Bitcoin : quelle crédibilité ?

par
Yorick de Mombynes

Yorick de Mombynes est conseiller référendaire à la Cour des comptes. Titulaire d'une licence en philosophie, diplômé de l'ESCP, de l'IEP de Paris et ancien élève de l'ENA il a également été conseiller de François Fillon à Matignon et a travaillé six ans au sein du groupe Total. Il a publié deux études sur le bitcoin à l'Institut Sapiens.

Bitcoin est un dispositif de stockage et de transfert de valeur sur internet, sans intermédiaire, incensurable, rapide, programmable, peu coûteux et protégeant bien la vie privée.

Les unités numériques et comptables circulant sur son réseau sont des « bitcoins », créés automatiquement par le système pour rémunérer les acteurs – appelés « mineurs » – qui engagent des ressources pour le sécuriser. Le nombre de ces unités émises toutes les dix minutes est divisé par deux tous les quatre ans, ce qui fera tendre leur quantité totale vers 21 millions, en 2140 (plus de 19 millions de bitcoin ont déjà été émis depuis 2009).

Pour la plus grande partie de la population, le bitcoin reste un sujet peu crédible : incompréhensible, suspect, sulfureux. Pourtant, cet étrange animal est toujours vivant et reste même le plus valorisé malgré la concurrence de milliers de cryptomonnaies. Il doit donc bien avoir une forme de crédibilité.

Cette crédibilité a trois facettes principales : technique, monétaire et sociale.

1. Une crédibilité technique massive

La crédibilité technique du système Bitcoin a trois composantes.

Premièrement, elle concerne sa capacité à inspirer confiance sur l'absence de double dépense. La prouesse de Bitcoin, rendre possible du cash numérique, est réalisée non par une prétendue « technologie blockchain » mais par une intégration novatrice de quatre technologies existantes : le pair-à-pair, le chiffrement asymétrique, le registre décentralisé (blockchain), et la preuve de travail. La crédibilité de l'absence de double dépense est aujourd'hui massive. Le bitcoin est ainsi le seul objet numérique non duplicable de l'histoire de l'informatique.

Deuxièmement, cette crédibilité concerne le fait qu'aucun acteur, notamment étatique, ne pourra prendre le contrôle du dispositif. Il est de plus en plus improbable que les États parviennent à contrôler voire éliminer Bitcoin, même s'ils se coalisaient. Ils peuvent tout au plus

freiner son essor de multiples manières, notamment par la réglementation, la fiscalité et la propagande. C'est d'ailleurs ce qu'ils font en ce moment. Mais ils sont probablement en train de se rendre compte que Bitcoin est désormais très difficile à supprimer, contrairement à la plupart des autres cryptomonnaies (dont celle de Facebook, qu'ils ont évincée sans trop d'efforts).

En effet, Bitcoin n'a jamais été piraté depuis sa création, notamment grâce à trois particularités :

— des fonctions cryptographiques robustes (dont certaines devront sans doute être adaptées à l'informatique quantique le moment venu) ;
— un niveau élevé de décentralisation des ordinateurs qui stockent et actualisent la blockchain : plusieurs dizaines de milliers de « nœuds » dans le monde ;
— une puissance de calcul globale du minage considérable, représentant la plus forte capacité de calcul présente sur Terre. Un mécanisme interne original permet d'adapter automatiquement toutes les deux semaines la difficulté du minage à la puissance de calcul présente, pour éviter une accélération du rythme de production de bitcoins, et pour maintenir une rentabilité attractive des mineurs. Au passage, ce mécanisme enclenche un étonnant cercle vertueux : toutes choses égales par ailleurs, une augmentation du prix du bitcoin incite les mineurs à déployer plus de puissance de calcul, ce qui entraîne une augmentation de la difficulté des opérations qu'ils doivent réaliser, ce qui renforce la sécurité du dispositif, ce qui rend le bitcoin plus attractif, ce qui fait monter son prix, etc.

Enfin, la crédibilité technique de Bitcoin repose sur sa capacité à s'améliorer d'un point de vue technologique. Le passage à l'échelle est en cours grâce au Lightning Network, et la programmabilité et les *smart contracts* sont à l'étude avec, par exemple, le protocole RGB.

2. Une crédibilité monétaire en construction

La crédibilité monétaire du bitcoin est la confiance que ce dernier inspire quant à sa capacité à devenir une véritable monnaie, et éventuellement une bonne monnaie.

Une vraie monnaie ?

Aujourd'hui, le bitcoin n'est une monnaie ni au sens légal, ni au sens économique : la loi ne lui donne pas ce titre (sauf au Salvador), et il n'est pas un moyen d'échange communément accepté.

A première vue, on peut penser que le bitcoin sert surtout à la spéculation et à l'épargne, et qu'il n'est que très marginalement utilisé comme unité de compte. Pourtant, très progressivement, de plus en plus de gens pensent qu'il deviendra une vraie monnaie, et de plus en plus l'utilisent comme telle, notamment pour les trois raisons suivantes.

Premièrement, le bitcoin possède les qualités objectives pour lesquelles certaines marchandises ont, dans l'histoire, été durablement utilisées comme monnaies : homogénéité, fongibilité, portabilité, divisibilité, rareté relative, coût de production élevé.

Deuxièmement, le bitcoin a un usage non monétaire. Or, pour être une véritable monnaie sans être imposée par la coercition de la loi, une chose doit d'abord avoir eu un usage non monétaire, d'après le théorème de régression de Ludwig von Mises. Au début de son histoire, il a été utilisé comme objet de curiosité pour les informaticiens, comme objet d'intérêt idéologique pour certains, et comme objet de collection pour d'autres.

Aujourd'hui encore, il a un double usage non monétaire : d'une part, en tant que plateforme d'horodatage décentralisé efficient, avec des applications commerciales, juridiques et industrielles ; d'autre part, en tant qu'infrastructure de paiement novatrice, capable de rivaliser avec les infrastructures traditionnelles. On peut d'ailleurs indirectement y transférer de la monnaie fiat, avec des performances techniques et

économiques visiblement supérieures, comme le montre l'entreprise Strike.

Troisièmement, il n'y aura jamais plus de 21 millions de bitcoins. Ce cap d'émission fait du bitcoin une valeur refuge appréciable contre l'inflation monétaire créée par les politiques monétaires expansionnistes, notamment dans les pays en développement, mais aussi, de plus en plus, dans les pays développés. La probabilité pour que ce régime d'émission soit modifié est pratiquement nulle car il repose sur un protocole *open source* : aucune autorité centrale ne peut en prendre le contrôle, et ses utilisateurs n'accepteront jamais une modification de paramètre, pour ne pas risquer d'anéantir la proposition de valeur de Bitcoin.

Une bonne monnaie ?

Dans un sens, le cap d'émission du bitcoin et la hausse rapide de son ratio stock-to-flow en font une véritable « sound money », une « hard money » comparable à l'or. Mais sa crédibilité monétaire doit surmonter deux défis importants.

D'une part, sa volatilité. C'est un inconvénient réel mais logique et sans doute transitoire, dû au fait que la capitalisation de marché du bitcoin est faible par rapport aux marchés financiers mondiaux, ce qui rend son cours plus vulnérable à des chocs de demande, son rythme de production n'étant pas ajustable. Cet inconvénient devrait diminuer avec l'augmentation de la valorisation du bitcoin. Et si ce dernier devait un jour remplacer les monnaies fiat, la volatilité de son prix exprimé par rapport aux biens de consommation n'aurait *a priori* pas de raison d'être très élevée.

D'autre part, la rigidité de son régime d'émission. Ce dernier, qui est *désinflationniste*, puisque son rythme d'émission est décroissant, rendrait possible une économie *déflationniste*. La déflation des prix n'est pas un problème en soi (contrairement à une opinion très répandue), d'autant moins que l'unité du bitcoin est très divisible, ce qui permettrait d'ajuster les prix. Mais la crainte de certains économistes –

y compris favorables à Bitcoin – est que cette déflation aille au-delà de celle qui serait naturellement entraînée par la hausse de la productivité globale de l'économie, ce qui ferait du bitcoin une mauvaise monnaie. Seul l'avenir permettra de voir si cet inconvénient peut être surmonté.

3. Une crédibilité sociale contrastée

La crédibilité sociale du bitcoin concerne notamment la vie privée, le champ politique, l'écologie et la criminalité.

En matière de vie privée et de souveraineté individuelle, Bitcoin est un progrès radical, comme le comprennent très bien les habitants des pays autoritaires. Pour eux, Bitcoin est un rempart contre la corruption, la surveillance, l'arbitraire politique. Dans les pays développés, nous le comprendrons aussi rapidement avec l'émergence des futures monnaies numériques de banque centrale (MNBC), outils potentiellement totalitaires dont nos dirigeants semblent puiser l'inspiration en Chine.

Bitcoin permet de dépolitiser la monnaie, de séparer la monnaie et l'État, rupture historique qui interromprait l'expansion déraisonnable des activités de la puissance publique et de son pouvoir sur les individus et la société (et empêcherait aussi les politiques monétaires déstabilisatrices pour l'économie).

Le débat sur le coût environnemental du bitcoin est biaisé, non scientifique et largement mensonger. L'utilisation d'électricité par Bitcoin est utile en soi puisque c'est elle qui rend possible ce système de monnaie décentralisée et incensurable. Et Bitcoin est un atout pour la transition énergétique puisqu'il incite économiquement les mineurs à utiliser des énergies renouvelables, souvent les moins chères dans des zones géographiques où la demande locale est faible. Les énergies renouvelables représentent environ 60% du mix énergétique de Bitcoin actuellement et cette proportion augmente. Enfin, son passage à l'échelle est en train de se faire sans consommation énergétique additionnelle, réfutant les prévisions alarmistes et souvent ridicules de ses détracteurs.

Enfin, s'agissant de la criminalité, Bitcoin rend les transactions suspectes traçables par la police, ce qui explique que les plus grands trafics se font toujours essentiellement par l'intermédiaire du système bancaire et en monnaies officielles.

Conclusion

Bitcoin est antifragile au sens de Nassim Taleb. Il bénéficie de « l'effet Lindy » : son espérance de vie augmente avec sa durée de vie. Plus il est attaqué d'un point de vue technique et politique, plus il y trouve des occasions de se renforcer et de prouver sa robustesse et sa proposition de valeur : en conséquence, il est progressivement davantage pris au sérieux par ceux qui l'ont d'abord ignoré ou critiqué. Plus le temps passe, plus sa crédibilité se renforce.

Ce processus étant cumulatif et bénéficiant de forts effets de réseau, il ne serait pas étonnant qu'il connaisse une accélération radicale dans les années qui viennent.