Relations

RELATIONS

Les cryptomonnaies, une technologie prometteuse ou dangereuse ?

Bertrand Schepper et Nadia Seraiocco

Numéro 799, novembre–décembre 2018

URI : https://id.erudit.org/iderudit/89299ac

Aller au sommaire du numéro

Éditeur(s)

Centre justice et foi

ISSN

0034-3781 (imprimé)
1929-3097 (numérique)

Découvrir la revue

Citer cet article

Schepper, B. & Seraiocco, N. (2018). Les cryptomonnaies, une technologie prometteuse ou dangereuse ? *Relations*, (799), 12–13.

DÉBAT

Depuis quelques années, les cryptomonnaies comme le Bitcoin et l'Ether suscitent à la fois enthousiasme et crainte de la part d'acteurs économiques et étatiques. Ces devises virtuelles et la technologie qui les soutient – appelée communément la chaîne de blocs ou *blockchain* – sont-elles porteuses d'innovation ou de risques économiques et écologiques importants ? Nos auteurs invités en débattent.

Les cryptomonnaies favorisent globalement la concentration de la richesse, la spéculation et la surconsommation d'énergie.

Bertrand Schepper

L'auteur est chercheur à l'Institut de recherche et d'informations socio-économiques (IRIS)

Alors que les transactions commerciales sont de plus en plus virtuelles, l'étonnante diversité et la hausse insoupçonnée de la valeur des cryptomonnaies ces dernières années laissent supposer, pour plusieurs, que ce type de devise serait l'avenir de la monnaie. Pour d'autres, au contraire, elles seraient un gadget virtuel à faible espérance de vie. Qu'en est-il ?

Une cryptomonnaie est une devise numérique et généralement décentralisée dont la création d'unités et la validation des transactions reposent sur la cryptographie. La cryptographie fait appel à une technologie, la chaîne de blocs, qui permet d'enregistrer dans une base de données à la fois cryptée et sécurisée toutes les transactions réalisées avec chacune des unités d'une cryptomonnaie depuis sa création.

Plusieurs considèrent que c'est la perte de confiance envers les institutions bancaires à la suite de la crise économique de 2008 qui a mené à la création de ce type de monnaie, puisque celle-ci exclut l'intervention d'institutions financières ou étatiques. On peut grossièrement considérer que ce système monétaire est opéré par les utilisateurs de la cryptomonnaie, qui valident les transactions inscrites au registre au moyen de leurs ordinateurs. En échange de ce travail, l'utilisateur reçoit une unité (ou part d'unité) de cryptomonnaie : c'est ce qu'on appelle « miner » des cryptomonnaies. Chaque transaction est agglomérée dans un bloc de données qui est vérifié, crypté puis rattaché à une chaîne de blocs, qui contient ainsi toutes les transactions précédentes. Alors que l'on évalue à plus de 1600 le nombre de cryptomonnaies, on ne peut qu'être impressionné par l'efficacité du système de chaîne de blocs qui les soutient. Cependant, les cryptomonnaies ont tout de même d'importants effets négatifs sur la société, qui méritent d'être évalués afin de juger si elles devraient faire partie de notre quotidien ou si elles deviendront l'apanage exclusif d'une élite financière initiée à leur fonctionnement.

Concentration de la richesse

Bien que les cryptomonnaies soient décentralisées, elles ne sont pas pour autant démocratisées. Elles permettent donc à de petits groupes d'initiés organisés d'influencer le cours de ces devises dans un objectif de spéculation et d'enrichissement personnel. Selon certaines analyses, c'est ce type d'opération qui aurait mené à la hausse foudroyante du cours du Bitcoin en 2017.

Il existe également une concentration des moyens de production des cryptomonnaies. Puisque l'équipement nécessaire à la validation des transactions est dispendieux, certaines entreprises ont mis en place des « fermes » d'ordinateurs hyperpuissants afin d'être en mesure de récolter les unités de cryptomonnaies. Cela entraîne nécessairement un effet de concentration de la richesse et renforce l'instabilité des cryptomonnaies, qui ne sont pas régulées par une banque centrale.

Dans ces circonstances, il n'est pas étonnant qu'elles soient peu utilisées par le commun des mortels. Elles restent avant tout un outil de spéculation de plus en plus récupéré par les institutions financières.

Par ailleurs, avec les cryptomonnaies se pose le problème de la fiscalité. Le principe d'anonymat qui les sous-tend complique grandement la capacité de l'État d'évaluer les revenus générés en cryptomonnaies, en plus de l'empêcher de prélever des impôts efficacement. C'est d'ailleurs pourquoi les cryptomonnaies sont devenues un outil privilégié par les organisations criminelles et par les acteurs pratiquant l'évasion fiscale.

Énergivores

L'augmentation des transactions et du nombre de cryptomonnaies ainsi que le besoin de les sécuriser exercent aussi une pression à la hausse sur la demande énergétique mondiale. Les ordinateurs spécialisés qui cryptent et décryptent des chaînes de blocs sont en effet extrêmement énergivores. À titre indicatif, l'énergie utilisée en 2018 pour « miner » des Bitcoins et de l'Ether, les deux cryptomonnaies les plus populaires, représente déjà plus que la consommation énergétique de la Belgique[1]. Cela en fait une activité extrêmement polluante et coûteuse dans des pays qui s'alimentent au charbon, comme la Chine. C'est ce qui explique la volonté de certaines « fermes » de s'installer au Québec afin de profiter d'une électricité bon marché.

Évidemment, chacune des cryptomonnaies a son propre algorithme. Certaines peuvent freiner ou limiter les problèmes présentés ci-haut. Cependant, globalement, les cryptomonnaies créent tout de même des problèmes de concentration de richesse, d'évasion fiscale et de surconsommation d'énergie. Cela en fait une forme de monnaie illégitime pour le commun des mortels et qui peut être néfaste pour la société. Par contre, les systèmes fondés sur le principe de la chaîne de blocs sont quant à eux porteurs d'avenir et risquent à terme de transformer nos vies. En ce sens, il devient primordial de ne pas se laisser éblouir par le phénomène que sont les cryptomonnaies, et d'étudier tout le potentiel que représentent les chaînes de blocs.

1. Digiconomist, « *Ethereum Energy Consumption Index (beta)* » et International Energy Agency, *Key World Energy Statistics*, 2017, [en ligne].

LES CRYPTOMONNAIES, UNE TECHNOLOGIE PROMETTEUSE OU DANGEREUSE ?

Au-delà des cryptomonnaies, la chaîne de blocs offre des applications prometteuses.

Nadia Seraiocco

L'auteure est doctorante et chargée de cours en médias numériques à l'UQAM

Le Bitcoin a attiré beaucoup d'attention récemment. Cette monnaie virtuelle décentralisée fondée sur une technologie d'encryptage complexe – la chaîne de blocs – a vu sa valeur exploser en quelques mois, pour continuer ses fluctuations, suscitant l'intérêt du secteur financier notamment. Certains ont louangé les possibilités qu'offre cette cryptomonnaie, d'autres ont mis en garde contre ses dérives. Mais cette attention a quelque peu détourné la discussion du véritable intérêt de cette innovation, soit la technologie de la chaîne de blocs elle-même.

Cette technologie a été créée en 2008 afin d'enregistrer et d'authentifier de manière sécurisée les transactions du Bitcoin, mais son utilisation en vue d'archiver des contrats dits intelligents, des prêts, voire des actes de médiation par une tierce partie, était déjà envisagée dès 2010[1]. Il existe aussi depuis quelques années des entreprises qui développent des applications fondées sur la chaîne de blocs dans les secteurs des contrats dits intelligents et de la protection du droit d'auteur.

Pour expliquer en des termes simples ce que peut apporter la chaîne de blocs à l'émission de contrats, résumons la chose ainsi : elle permet à des parties inconnues l'une de l'autre d'authentifier une transaction (ponctuelle) ou un contrat (donc une entente qui inclut une notion de durée) sans l'intervention d'une tierce partie dite fiable (par exemple un notaire), évitant ainsi des coûts de services liés à cet échange. Le cryptage et la distribution décentralisée de l'authentification par la chaîne de blocs permettent ce procédé communément appelé « contrat intelligent ». Toutefois, les caractéristiques qui donnent à la chaîne ses propriétés sécuritaires (la possibilité pour tout utilisateur de voir toutes les transactions du registre, notamment) compliquent énormément la faculté d'assurer l'aspect privé des renseignements contenus dans les contrats. Si la chaîne de blocs permet aux utilisateurs d'agir sous des pseudonymes, elle exige de créer des clés de cryptage publiques : le contenu comme la nature des transactions demeurent ainsi exposés. Cette transparence est un atout pour l'archivage des contrats des organismes publics. Sauf que pour consigner de façon sécuritaire des transactions dont le contenu doit demeurer privé, il faut joindre à la chaine de blocs des services supplémentaires de cryptage ou de chiffrement, ajoutant ainsi une couche de complexité à un système déjà très élaboré.

Protéger le droit d'auteur

Le piratage et la reproduction illégale d'œuvres numériques ont grandement remis en question l'industrie culturelle, comme le marché de l'art, fondée sur les revenus générés par chaque copie d'une œuvre mise en circulation par les détenteurs des droits d'auteur. Avec la création de biens culturels en format numérique, pouvant être copiés et distribués sans aucune compensation pour les ayants droit, plusieurs souhaitaient une option de chiffrement qui permette de mieux contrôler leur distribution.

De nouveaux joueurs, issus du secteur créatif, comme Monegraph ou Rhizome.org, proposent maintenant des solutions d'enregistrement destinées aux produits culturels, et ce, grâce à la chaîne de blocs. Ces solutions de chiffrement et de distribution permettent de télécharger des œuvres numériques, de choisir les termes de leur distribution et d'en faire la mise en marché. Si ces nouvelles avancées en protection du droit d'auteur et de la propriété intellectuelle ne sont pas des panacées dans la culture du « tout gratuit » bien ancrée sur le Web, elles constituent une avenue intéressante et ouvrent de nouvelles voies pour penser les droits rattachés aux œuvres d'art et aux produits créatifs.

L'avenir du Web ?

Le Bitcoin est la plus connue des cryptomonnaies, mais il en existe d'autres qui fonctionnent avec différents types de chaînes de bloc. Celle créée par Vitalik Buterin, Ethereum, et sa cryptomonnaie, l'Ether, est la principale concurrente de la chaîne soutenant le Bitcoin et serait plus performante et moins énergivore. Cela fait dire à son créateur et à certains observateurs du développement des chaînes de blocs qu'Ethereum pourrait éventuellement supplanter le Web actuel, pour créer le « Web 3.0 ». Ainsi, ce sont toutes les interactions sur Internet qui seraient enregistrées, authentifiées et chiffrées pour plus de sécurité, le tout par des tiers dans un réseau décentralisé. Transparence et sécurité des données : qui ne souhaiterait pas en théorie un pareil Web ?

Or, les chaines de blocs sont-elles vraiment la seule solution qui s'offre à nous pour préserver l'intégrité de l'information contenue dans les contrats ou protéger les droits des créateurs ? Ces systèmes sont encore très lourds à opérer : ils demandent une immense puissance de calcul et consomment des quantités considérables d'énergie. Serions-nous si éblouis par les prouesses informatiques promettant de mettre fin aux transactions malhonnêtes, aux vols de propriété intellectuelle improuvables, que nous nous laissons une fois de plus envoûter par l'espoir de pallier les tromperies humaines par le biais des avancées technologiques ?

1. Melanie Swann, *Blockchain : Blueprint For a New Economy*, O'Reilly Media Inc, 2015.