D'autres politiques économiques sont possibles
Le blog de Les économistes atterrés
18/11/2017
Matthieu Montalban, Université de Bordeaux

Bitcoin, crypto-monnaies et blockchain : mirage ou miracle ? (1/2)

Les pratiques liées au Bitcoin et à la blockchain (ou technologie de la chaîne de blocs) commencent à se répandre. Pour certains ce n'est qu'un gadget, ou encore une arnaque, pour d'autres c'est une vraie révolution qui pourrait durablement transformer le système monétaire et financier, voire le système économique. On se propose dans cet article de faire un point sur les origines, potentialités et risques associés aux crypto-monnaies et à la blockchain. Cet article se focalisera sur les crypto-monnaies comme Bitcoin. Après un retour sur leurs fondements philosophiques, nous verrons quelles sont les raisons et les avantages expliquant le développement du Bitcoin et des autres crypto-monnaies. Nous aborderons ensuite leurs limites et les critiques qui peuvent en être faites.

Les fondements philosophiques des crypto-monnaies

Le Bitcoin est le produit d'un projet politique et la blockchain est la technologie qui a rendu possible ce projet. Depuis au moins la fin des années 1970 et l'article de Friedrich Hayek sur le projet de dénationalisation de la monnaie[1], une des obsessions des libertariens (autre nom des anarcho-capitalistes ou ultra-libéraux) est de libérer la création monétaire de l'influence des banques centrales et des Etats. Celle-ci serait selon eux responsable de l'inflation et des prises de risques excessives des banques. Plusieurs projets ont germé dans les esprits des ultra-libéraux inspirés de l'école autrichienne, comme le free banking (les banques privées se font concurrence pour émettre leur propre monnaie sans banque centrale pour jouer les prêteurs en dernier ressort), le retour à l'or, le 100 % monnaie (interdire aux banques de prêter au-delà de leurs dépôts, système qu'on appelle chez les ultra-libéraux le système des réserves fractionnaires).

Inventé au lendemain de la crise de 2008, censé remédier aux défauts du régime monétaire et financier, le Bitcoin se rapproche de cet idéal anarcho-capitaliste d'une "monnaie libre" visant à saper le monopole d'émission monétaire par les banques centrales et privées. Créé par un ou des codeurs anonymes surnommé(s) Satoshi Nakamoto (les spéculations vont bon train pour trouver de qui il s'agit), le Bitcoin est une crypto-monnaie, c'est-à-dire une monnaie numérique, émise de façon décentralisée sans contrôle étatique, mais contrôlée par un algorithme qui permet d'assurer la sécurité des transactions et l'absence de manipulation ou de "faux monnayage". En somme, le rêve de la monnaie anarcho-capitaliste version Silicon Valley. Depuis l'invention de Bitcoin, bien d'autres

[1] https://iea.org.uk/publications/research/denationalisation-of-money

crypto-monnaies et *blockchains* ont été inventées (comme *Ethereum, Litecoin, Peercoin*, etc.). Certains libertaires de gauche semblent aussi très excités par cette monnaie, qui s'attaque aux banques et à l'autorité des Etats.

Aux sources du développement de la *blockchain, Bitcoin* et des autres crypto-monnaies

Une monnaie pour s'institutionnaliser a besoin de confiance : il faut que ceux qui l'utilisent croient qu'elle sera acceptée comme moyen de paiement et que sa valeur soit garantie d'une façon ou d'une autre.

On donne en général trois sources à la confiance dans la monnaie :

❒ une confiance méthodique, liée à l'usage rationnel du symbole (je sais que les autres l'utilisent, donc je l'utilise),

❒ la confiance hiérarchique liée à l'existence d'un tiers de confiance (je sais que le système de paiement est garanti par la banque centrale et le réseau des banques privées)

❒ et la confiance éthique (l'émission monétaire se fait selon des règles légitimées)[2].

On a pendant longtemps pensé que, pour assurer la confiance dans la monnaie, la confiance hiérarchique et l'Etat étaient nécessaires. Le *Bitcoin* tente de se passer de cet intermédiaire centralisé, que les libertariens et néolibéraux ont toujours critiqué du fait de la possible manipulation inflationniste de la quantité de monnaie pour assurer le financement de l'Etat.

Les crypto-monnaies s'appuient pour cela sur une technique de cryptage et des vérifications automatisées mobilisant la puissance de calcul de tous les ordinateurs participant au réseau : la *blockchain*. C'est une sorte de grande base de données décentralisée faisant office de livre de compte, un registre distribué, transparent et sécurisé de toutes les transactions depuis le démarrage du système, qui automatise la vérification des transactions en mobilisant la puissance de calcul de tous les ordinateurs du réseau, sans contrôle centralisé et sur la base d'un consensus. Elle peut être assimilée à une sorte de système décentralisé d'organisation et de contrôle du transfert de propriété.

Elle s'affranchit donc du tiers de confiance (la confiance hiérarchique). Chaque ordinateur réalise pour chaque bloc de transactions des vérifications coûteuses en calcul et en énergie (*Proof of work* ou preuve de travail dans le cas du *Bitcoin*) permettant de maintenir la fiabilité y compris face à des tentatives malveillantes de pirates diffusant des informations erronées. Ce système est réputé quasi inviolable par les spécialistes de cryptographie.

La puissance de calcul de nombreux ordinateur étant mobilisée, il faut inciter de plus en plus d'utilisateurs à participer au réseau et à assurer la diffusion du *Bitcoin*. L'astuce vient ici de ce que le propriétaire de chaque ordinateur qui, en mettant sa machine à disposition, parvient à résoudre les problèmes dits de minage (et les ordinateurs sont des *"mineurs"*), obtient des *Bitcoins* en rémunération. Au fond, les *Bitcoins* sont émis en contrepartie du coût en électricité et en puissance de calcul de la mise à disposition de l'ordinateur. Comme l'algorithme du *Bitcoin* est fait pour que son émission soit limitée, sa valeur par rapport aux monnaies souveraines doit avoir tendance à augmenter, incitant de plus en plus de mineurs à miner et assurant ainsi la diffusion de la crypto-

[2] Alary et al. (2016), Théories françaises de la monnaie, PUF, Paris.

monnaie. Celle-ci peut ensuite être convertie dans des sortes de plateformes faisant office de bureaux de change en monnaie souveraine ou dans une autre crypto-monnaie.

Le Bitcoin se passe d'intermédiaires bancaires et permet donc de réaliser des économies sur les coûts de transaction liés à l'intermédiation bancaire (commissions, frais de tenue de compte, etc.). Le transfert des Bitcoins ou son échange dans une devise souveraine est (ou plutôt était, c'est ce que nous verrons après) assez aisé, ce qui rend possible des paiements sur n'importe quel point de la planète en un temps record, à condition bien entendu que la personne avec qui on les échange les accepte. Par ailleurs, ce transfert n'est possible que si préalablement les Bitcoins existent sur un compte, il n'y a pas ici de système de réserves fractionnaires (les banques ne peuvent créer de monnaie par crédit), ce qui dans la vision ultra-libérale est une vertu protégeant des risques inflationnistes et du faux-monnayage dont ils accusent les banques.

Ainsi, le Bitcoin peut être considéré comme une sorte d'or numérique, et le régime monétaire qu'il instituerait s'il venait à se généraliser (nous discuterons après de la faisabilité de ce scénario) ressemblerait à un régime d'étalon-or (le terme de minage étant utilisé à dessein).

Le Bitcoin, un produit spéculatif

Une critique majeure consiste à dire que le Bitcoin est un pur produit spéculatif. Il n'est en effet guère discutable qu'il soit un actif spéculatif : la plupart des personnes investissant dans ces crypto-monnaies le font pour obtenir un rendement élevé. De fait, le Bitcoin s'apprécie au fil du temps et au vu de la croissance de son cours, on peut légitiment se demander s'il ne s'agit pas d'une bulle : https://www.coindesk.com/price/

Est-ce une bulle ? En l'occurrence, l'algorithme du Bitcoin fait que la création monétaire par Bitcoin est limitée à terme à 21 millions d'unités. Vous avez bien lu : il n'y aura en tout et pour tout que 21 millions de Bitcoins qui seront créés *in fine*, sachant que pour le moment 12 millions l'ont été. C'est donc une monnaie rare par définition et c'est ce qui explique une partie de son succès, à la fois comme valeur refuge et parce qu'il peut inspirer une forme de confiance éthique, puisque la création monétaire ne peut être manipulée. Le Bitcoin est perçu comme une sorte de valeur refuge et les acteurs anticipent de façon mimétique que son cours va monter parce que la taille du réseau et sa diffusion augmentent tandis que son volume est limité.

Cette pseudo-monnaie n'est donc pas stable puisqu'elle s'apprécie et est soumise à la spéculation. Si une telle monnaie et un tel régime monétaire s'institutionnalisaient et se généralisaient, on observerait des mécanismes déflationnistes, dont les effets seraient potentiellement dépressifs sur l'activité. En effet, la déflation renchérit les dettes, ce qui a pour effet d'étrangler les débiteurs (entreprises, ménages ou Etats), à savoir les agents ayant la plus forte propension à consommer. On pourrait certes arguer que la baisse des prix augmente le pouvoir d'achat des encaisses monétaires et donc la consommation, mais cet effet dit d'encaisses réelles est plutôt faible en général. Qui plus est, si les salaires sont plus rigides que les prix (ce qu'ils sont en règle générale), la déflation diminue les profits et réduit l'incitation à investir. Actuellement, tant que nous sommes en régime de monnaie fiduciaire souveraine, comme le Bitcoin ne sert pas à fixer des prix et des salaires, cet effet déflationniste ne peut guère jouer et l'appréciation de cet actif est essentiellement spéculative.

Les moyens de paiement ne sont pas créés en fonction des besoins en liquidité liés à la circulation monétaire, mais en fonction de l'activité de minage, dont le rendement est décroissant au cours du temps (la probabilité qu'un ordinateur parvienne à obtenir un Bitcoin décroît). Si tout le monde pouvait

prêter ses Bitcoins pour financer telle ou telle activité, ces dettes et créances ne pourraient ni créer de monnaie ni circuler comme de la monnaie via la blockchain Bitcoin. On se rapprocherait de l'idéal d'un Maurice Allais ou de certains ultra-libéraux autrichiens, qui voulaient séparer les fonctions monétaires et de prêt en interdisant les réserves fractionnaires.

Cependant, le Bitcoin n'interdit pas le système de réserves fractionnaires : si une banque crée des comptes en Bitcoin, rien ne lui interdit de mettre en circulation, via le crédit, des moyens de paiement (des chèques par exemple) au-delà de ses réserves en Bitcoin. Mais il faudrait pour cela que les banques offrent un service plus intéressant, du fait de la transparence du registre et parce que les agents dans le réseau peuvent avoir leurs propres compte/portefeuilles ("wallet") sans recourir aux banques. D'autant que l'objectif du Bitcoin est de se passer des banques en proposant un service avec de moindres coûts de transaction. Qui plus est, dans un système complètement "bitcoinisé", les banques auraient toujours cette limitation quantitative des réserves en Bitcoin, comme l'or pouvait en partie limiter l'expansion du crédit dans l'étalon-or. Il y a donc fort à parier que le régime serait déflationniste et néfaste pour le niveau d'activité du fait de sa faible élasticité. Dans un tel scénario, il entraînerait une perte totale de l'outil de la politique monétaire.

Une absence de régulation ouvrant la voie à des activités illégales

Le Bitcoin est-il réellement une monnaie ou est-ce une fraude à la fausse monnaie comme le prétendent certains, notamment Jamie Dimon, le directeur de JP Morgan Chase ? Rappelons qu'une monnaie n'est monnaie que parce qu'elle est conventionnellement considérée comme telle. Cela veut dire que si le Bitcoin est un jour accepté comme tel, c'est-à-dire s'il suscite assez de confiance pour permettre des achats, il sera une monnaie. Parmi les éléments qui peuvent alimenter la méfiance, il y a eu plusieurs cas d'arnaques aux crypto-monnaies, qui peuvent jeter la suspicion pour le grand public et qui montrent qu'une technique, même inviolable, peut ne pas suffire à instituer la confiance. Il y a eu également des cas de chaînes Ponzi (montages frauduleux) sur le Bitcoin.

Les opérations dites d'Initial Coin Offerings (ICO), c'est-à-dire des émissions de token à taux préférentiel à destination des financeurs par et pour le financement des start-ups de minage contre monnaie souveraine, ne sont pas régulées et se développent pour contourner le financement classique en actions avec ses règlementations. Dans les ICO, des tokens de crypto-monnaies sont émis qui donnent à terme non pas un droit à dividende et des droits de vote, mais un droit d'acheter un des produits ou service que l'entreprise fournira après, ou de revendre avec plus-value les tokens de crypto-monnaies obtenus si le cours a augmenté. Mais si la crypto-monnaie fait un flop, les investisseurs perdent tout. L'Autorité des Marchés Financiers s'inquiète de ces opérations et réfléchit à des mesures pour les réguler. Il y a dans ces ICOs de nombreux cas d'arnaques qui pourraient fragiliser la confiance dans cette pseudo-monnaie. Par ailleurs, les crypto-monnaies sont souvent utilisées dans le blanchiment d'activités illégales. Bref, l'absence de régulation encourage des comportements plus que litigieux. L'innovation financière et monétaire est souvent un moyen de contourner les régulations pour faire des affaires douteuses, le Bitcoin n'échappe pas à la règle.

Une monnaie incomplète

Par ailleurs, une monnaie est complète si elle réunit les fonctions d'unité de compte, de moyen de paiement et règlement, et de réserve de valeur. Pour le moment, le Bitcoin sert essentiellement comme réserve de valeur et comme moyen de paiement pour un certain nombre de produits sur

Internet, ou depuis quelques temps dans quelques magasins physiques au Japon et en Allemagne. Ces sites ou commerces acceptent le Bitcoin comme moyen de paiement à la fois parce que l'algorithme est sécurisé et parce qu'ils anticipent qu'ils pourront changer les Bitcoins contre de la monnaie souveraine, éventuellement avec une plus-value étant donnée la croissance actuelle du cours.

Mais le Bitcoin n'a pas encore réellement acquis de fonction d'unité de compte, sauf dans les échanges entre crypto-monnaies où il est "la" monnaie de référence. Il ne peut donc pas être considéré comme une monnaie complète. Le principal facteur qui peut ralentir l'usage de ces crypto-monnaies vient des Etats et banques centrales qui décident souverainement de l'unité de compte sur leur territoire et obligent à payer les impôts en monnaie souveraine. Cette obligation assure que la monnaie nationale soit utilisée à la fois comme unité de compte et moyen de paiement. Par ailleurs, des Etats peuvent très bien décider d'interdire le Bitcoin et autres crypto-monnaies libres pour créer leur propre crypto-monnaie souveraine, sur des règles d'émissions différentes pour ce qui est de l'émission monétaire : c'est ce à quoi réfléchissent la Russie, l'Estonie et le Viêt-Nam.

Certains des prétendus avantages du Bitcoin sont en train de disparaître. D'abord, à mesure que le nombre de transactions augmente, il faut de plus en plus de temps pour qu'une transaction soit validée, parfois plusieurs dizaines de minutes, ce qui est loin d'être pratique. Comme en plus il n'y a pas l'équivalent de moyens de paiement de type carte bleue ou billets, il est peu probable pour le moment que ce type de monnaie soit utilisé dans les transactions quotidiennes au supermarché ou au café. Or transformer les Bitcoins en dollars génère de plus en plus de coûts de transactions (ils atteignaient 5,5 $ en juin dernier et la tendance est à la hausse par transaction), réduisant l'intérêt de la crypto-monnaie pour les transactions de petite valeur. Tout cela s'explique par le coût en calcul et en énergie du maintien de la blockchain Bitcoin.

Un régime insoutenable

Etant donné la probabilité décroissante de parvenir à miner, il faut faire tourner les ordinateurs de plus en plus longtemps pour obtenir du Bitcoin ou alors mobiliser de plus en plus d'ordinateurs. Il se trouve que le Bitcoin est un vrai gouffre énergétique, car le protocole de vérification (Proof of work) mobilise énormément d'énergie et de puissance de calcul, et cela d'autant plus que le nombre des transactions augmente.

On estime actuellement, alors que le Bitcoin est relativement peu diffusé, que la consommation d'électricité pour faire fonctionner cette blockchain représente l'équivalent de la consommation de l'Irlande. Et cela va croissant, donc ça n'est aucunement soutenable sur le plan énergétique. De façon complètement délirante, certains Russes et Chinois font tourner des centaines d'ordinateurs en continu pour miner des Bitcoins (on parle de fermes de minage). Comme le rendement est de plus en plus faible, il faut toujours plus de machines dans les fermes de minage pour parvenir à résoudre les problèmes de calcul… On a vu allocation des ressources plus intelligente pour la collectivité. Ce qu'il y a de cocasse d'ailleurs, c'est que le Bitcoin a été créé pour limiter le soi-disant faux-monnayage étatique, mais cela ne semble pas gêner ses promoteurs que des gens se contentent pour gagner leur vie (certains sont devenus millionnaires) de faire tourner des ordinateurs à longueur de journée pour résoudre des problèmes de généraux byzantins en consommant de l'énergie qui serait certainement mieux utilisée ailleurs ; activité qui ressemble quand même beaucoup au "vrai" faux-monnayage.

Quoiqu'il en soit, il est probable qu'à terme le rendement du minage diminuant tandis que les coûts énergétiques et de transaction augmentent, l'intérêt de miner du Bitcoin se réduise, voire disparaisse.

Qui aurait alors intérêt à laisser son ordinateur tourner en permanence sans espoir de minage ? En l'occurrence, d'autres crypto-monnaies comme Litecoin ou Ethereum ont été créées avec des protocoles moins coûteux sur le plan énergétique, mais il reste à prouver que tout cela soit soutenable.

Pour être honnête, il faudrait comparer le coût des blockchains des crypto-monnaies avec celui des systèmes de paiement existants. Celui-ci n'est pas nul, contrairement à ce qu'on peut entendre parfois : il faut des machines à cash, des terminaux de paiement, imprimer des billets, l'infrastructure informatique, etc. Mais on sent bien que les avantages tant vantés du Bitcoin sont à réexaminer.

Qui plus est, comme les coûts de transaction ont augmenté, pour pouvoir utiliser des Bitcoins au quotidien, une solution pourrait être que des banques émettent des moyens de paiement "physiques" (des chèques) en contrepartie de Bitcoins, faisant perdre sa philosophie originelle puisque la bancarisation reviendrait et avec elle, la possibilité du système de réserves fractionnaires. Les banques n'ont pas encore dit leur dernier mot. Je ne doute pas cependant que la valeur du Bitcoin va continuer à augmenter encore, tant que le coût marginal du minage est inférieur à sa valeur (la comparaison valeur / coût de production détermine la production ; le rendement espéré la demande) et que les Etats ne prennent pas des dispositions pour les interdire ou en réglementer la diffusion.Cela génèrera encore pour un moment un gaspillage absurde d'énergie et de ressources.

L'improbable "disruption" du secteur bancaire et financier par les crypto-monnaies

La dernière raison à même de freiner le développement des crypto-monnaies est la réaction de l'oligopole bancaire, qui sent bien qu'elle peut malgré tout être menacé par les crypto-monnaies, la blockchain et plus généralement tout le secteur de la Fintech. Mais avouons que parvenir à "disrupter" le secteur bancaire et financier pour réduire sa capacité de nuisance et notre dépendance pourrait ne pas complètement nous déplaire.

Au final, même si le Bitcoin venait à s'imposer comme moyen de paiement pour le commerce électronique, il y a peu de chances qu'il parvienne à "disrupter" les monnaies souveraines. Il poserait, s'il était généralisé en substitut des monnaies souveraines, de graves problèmes de déflation, en raison de la rigidité de son processus de création monétaire et d'une création monétaire qui ne s'ajuste pas aux besoins en liquidités. Si le Bitcoin comme les crypto-monnaies ne sont que des actifs spéculatifs en plus, au mieux leur intérêt est limité, au pire ils sont néfastes. Le scénario le plus probable à moyen terme est celui d'une cohabitation entre les monnaies souveraines et les crypto-monnaies. Ces dernières seraient utilisées dans certaines transactions et acceptées par quelques entreprises et commerces, tandis que les monnaies souveraines conserveraient leur rôle pivot du fait de leur cours légal et de leur rôle dans le paiement de l'impôt.

Les crypto-monnaies présentent d'importantes limites, mais la technique sous-jacente, la blockchain, a de nombres potentialités d'applications. Nous les examinerons dans un prochain article.