> À l'heure où cette technologie en évolution rapide commence à être exploitée pour des applications de plus en plus nombreuses et variées, la confusion règne dans de nombreux esprits. Comme le bitcoin est actuellement la forme de monnaie numérique la plus connue (en bien ou en mal, les avis sont partagés), il est utile de revenir un peu en arrière pour explorer ses origines et ses faiblesses, et comprendre en quoi elle diffère des versions plus prometteuses qui sont maintenant à l'étude.

La monnaie bitcoin a été conçue comme un système de paiement numérique pair à pair qui fonctionne sans autorité centrale. N'importe qui peut y adhérer, ce qui est à la fois une force et une faiblesse. Les utilisateurs effectuent entre eux des transactions financières directes (par exemple l'achat d'un bien), sans l'aide d'intermédiaires. Ces transactions sont inscrites dans un registre à blockchain distribué publiquement, que tous les participants peuvent (théoriquement) voir. Depuis la création du bitcoin en 2009, son cours a augmenté de plusieurs ordres de grandeur, ce qui en fait la coqueluche des spéculateurs.

Les promesses du système des bitcoins sont grandes. Ses partisans – essentiellement des idéalistes et libertaires férus de technologie, mais aussi certains criminels – s'attendent à ce que le bitcoin devienne une devise mondiale qui finira par supplanter les devises nationales, facilement manipulables selon eux. Certains enthousiastes voient même dans le bitcoin une version numérique de l'or, oubliant peut-être que l'or tient sa stabilité à la fois de ses attributs physiques et de ses milliards de détenteurs, et que dans le monde numérique les bonnes techniques sont régulièrement dépassées par de meilleures encore.

Le bitcoin n'est d'ailleurs pas la première monnaie virtuelle, et ce ne sera très probablement pas la dernière non plus à jouer dans la cour des grands. Elle souffre par ailleurs de sérieuses contraintes logistiques.

LE BITCOIN N'EST PAS LA PANACÉE

Par exemple, le nombre de transactions qui peuvent être traitées à chaque seconde tourne autour de 7, à comparer avec les 2000 que traite en moyenne le système Visa de cartes de paiement.

De plus, c'est un gouffre à énergie : le minage (le processus par lequel les membres du réseau de cryptomonnaie se font la compétition pour ajouter de nouveaux blocs de transactions à la blockchain, et ainsi gagner des bitcoins) consomme une énorme quantité d'électricité. Dans les pays où l'électricité coûte cher, les mineurs font rapidement faillite s'ils ne peuvent honorer les factures d'électricité des systèmes informatiques. On ne connaît pas

© Borja Bonaque

les chiffres exacts, mais on estime que le système des bitcoins consomme autant d'électricité qu'eBay, Facebook et Google réunis.

Le bitcoin a également été mis en place pour que l'autorité soit répartie entre de nombreux mineurs ; or en se rassemblant pour former de gigantesques pools, un petit nombre de groupes sont devenus suffisamment puissants pour contrôler le système. Peut-on encore parler de pair à pair ?

L'utilisation du bitcoin est de plus limitée. Le terme « monnaie » peut être défini par ses trois types d'utilisation : pour les transactions, comme réserve de valeur et en tant qu'unité de compte. Comme le cours du bitcoin par rapport aux monnaies légales, reconnues par les États, est extrêmement instable, il est difficile à utiliser au quotidien. Le bitcoin et l'ether, une autre grande cryptomonnaie, ne sont pas couverts par des biens réels ni même par des engagements gouvernementaux. Par conséquent, ils sont purement spéculatifs. En termes familiers, cela signifie que ces monnaies numériques ne sont pas de l'argent « véritable » : ce qui n'a pas de valeur ne peut avoir de prix. Certains enthousiastes du bitcoin présentent cette absence de valeur comme un avantage et affirment que, dans le futur, tout l'argent sera du même type que le bitcoin. Cela est hautement improbable, pour des raisons à la fois techniques et politiques.

Cependant, en tant que première monnaie virtuelle décentralisée prospère, le bitcoin

À PROPOS DES AUTEURS

ALEXANDER LIPTON
a fondé une jeune entreprise, StrongHold Labs. Il a auparavant occupé plusieurs hautes fonctions à la Bank of America, et des postes de professeur invité à l'université d'Oxford et à l'Imperial College de Londres.

ALEX « SANDY » PENTLAND
**dirige le laboratoire Human Dynamics du MIT, et est notamment membre de l'Académie d'ingénierie des États-Unis.
Son dernier ouvrage en date est *Social Physics* (Penguin Books, 2015).**

représente une percée impressionnante. La technologie sous-jacente et la philosophie d'un système financier pair à pair non régulé par une autorité centrale sont innovantes.

Le bitcoin n'est bien sûr que l'une des applications des registres distribués fondés sur des chaînes de blocs. La blockchain, après tout, est une technique, et non une idéologie particulière : on ne devrait pas la confondre avec la philosophie qui anime le système du bitcoin ou avec les motivations de l'une quelconque de ses applications actuelles ou futures. Les blockchains ont certes le potentiel de résoudre certains des problèmes existants de notre système financier, mais on pourrait tout autant les utiliser pour les exacerber. Et quand on considère qu'un élément clé de la puissance est le contrôle de la monnaie (à la fois la masse monétaire existante et la future création de monnaie), on peut déjà avoir un petit aperçu de la boîte de Pandore de dangers moraux que cette technologie a ouverte.

Prenons les banques centrales des principales monnaies de réserve, telles que la Réserve fédérale des États-Unis et la Banque d'Angleterre. La confiance qu'on leur accorde est souvent liée à leur taille (plus c'est grand, plus c'est fiable), mais ces acteurs ont prouvé qu'un tel raisonnement est erroné. Ces banques centrales ont maintes fois pris le parti d'appauvrir les petites gens en diluant leurs obligations financières par le biais de l'inflation, la suppression des taux d'intérêts et autres politiques. Elles ont récemment testé des taux d'intérêt négatifs et envisagé des moyens de se débarrasser de l'argent liquide.

Plus alarmant encore, certaines banques centrales réfléchissent à la possibilité de rendre numériques toutes leurs monnaies et de consigner les achats directement dans un registre. Cela pourrait court-circuiter la contribution des banques privées et conférer aux gouvernements le contrôle absolu de l'économie. Cela signifie également que le gouvernement disposerait d'une trace de tout ce que vous achetez, y compris ce que vous achetez aujourd'hui en espèces précisément pour éviter de laisser une trace écrite.

Cette possibilité semble de moins en moins relever de la science-fiction, et des pays tels que la Chine, le Royaume-Uni, Singapour et la Suède ont annoncé des projets d'étude et éventuellement d'implémentation d'une telle stratégie. La conclusion de tout cela est que la technologie elle-même a beau être décentralisée par conception, on peut l'utiliser pour créer des systèmes à contrôle centralisé.

Il est clair que l'invention des chaînes de blocs et des registres distribués n'éradiquera pas les problèmes de krachs financiers ou d'inflation malsaine, du moins pas à court terme. Mais elle rend possible la création de substituts légitimes aux grands et puissants acteurs. La technologie permet désormais de former des systèmes de monnaie globale spécialisés qui, auparavant, n'auraient pas joui d'une ampleur, d'une confiance ou d'une stabilité politique suffisantes pour se poser en concurrents. C'est pourquoi une prochaine étape naturelle serait que les petits acteurs, tels que des économies émergentes ou un grand nombre de citoyens, se groupent pour former des substituts aux banques centrales.

LE TRADECOIN, POUR UN SYSTÈME FINANCIER PLUS STABLE

En ayant cette possibilité à l'esprit, notre laboratoire au MIT (l'institut de technologie du Massachusetts) travaille à la création d'une monnaie numérique adaptée aux transactions à grande échelle. Dénommée tradecoin, cette monnaie sera enregistrée de manière indélébile dans une chaîne de blocs et adossée à tout instant à un panier de biens réels tels que des récoltes agricoles, de l'énergie ou des minéraux. Cela aidera à stabiliser sa valeur et à la rendre plus fiable aux yeux du public. L'idée centrale est que, pour que son utilité ne soit pas limitée, une monnaie doit à la fois inspirer confiance et reposer sur des systèmes de transaction efficaces.

Un tradecoin numérique et fondé sur un registre distribué permettrait à des alliances de petites nations, d'entreprises, de commerçants, d'associations coopératives d'épargne et de crédit, ou même de fermiers de rassembler suffisamment de biens pour garantir une grande monnaie liquide qui serait potentiellement aussi fiable et au moins aussi efficace que les devises nationales utilisées par la Banque mondiale et le Fonds monétaire international. Les membres de l'alliance Tradecoin seraient dans une certaine mesure protégés des politiques égoïstes adoptées par les gros acteurs. Grâce à la structure cryptographique du système, il serait pour eux plus facile, plus sûr et moins coûteux de se lancer dans le commerce international. Si les membres de l'alliance sont géographiquement et politiquement diversifiés, ils seront probablement mieux immunisés contre le risque de cessation de paiement que s'ils étaient couverts par une unique grosse entité. De fait, c'est exactement ainsi que la Banque d'Angleterre a fait ses débuts en 1694 : en tant qu'alliance de marchands.

Par conception, les principes sur lesquels reposent les monnaies telles que le tradecoin sont fondamentalement différents de ceux des cryptomonnaies telles que le bitcoin, qui ne sont pas garanties par des biens réels et ne font pas intervenir d'alliances. Le tradecoin >

UNE BRÈVE HISTOIRE DE LA MONNAIE

VII^e SIÈCLE AVANT NOTRE ÈRE
Les Lydiens et les Grecs introduisent les pièces de monnaie en métal.

XIV^e SIÈCLE
Les banques marchandes telles que celle des Médicis étendent leur activité à la finance internationale, au commerce et à l'industrie.

XVII^e SIÈCLE
En prêtant la valeur de l'argent déposé, les banquiers stimulent la productivité économique, mais créent aussi de nouvelles sources de risque qui produisent régulièrement des krachs locaux, voire de grandes dépressions. Les banques centrales, qui lient l'activité bancaire et l'impôt, apparaissent.

XVIII^e SIÈCLE
On adopte l'étalon-or, dérivé de systèmes antérieurs où la circulation de monnaie était contrôlée sans grande rigueur par une réserve de métaux précieux. Il en résulte une réduction du risque.

XX^e SIÈCLE
Avec les Accords de Bâle (à partir de 1988), l'étalon-or est remplacé : ces accords stipulent que détenir des biens faciles à vendre est aussi valable que de détenir de l'or.