs utilisateurs basculer instantanément de l'une à l'autre en fonction de la règle vers laquelle vont leurs préférences. Par exemple, certaines de ces monnaies peuvent être qualifiées d'inflationnistes par opposition aux caractéristiques du bitcoin, soit parce qu'aucune limite stricte n'a été définie, comme pour le peercoin, lancé en 2012 et conçu pour connaître un taux d'inflation annuel de 1 %, soit parce que leur détention occasionne des frais, comme dans le cas du freicoin qui perd 5 % de sa valeur chaque année⁴⁶.

La coexistence actuelle de nombreuses cryptomonnaies est donc sans doute différente de la concurrence à laquelle devait penser Hayek dans son projet de dénationalisation des espaces monétaires, sans parler des aspects technologiques qu'il ne pouvait deviner il y a 40 ans. La concurrence, dans son analyse, doit empêcher chaque banque privée de fixer à sa guise la quantité disponible de sa propre monnaie dès lors que les autres sont de parfaits substituts, et doit également, à l'issue d'une période de transition, « *conduire à l'acceptation générale d'un étalon universel largement utilisé (ou peut-être à celle d'un nombre très limité d'étalons)* » (Hayek [1976], cité dans Tutin [1989]). Or, les cryptomonnaies ne sont pas de parfaits substituts, puisque les spécificités introduites dans l'algorithme pour gérer leur rareté relative les destinent *a priori* à des utilisations distinctes. Si le bitcoin est d'abord détenu dans l'optique d'une plus-value financière, une devise fondante telle que le freicoin est au contraire conçue pour être dépensée rapidement. Ces différents usages des devises virtuelles, qui renvoient à la notion précédemment mentionnée de monnaies monofonctionnelles au sens de Polanyi, suggèrent que leur coexistence pourrait durer et par conséquent limiter leur caractère concurrentiel.

Par ailleurs, la possibilité évoquée un peu plus haut de s'appuyer sur une règle de croissance à un rythme régulier de la quantité d'une monnaie virtuelle, dans le but de stabiliser son pouvoir d'achat, ne s'accorde absolument pas avec la vision de Hayek, qui s'est toujours montré critique vis-à-vis de la théorie quantitative parce qu'elle ignore les conséquences sur la structure de production de la modification des prix relatifs induite par la création monétaire. Cette théorie suppose l'existence d'un seul type de monnaie dont la quantité pourrait être mesurée par l'addition d'unités homogènes ; or, pour Hayek, même dans une économie n'ayant que la monnaie d'État, il existe toujours des substituts plus ou moins liquides à celle-ci, de sorte que parler de masse monétaire n'a guère de sens. Si la théorie quantitative n'est déjà pas pertinente quand une seule monnaie circule à l'intérieur d'un territoire, elle le sera encore moins avec une pluralité de devises soumises à un processus concurrentiel : dans ce dernier cas, « *le montant de la masse monétaire se*

les faits, comme le suggère le départ en janvier dernier de Mike Hearn, l'un des développeurs historiques du logiciel, après avoir annoncé qu'il ne croyait plus dans le projet et que le bitcoin est mort de son point de vue. La raison de ce départ est l'absence de consensus sur les modifications à apporter à l'algorithme, plus précisément à la taille des blocs, dont le maximum actuel est de 1 Mo, pour pouvoir absorber un volume plus important de données et éviter la saturation du système d'échange. En l'état, le réseau ne pourrait traiter que 7 transactions environ par seconde, quand on estime que le système Visa pourrait en principe supporter jusqu'à 10 000 transactions par seconde. Plus largement, les intérêts de tous les participants à l'expérience ne sont pas convergents : l'idéal de départ des programmeurs de fournir un système sans aucune contrainte se heurte au désir des entreprises et des banques intéressées par cette nouvelle technologie d'apporter les modifications susceptibles de répondre aux attentes de leurs clients, pendant que les mineurs se préoccupent surtout de leur rémunération et redoutent la chute des cours qui pourrait résulter de la multiplication des systèmes parallèles.

46 De façon générale, il y a presque autant de limites d'émission que de cryptomonnaies. Certains systèmes, comme Dash ou Namecoin, prévoient une quantité en circulation identique ou comparable à celle du bitcoin. D'autres ont fixé des limites beaucoup plus hautes, comme Litecoin (84 millions), MaidSafecoin (4,3 milliards) ou Ripple (100 milliards).

PEPS « Monnaies virtuelles »

déduit de la valeur relative des différentes devises et n'a en lui-même aucune signification » (Hayek [1976], cité dans Tutin [1989]). Définir une règle stricte visant à contrôler l'évolution de l'offre de monnaie n'a jamais fait partie du projet hayékien.

Malgré ces différences, le rapprochement entre l'univers des cryptomonnaies et l'œuvre de l'économiste autrichien est logique. Le bouillonnement d'idées nouvelles et la multiplication des expériences dans ce domaine en seulement quelques années ressemblent en effet à une illustration du processus de sélection naturelle qu'il a toujours défendu et à l'issue duquel ne devraient normalement être conservées que les monnaies jugées les plus adaptées par une majorité d'internautes. Le point essentiel pour les tenants de cette vision est que l'ordre spontané qui résultera de ce processus ne pourra qu'être supérieur au système actuel des monnaies d'État gérées par les banques centrales.

4. Quelle place pour le bitcoin dans le paradigme hétérodoxe ?

À la différence de l'approche réaliste, selon laquelle la détention et l'utilisation de la monnaie doivent être analysées sur la base des motivations personnelles, conformément au principe de l'individualisme méthodologique, la conception institutionnaliste s'inscrit dans une démarche holiste et souligne d'emblée le caractère fondamentalement collectif de la monnaie. Avant d'être un instrument économique, la monnaie est d'abord un outil de cohésion sociale, ou, pour employer la formule célèbre de Mauss, un « *fait social total* », son acceptation signifiant l'adhésion aux normes de la société. Elle symbolise l'appartenance des individus à une même communauté et les met en relation les uns avec les autres. Pour Knapp [1905], le fondateur de l'école chartaliste, qui est la première à avoir développé cette idée, « *la monnaie est une créature de la loi* » : il s'agit d'une convention dans le sens où elle est fondée sur la confiance collective dans son acceptation comme moyen de règlement ultime. Le support utilisé importe peu ; la monnaie n'a pas à être liée à un bien particulier, contrairement à ce qu'affirme le théorème de régression. C'est l'autorité chargée de faire respecter cette convention, c'est-à-dire l'État pour les chartalistes, qui sélectionne sa forme et impose son utilisation à l'intérieur du territoire. Il s'ensuit que la monnaie se définit dans cette grille de lecture à partir de sa fonction d'unité de compte, et que l'acceptation de cette unité de compte favorise sa circulation et lui confère dès lors sa fonction d'intermédiaire des échanges.

On retrouve ce rôle prééminent de la fonction d'unité de compte chez Keynes [1930], pour qui « *la monnaie de compte est le concept premier de toute théorie monétaire* ». Dans son *Traité sur la monnaie*, la nature politique du signe monétaire se manifeste initialement dans l'unité de compte permettant l'expression des dettes et des prix (Pineault [2003]). Cette monnaie de compte est pour Keynes le point de départ de l'évolution monétaire et précède la monnaie-crédit, développée dans sa *Théorie générale* (Keynes [1936]), puis reprise par les post-keynésiens pour décrire une « économie monétaire de production », par opposition à une « économie d'échanges réels », et défendre une conception endogène de la monnaie.

L'approche institutionnaliste qui s'est par la suite développée en France à partir des années 1980 (Aglietta et Orléan [1982]) a intégré les apports des autres sciences humaines, en particulier l'anthropologie et l'histoire. Son point de départ est la contestation de l'idée que le troc aurait précédé la monnaie en tant que mode d'organisation des échanges. C'est au contraire la monnaie qui permet l'échange en introduisant la notion de valeur et un espace commun

PEPS « Monnaies virtuelles »

d'évaluation des choses. Le troc n'est qu'une fable commode utilisée par les classiques pour expliquer l'apparition de la monnaie ; si le troc a certes existé à un niveau local, et s'il a aussi été observé dans des cas extrêmes de monnaies détruites par l'hyperinflation, il n'a pour autant jamais constitué le principe structurant d'un système d'échanges entièrement décentralisés, les anthropologues et les historiens n'ayant trouvé aucun exemple dans les sociétés primitives permettant d'accréditer cette thèse. La différence avec le chartalisme, qui donne à l'État un rôle direct dans l'acceptation de la monnaie en la reliant au paiement de l'impôt, est que cette approche interdisciplinaire insiste davantage sur l'influence du pouvoir dans la convergence mimétique des opinions vers la même croyance. Mais l'existence de la monnaie est inséparable pour les deux d'une instance supra-individuelle attestant d'une hiérarchie au sein de son espace de circulation.

Comme le note Orléan [2007], le courant institutionnaliste reprend la pensée keynésienne et post-keynésienne. De manière plus générale, les nombreux points de rapprochement, sur l'importance de l'unité de compte, le rejet de la dichotomie des volets réel et monétaire et donc de la neutralité de la monnaie, le refus de l'hypothèse d'hyperrationalité des agents économiques, la reconnaissance des limites des mécanismes du marché et de la nécessité de l'intervention étatique, mais aussi la conception endogène de la monnaie, permettent sans doute de regrouper ces deux ensembles théoriques dans le même paradigme épistémologique hétérodoxe qui se caractérise par sa rupture fondamentale avec la grille de lecture dominante (Fémenias [2012]).

L'apparition du bitcoin soulève deux problèmes par rapport à ce paradigme. D'une part, les règles mathématiques commandant l'évolution de sa quantité en circulation en font une monnaie totalement exogène et sont donc incompatibles avec la vision keynésienne selon laquelle ce sont les entreprises qui sont à l'origine de l'émission monétaire par leur demande de fonds prêtables. D'autre part, si la monnaie est une construction sociale impliquant une autorité supérieure pour garantir la confiance que nécessite son utilisation, elle ne saurait *a priori* exister en dehors de cette autorité. Or, c'est précisément ce lien entre la monnaie et le pouvoir que les promoteurs du bitcoin et des autres devises virtuelles cherchent à supprimer.

4.1. Le bitcoin : une aberration dans une économie monétaire de production

La théorie classique énonce traditionnellement que la monnaie est exogène dans la mesure où les autorités sont supposées capables de contrôler le stock de monnaie disponible pour les agents à partir des instruments dont elles disposent, de sorte que ce stock n'est pas expliqué par les variables réelles. C'est la conception de la *currency school* au 19^e siècle, défendant une gestion stricte de l'émission de monnaie pour garantir la couverture en or des billets en circulation et éviter ainsi l'inflation, puis des monétaristes avec la théorie du multiplicateur de crédit, selon laquelle la banque centrale peut directement agir sur l'évolution de la masse monétaire par son contrôle de la base monétaire. Même s'il n'existe aucune autorité dans le cas du bitcoin, les règles de son émission renvoient à ce principe. Sa particularité est que c'est la technologie elle-même qui tient en quelque sorte lieu de mécanisme régulateur, dans le sens où l'algorithme a fixé dès le départ une limite à la création monétaire. Mais c'est là une méthode de régulation sommaire, et surtout totalement inappropriée du point de vue keynésien.

L'une des caractéristiques majeures de l'économie post-keynésienne est de renverser le point de vue classique et de défendre une conception endogène de la monnaie. Elle se fonde sur l'idée que les banques de second rang ne peuvent créer de la monnaie, par l'octroi de crédits, que si une demande de fonds leur est d'abord adressée. En d'autres termes, ce sont les variations de l'activité et du revenu qui expliquent l'évolution de la masse monétaire. À la différence de l'économie d'échanges réels des classiques, dans laquelle la neutralité de la monnaie ne fait jouer à

PEPS « Monnaies virtuelles »

cette dernière aucun rôle, l'économie monétaire de production des keynésiens implique que la création monétaire par le crédit bancaire dépend avant tout des besoins des agents et qu'elle s'avère également nécessaire pour enclencher le processus productif. On retrouve ici le motif de financement de Keynes, c'est-à-dire que la monnaie est aussi demandée pour pouvoir financer la création de richesses, en raison du décalage temporel entre les dépenses indispensables pour lancer la production et l'encaissement par les entreprises du produit de leurs ventes.

La controverse sur la nature exogène ou endogène de la monnaie a bien évidemment des implications majeures sur le choix du système monétaire. Si la monnaie est endogène, tout rattachement à un métal précieux dont la quantité est par nature finie risque de provoquer à terme une pénurie de moyens de paiement préjudiciable à l'activité. Dès lors, si le système fondé sur l'or métallique était déjà une « relique barbare » dans les années 1920, pour reprendre l'expression bien connue de Keynes, celui de l'or numérique se heurte inévitablement à la même critique un siècle plus tard. Krugman [2011] ne voit ainsi dans Bitcoin qu'une tentative de réintroduction de l'étalon-or et une menace déflationniste. Une monnaie qui se prête davantage à l'épargne qu'à la dépense et l'absence d'un système bancaire capable de garantir le financement de l'économie réelle ne peuvent être que des problèmes dans la logique keynésienne (Dupré *et al.* [2015]). L'idée ou l'espoir que le bitcoin pourrait être une partie de la réponse aux défis actuels ne trouvent donc ici aucune justification.

4.2. Bitcoin et le remplacement des institutions par la technologie

La monnaie est un symbole de la valeur accepté par la société qui en fait usage. C'est précisément parce qu'elle est un symbole qu'elle ne peut fonctionner que sur la base d'une confiance collective dans ce que celui-ci représente et dans son acceptabilité inconditionnelle dans l'échange, c'est-à-dire qu'elle implique l'engagement de la société elle-même à fournir l'équivalent réel de cette valeur. Ce rôle central de la confiance fait que toute monnaie, quelle que soit sa forme, est, en dernière instance, toujours fiduciaire. Simiand [1934] l'a exprimé dans une formule restée célèbre : « *L'or n'est que la première des monnaies fiduciaires.* »

Selon les institutionnalistes, la confiance dans la monnaie revêt traditionnellement trois formes qui doivent s'articuler harmonieusement entre elles (Aglietta et Orléan [1998], Théret [2008]). La première correspond à la confiance *méthodique* provenant de la répétition journalière des opérations d'achat, ce qui crée une routine et fournit aux agents économiques des repères leur permettant de s'assurer du bon fonctionnement des pratiques monétaires. Cette première forme vise à instaurer un climat de sécurité propice à la répétition des transactions et souligne l'importance des mécanismes mimétiques. Elle demeure toutefois insuffisante dans le sens où elle n'élimine pas définitivement le doute dans les relations contractuelles. Un niveau plus élevé de confiance s'avère donc nécessaire, d'où la confiance *hiérarchique* impliquant l'acceptation d'un rapport de subordination à une instance supérieure en charge de définir les règles encadrant l'utilisation de la monnaie et de veiller à leur respect. La banque centrale, en tant que prêteuse en dernier ressort et émettrice du moyen de règlement ultime, contribue à renforcer la confiance dans le système, car c'est bien l'acceptation de ce moyen de règlement qui constitue le pivot de l'ordre marchand. La troisième et dernière forme de confiance est la forme *éthique*, qui se situe au-delà du politique et renvoie à un consensus sur des normes et des valeurs collectives, l'acceptation de la monnaie traduisant *in fine* sa conformité à ces éléments. Cette forme supérieure légitime ainsi l'ordre politique qui institue les règles monétaires. Il existe donc une hiérarchie entre ces trois niveaux de confiance : la confiance méthodique est assurée par le pouvoir auquel est associée la confiance hiérarchique, qui se trouve elle-même subordonnée à la confiance éthique.

PEPS « Monnaies virtuelles »

L'application de cette grille de lecture aux devises virtuelles suggère que ces trois formes de confiance sont toutes remises en cause, à des degrés divers, par la *blockchain*. La confiance méthodique d'abord, ne serait-ce que parce que ces devises n'ont justement aucun support physique ; l'obligation de recourir à un ordinateur, une tablette ou un smartphone et un niveau minimal de compréhension du fonctionnement du système peuvent être de nature à limiter le caractère routinier des transactions. Mais aussi et surtout à cause des affaires qui ont sérieusement écorné leur image, avec la disparition début 2014 de la plate-forme MtGox après sa déclaration d'un vol de 850 000 bitcoins (soit près d'un demi-milliard de dollars au cours de l'époque), puis la fermeture moins d'un mois plus tard de l'intermédiaire canadien Flexcoin suite au vol des 896 bitcoins qu'il stockait en ligne, ou encore l'annonce récente par la place d'échange Cryptsy du gel complet des transactions consécutivement au vol de 13 000 bitcoins et 300 000 litecoins. Le caractère public de la chaîne de blocs, qui est toujours mis en avant pour garantir la validité des transactions, n'est clairement pas suffisant. De plus, les détenteurs ne disposent d'aucun recours juridique en cas de piratage des données et de vol. On touche là les limites de Bitcoin : comment sécuriser un système de paiement qui impose lui-même l'absence de toute autorité de contrôle ?

Cette question renvoie à la seconde forme de confiance et reçoit une réponse simple de la part des partisans des cryptodevises : la sécurité par la technologie. Il n'est pas anodin que la devise *In God We Trust* qui figure sur tous les billets américains, et qui traduit mieux que toute autre l'entremêlement du sacré et de la loi qui caractérise la monnaie, ait été détournée pour devenir *In Technology We Trust*. Tout est dit dans cette formule. Il ne faut pas comprendre par là que la question de la confiance est rendue obsolète par l'apparition de la chaîne de blocs. La monnaie sera toujours indissolublement liée à la confiance, quelle que soit sa forme. Cette nouvelle devise révèle simplement la croyance ferme que les missions assignées d'habitude aux institutions peuvent être aisément remplies par des acteurs privés de manière totalement décentralisée. En un sens, ce n'est pas tant cette confiance qui disparaît dans leur projet que le support censé l'installer qui change radicalement. Cette évolution demanderait en fait de requalifier la seconde forme de confiance, vu que le système Bitcoin a précisément été conçu pour rompre dans son fonctionnement avec le principe même de la hiérarchie. Peut-être faudrait-il à présent parler de confiance « numérique ». Mais cette nouvelle forme de confiance peut-elle vraiment s'installer sans la moindre référence à la puissance publique ? Les cas de piratage et de vol mentionnés un peu plus haut conduisent malheureusement à douter de la réelle fiabilité d'un système sans aucune autorité de contrôle et qui se contente d'affirmer que la gouvernance est l'affaire de tous.

Le bitcoin ne permet pas non plus d'installer la troisième forme de confiance fondée sur des considérations éthiques dans la mesure où les logiques poussant à son utilisation sont différentes, voire antagoniques (Lakomski-Laguerre et Desmedt [2015]). La communauté Bitcoin est en effet composée à la fois de libertariens qui y voient l'occasion de contester la puissance de l'État, de *geeks* et de développeurs intéressés par les nouveaux usages qui pourraient être imaginés à partir de la *blockchain*, et de spéculateurs qui se soucient finalement assez peu de ces avancées et qui envisagent d'abord les gains potentiels associés à l'évolution de son cours. Comme le font remarquer ces deux auteurs, si les entrepreneurs ont naturellement tout intérêt à ce que l'image du bitcoin s'améliore dans l'opinion publique, pour que le nombre de transactions sur biens et services continue de progresser, les investisseurs qui n'y voient qu'une nouvelle source potentielle de profits sont beaucoup moins regardants sur ce point et sur les activités illégales qui peuvent être associées à la cryptomonnaie. De même, les acteurs poussés par une logique entrepreneuriale eu égard aux multiples possibilités offertes par la *blockchain* verront peut-être dans l'absence de protection par les pouvoirs publics un frein à leurs projets, alors que cet élément est décisif aux yeux des cryptoanarchistes. Ces attentes différentes au sujet du bitcoin ne peuvent que compliquer son

PEPS « Monnaies virtuelles »

entreprise de légitimation et semblent difficilement conciliables avec le principe de valeurs collectivement acceptées qui fonde la notion de confiance éthique.

Ce paradigme conduit finalement à voir dans le bitcoin un curieux paradoxe. Issu d'une réflexion critique sur les politiques des banques centrales et les dérives de la finance ayant mené à la crise (Nakamoto [2009]), il tend pourtant aujourd'hui, du fait de sa quantité limitée, à ressembler davantage à une illustration de ces dérives, ainsi qu'en témoigne l'évolution de son taux de change, et pourrait même à l'avenir contribuer à un accroissement de la prise de risque. En effet, en cherchant délibérément à contourner les circuits traditionnels de financement, les cryptomonnaies pourraient potentiellement être dans les années qui viennent à la base d'une nouvelle forme de *shadow banking*. Il paraît clair aujourd'hui que le régulateur ne pourra pas faire l'économie d'une réflexion beaucoup plus poussée sur les réponses à apporter face à leur sophistication grandissante.

5. Remarques conclusives : de Hayek à Gesell

Si les caractéristiques du bitcoin conduisent à conclure qu'il ressemble beaucoup plus à un actif financier qu'à une monnaie, il n'en reste pas moins que la technologie sur laquelle il repose laisse entrevoir des bouleversements de premier ordre. La chaîne de blocs et les protocoles décentralisés de vérification des échanges offrent en effet un nouveau système de paiement susceptible de concurrencer à terme le secteur bancaire traditionnel. Dire dès à présent que Bitcoin annonce la fin des banques est sans doute exagéré, car ce système ne fonctionne qu'en vase clos et ne bénéficie d'aucune garantie publique, mais il est clair qu'il obligera ces dernières à s'intéresser de plus en plus dans les années qui viennent à cette nouvelle technologie et à ses applications potentielles. Cette prise de conscience a en fait déjà débuté, comme l'illustre la fondation en 2014 du consortium R3 CEV (qui regroupe à ce jour plus d'une quarantaine de grands établissements) pour réfléchir à la mise en œuvre d'une *blockchain* partagée qui définirait une nouvelle forme de compensation interbancaire et remplacerait le réseau SWIFT.

Du point de vue des innovations qui ont marqué l'histoire monétaire, cette technologie paraît sans conteste une étape encore plus importante que ne le fut le système de Law, qui chercha au début du 18^e siècle à remplacer l'or par la monnaie papier pour soutenir l'investissement et développer le commerce. La spéculation qui conduisit rapidement à l'effondrement de ce système menace aujourd'hui le bitcoin dans sa dimension monétaire. De même que l'échec de Law laissa des traces dans la mémoire collective et se traduisit par une méfiance durable vis-à-vis du papier-monnaie qui freina le développement du secteur bancaire en France, de même l'échec du bitcoin pourrait limiter significativement le degré d'adhésion aux systèmes purement virtuels et donc leur expansion.

Les solutions théoriques pour réduire la volatilité d'une cybermonnaie dérivée du modèle Bitcoin et encourager son utilisation comme instrument de paiement existent, mais soulèvent aussi des questions. La première consiste à moduler l'offre en fonction de la demande grâce à des programmes d'embranchement. Mais qu'est-ce qui garantit alors que la nouvelle règle de création monétaire sera toujours optimale, ou simplement préférable à celle suivie par une banque centrale ? Il nous semble en outre qu'il n'y a guère de raisons de penser que la critique traditionnelle selon laquelle le décideur public n'est pas forcément bienveillant et ne se soucie pas assez de l'intérêt général ne pourrait pas s'appliquer à des individus isolés. Le marché doit certes faire disparaître les

PEPS « Monnaies virtuelles »

mauvais émetteurs pour Hayek, mais sa capacité d'autorégulation a malheureusement montré ses limites. On peut aussi envisager leur surveillance par les pouvoirs publics, et l'intervention de ces derniers le cas échéant, mais c'est alors reconnaître qu'une autorité souveraine demeure nécessaire dans le domaine monétaire. Plus largement, n'est-il pas illusoire de croire que la technologie et des acteurs privés n'ayant fait l'objet d'aucun choix démocratique constitueraient systématiquement un meilleur support pour la confiance collective que des institutions ?

Une solution complémentaire pour éviter la volatilité excessive de son cours pourrait être l'ancrage à une devise, ou un panier de devises, mais l'idéal de départ du projet se trouverait dès lors perverti. La monnaie privée en question ne serait plus indépendante des monnaies officielles. Le rattachement à des monnaies d'État jugées plus ou moins inflationnistes ou encore trop couplées à la finance entre en contradiction avec la philosophie sous-jacente des promoteurs du bitcoin.

Une autre voie, enfin, consiste à programmer une perte régulière de valeur au fil du temps. Cette solution de la monnaie fondante, qui trouve ses origines dans Gesell [1916], semble être à première vue la plus facile à mettre en place pour développer la fonction d'intermédiaire des échanges et limiter ce faisant la dimension spéculative. Le freicoïn est une tentative d'application du système de « monnaie franche » défendu par cet auteur⁴⁷. Pour ce dernier, la détention de monnaie (qui ne coûte rien) peut freiner la dynamique économique si elle tend à devenir trop longue entre deux achats, d'où son idée de diminuer sa valeur progressivement, selon une règle de dépréciation préalablement définie, afin de la faire circuler plus rapidement. À la différence du bitcoin qui renvoie aux thèses de l'école autrichienne, le freicoïn s'inscrit dans une logique beaucoup plus proche des idées keynésiennes, puisqu'il s'agit de dissuader les agents de thésauriser les unités qu'ils détiennent et de les empêcher de s'enrichir en ne faisant rien⁴⁸.

En conclusion, il apparaît que les monnaies virtuelles, grâce à l'adaptabilité de leurs règles de fonctionnement, permettent de se référer à des approches très différentes, en même temps qu'elles remettent au goût du jour certaines théories que l'on pensait définitivement oubliées. Une cybermonnaie adossée à l'or, le Hayek, a été lancée en 2015, et on aurait tout aussi bien pu dénommer Gesell le freicoïn. Peut-être assisterons-nous dans l'avenir à l'apparition d'une variante baptisée Keynes. Quoi qu'il en soit, l'accélération de leur diffusion au sein de la société en tant que moyens de paiement appelle d'autres révisions de l'algorithme initial dans un sens qui n'est pas forcément celui auquel pensait Satoshi Nakamoto en 2009.

47 Le nom du freicoïn dérive d'ailleurs directement de l'allemand *Freigeld* (« argent libre » ou « monnaie franche »), qui est le terme donné par Gesell lui-même à sa monnaie pour indiquer le fait que les agents économiques ne sont pas incités à la garder.

48 On peut rappeler à ce propos la fameuse phrase de Keynes [1936] dans la *Théorie générale* au sujet de Gesell : « *Je crois que le futur apprendra davantage de l'esprit de Gesell que de celui de Marx.* »

PEPS « Monnaies virtuelles »

Bibliographie

- Aglietta, M., et A. Orléan [1982], *La violence de la monnaie*, Presses universitaires de France, Paris
- Aglietta, M., et A. Orléan (dir.) [1998], *La monnaie souveraine*, Odile Jacob, Paris
- Aït-Kacimi, N. [2014], « Ce que montrent les turbulences du bitcoin », *Les Échos*, 20 août
- Ametrano, F.M. [2014], « Hayek Money : The Cryptocurrency Price Stability Solution », document disponible à la page http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270
- Bagus, P. [2003], « Deflation : When Austrians Become Interventionists », *The Quarterly Journal of Austrian Economics*, vol. 6, n° 4, pp. 19-35
- Banque de France [2013], « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus*, n° 10, 5 décembre
- BCE [2012], *Virtual Currency Schemes*, octobre
- Blanc, J. [2006], « Karl Polanyi et les monnaies modernes : un réexamen », *Contributions à une sociologie des conduites économiques*, L'Harmattan, Paris, pp. 51-66
- Cowen, T., et R. Kroszner [1994], *Explorations in the New Monetary Economics*, Basil Blackwell, Oxford
- Davidson, L., et W.E. Block [2015], « Bitcoin, the Regression Theorem, and the Emergence of a New Medium of Exchange », *The Quarterly Journal of Austrian Economics*, vol. 18, n° 3, pp. 311-338
- Dupré, D., J.-F. Ponsot et J.-M. Servet [2015], « Le bitcoin contre la révolution des communs », communication au 5^e congrès de l'Association française d'économie politique, Lyon, juillet
- Fémenias, L. [2012], « L'approche monétaire de l'économie : vers un paradigme épistémologique hétérodoxe », communication au colloque international de philosophie économique, Sciences Po Lille, 21-22 juin
- Fontan, S. [2014], « Ce que signifie l'émergence du bitcoin », *La Tribune*, 7 octobre
- Friedman, M. [1968], « The Role of Monetary Policy », *The American Economic Review*, vol. 58, n° 1, pp. 1-17
- Gertchev, N. [2013], « The Money-ness of Bitcoins », disponible à la page <https://mises.org/library/money-ness-bitcoins>
- Gesell, S. [1916], *The Natural Economic Order*, Peter Owen, Londres, 1958
- Graf, K.S. [2013], « Bitcoins, the Regression Theorem, and That Curious but Unthreatening Empirical World », disponible à la page <http://www.konradsgraf.com/blog1/2013/2/27/in-depth-bitcoins-the-regression-theorem-and-that-curious-bu.html>
- Hayek, F.A. [1943], « The Facts of the Social Sciences », *Ethics*, vol. LIV, n° 1, pp. 1-13
- Hayek, F.A. [1976], *Denationalisation of Money: An Analysis of the Theory and Practice of Concurrent Currencies*, Institute of Economic Affairs, Londres

PEPS « Monnaies virtuelles »

- Holden, W. [2015], *The Future of Cryptocurrency, Bitcoin & Altcoin: Impact & Opportunities, 2015-2019*, Juniper Research, mars
- Iwamura, M., Y. Kitamura, T. Matsumoto et K. Saito [2014], « Can We Stabilize the Price of a Cryptocurrency? Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money », *Discussion paper series A*, n° 617, Institute of Economic Research, Hitotsubashi University, novembre
- Keynes, J.M. [1930], *A Treatise on Money*, Macmillan, Londres
- Keynes, J.M. [1936], *The General Theory of Employment, Interest and Money*, Macmillan, Londres
- Knapp, G.F. [1905], *The State Theory of Money*, Macmillan, Londres, 1924
- Krawisz, D. [2013], « The Original Value of Bitcoins », disponible à la page <http://nakamotoinstitute.org/mempool/the-original-value-of-bitcoins>
- Krugman, P. [2011], « Golden Cyberfettters », *The New York Times*, 7 septembre
- Lakomski-Laguerre, O., et L. Desmedt [2015], « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, n° 18, automne
- LeRoux, C.D. [2014], « Why Bitcoin Can Never Be Money », *Procesos de Mercado: Revista Europea de Economía Política*, vol. 11, n° 1, pp. 249-271
- Lo, S., et J.C. Wang [2014], « Bitcoin as Money? », *Current Policy Perspectives*, n° 14-4, Federal Reserve Bank of Boston, septembre
- McCallum, B.T. [2015], « The Bitcoin Revolution », *Cato Journal*, vol. 35, n° 2, pp. 347-356
- Menger, K. [1892], « On the Origin of Money », *The Economic Journal*, vol. 2, n° 6, pp. 239-255
- Mises, L. von [1912], *The Theory of Money and Credit*, Yale University Press, New Haven, 1953
- Mises, L. von [1949], *Human Action: A Treatise on Economics*, Yale University Press, New Haven
- Nakamoto, S. [2009], « Bitcoin Open Source Implementation of P2P Currency », disponible à la page http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?xg_source=activity
- Orléan, A. [2007], « L'approche institutionnaliste de la monnaie : une introduction », document de travail, *Paris School of Economics*, disponible à la page <http://provisoire42.free.fr/ISEAG/regul-fi/Orlean/Approche-institutionnelle-de-la-monnaie.pdf>
- Pineault, E. [2003], « Pour une théorie de l'institution monétaire : actualité du *Treatise on Money* », *L'Actualité économique*, vol. 79, n° 1-2, pp. 101-116
- Polanyi, K. [1968], *Primitive, Archaic, and Modern Economies: Essays of Karl Polanyi*, George Dalton (éd.), Garden City, New York
- Ron, D., et A. Shamir [2013], « Quantitative Analysis of the Full Bitcoin Transaction Graph », *Financial Cryptography and Data Security, Lecture Notes on Computer Science*, vol. 7859, Springer, pp. 6-24
- Rothbard, M.N. [1992], « The Case for a Genuine Gold Dollar », in *The Gold Standard: Perspectives in the Austrian School*, Ludwig von Mises Institute, Auburn, pp. 1-17
- Rothbard, M.N. [1995], *Making Economic Sense*, Ludwig von Mises Institute, Auburn

PEPS « Monnaies virtuelles »

Servet, J.-M. [1993], « L'institution monétaire de la société selon Karl Polanyi », *Revue économique*, vol. 44, n° 6, pp. 1127-1150

Shostak, F. [2013], « The Bitcoin Money Myth », disponible à la page <https://mises.org/library/bitcoin-money-myth>

Simiand, F. [1934], « La monnaie, réalité sociale », *Annales sociologiques*, série D, sociologie économique, fasc. 1, pp. 1-58

Šurda, P. [2014], « The Origin, Classification and Utility of Bitcoin », disponible à la page http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436823

Théret, B. [2008], « Les trois états de la monnaie. Approche interdisciplinaire du fait monétaire », *Revue économique*, vol. 59, n° 4, pp. 813-841

Tucker, J. [2014], « Bitcoin and Mises's Regression Theorem », disponible à la page <https://tucker.liberty.me/bitcoin-and-mises-regression-theorem>

Tutin, C. [1989], « Monnaie et libéralisme : le cas Hayek », *Cahiers d'économie politique*, n° 16-17, pp. 153-178

Weber, W.E. [2016], « A Bitcoin Standard: Lessons from the Gold Standard », *Bank of Canada staff working paper*, n° 2016-14, mars

Yermack, D. [2013], « Is Bitcoin a Real Currency? An Economic Appraisal », *NBER working paper*, n° 19 747, décembre

PEPS « Monnaies virtuelles »

RECENT LAREFI WORKING PAPERS

For earlier LAREFI Working Papers, please go to <http://lare-efi.org.u-bordeaux4.fr>

All Discussion Papers can be downloaded free of charge

CR16-EFI06 Lapteacru, I., "Convergence of bank competition in Central and Eastern European countries : Does ownership matter ?"

CR16-EFI05 Lapteacru, I., "On the consistency of the Z-score to measure the bank risk"

CR16-EFI04 Lapteacru, I., "Income and funding structures, banking regulation and bank risk-taking : The role of ownership in Central and Eastern European banks"

CR16-EFI03 Humblot, T., "Distance et accès au crédit sous Bâle III"

CR16-EFI02 Berthoumieu, J. and V. Lamani, "Vertical Differentiation, Uncertainty, Product R&D and Policy Instruments in a North-South Duopoly"

CR16-EFI01 Raffestin, L., "Foreign exchange investment rules and endogenous currency crashes"

CR15-EFI05 Berthoumieu, J., "Technology Diffusion via Patent Collaborations : The Case of European Integration"

CR15-EFI04 Bouet, A. and A-G. Vaubourg, "Financial Constraints and International Trade with Endogenous Mode of Competition"

CR15-EFI03 Lahet, D. and A-G. Vaubourg, "Banks' shareholding in multilateral trading facilities : A two-sided market perspective"

CR15-EFI02 Berthoumieu, J., "Policy Instruments, Patents and International Technology Diffusion in a North-South Duopoly"

CR15-EFI01 Dupuy, L., "International trade and structural change : a dynamic model of weak sustainability"