Les monnaies numériques

OBJET

Au cours des dix dernières années, l'utilisation combinée d'Internet et de la cryptographie asymétrique[1] a donné naissance aux monnaies numériques ou cryptomonnaies. Bien qu'il en existe quelques centaines, la plus connue et la plus utilisée est le bitcoin. C'est aussi lui qui a fait jusqu'à présent l'objet de la plupart des articles consacrés à la nature et au fonctionnement de ces nouveaux moyens de paiement.

Pour certains, les cryptomonnaies ne sont pas de vraies monnaies, car elles ne posséderaient pas les caractéristiques de ces dernières. Pour d'autres, elles affranchissent les utilisateurs du contrôle des banques centrales et commerciales sur l'émission et la circulation des monnaies et sur les frais bancaires.

Quels sont les arguments des uns et des autres? Quelles sont les caractéristiques des monnaies numériques? Comment fonctionnent-elles et qui peut les utiliser? Quels avantages et inconvénients présentent-elles par rapport aux monnaies traditionnelles? Quelle évolution peut-on leur prévoir? Les lectures et les références qui suivent apportent des éléments de réponse à ces questions.

LES CINQ LECTURES POUR COMPRENDRE

1 / **Banque du Canada, *La monnaie électronique et les monnaies électroniques décentralisées (comme le bitcoin)*, Documents d'information, avril 2014.**

Selon la Banque du Canada, il existe deux formes de monnaies électroniques : la centralisée et la décentralisée. La première catégorie comprend les cartes de crédit, les cartes prépayées, les comptes PayPal. Ces moyens de paiement ont en commun d'être émis et administrés par une institution financière et d'être liés à une monnaie nationale. La deuxième catégorie, les monnaies électroniques décentralisées, n'a pas ces deux caractéristiques. Elles circulent dans les réseaux informatiques de pair à pair, en marge des systèmes monétaires nationaux et sans lien avec eux. Elles sont aussi appelées cryptomonnaies. La première, le bitcoin, a vu le jour le 3 janvier 2009.

Selon les deux documents de la Banque, actuellement, les cryptomonnaies ne répondent pas aux trois critères qui définissent une monnaie conventionnelle. Elles ne sont pas acceptées par tous les marchands; elles ne peuvent être utilisées pour comparer les prix des biens et services au fil du temps et d'un marchand à l'autre; et elles sont trop volatiles pour servir d'instruments de réserve de valeur.

[1] La cryptographie consiste à crypter ou chiffrer un message en vue de le rendre inintelligible à quiconque n'est pas autorisé d'en prendre connaissance. La cryptographie asymétrique chiffre le message à l'aide de deux clés : une publique et une privée. La clé publique du destinataire d'un message est utilisée par l'expéditeur pour le chiffrement. Le destinataire utilise sa clé privée pour décoder le message de l'expéditeur.

BIBLIOTHÈQUE
SERVICE DE LA RECHERCHE
ASSEMBLÉE NATIONALE
DU QUÉBEC

Les cryptomonnaies présentent trois types de risques. Le risque de perte lié à la volatilité du cours, le risque de faillite des plateformes d'échange et le risque lié à l'absence d'encadrement juridique.

En décembre 2017, il y avait plus de 900 cryptomonnaies. Elles avaient une capitalisation de plus 510 milliards de dollars. On comptait en outre une cinquantaine de plateformes d'échange de ces monnaies. La plus importante est Coinbase, fondée en 2012 à San Francisco, en Californie. En avril 2018, quelque 10 millions de clients y ont déjà négocié pour plus de 10 milliards de dollars américains. Ces échanges ont impliqué la conversion de 32 devises[2].

2 / Pérez, Marco Ricardo, « *Blockchain* : l'autre révolution venue du bitcoin », CNRS, *Le journal*, 19 mai 2016.

Le bitcoin s'échange de pair à pair, c'est-à-dire entre deux utilisateurs, sans aucun intermédiaire. Sa création, son émission, son échange et sa gestion sont assurés par des logiciels. Son inventeur est connu sous le pseudonyme de Satoshi Nakamoto. On ne sait s'il s'agit d'un individu ou d'un groupe de gens. Il n'a pas donné signe de vie depuis 2010.

Tous les utilisateurs du bitcoin doivent avoir au moins un ordinateur muni d'un logiciel-client, une adresse Bitcoin, une clé publique et une clé privée. L'adresse est un condensé de la clé publique. La clé publique permet de chiffrer le message et est accessible à tous les utilisateurs. La clé privée, générée aléatoirement de préférence[3], est connue seulement de son propriétaire. Elle lui permet d'accéder à ses fonds et de signer ses envois de bitcoins. La clé privée est liée à la clé publique par une relation mathématique[4] et permet de déchiffrer cette dernière. Le receveur encaisse l'envoi grâce à sa clé privée qui déchiffre sa clé publique utilisée par le payeur pour lui envoyer des bitcoins. Un utilisateur peut avoir autant de clés publiques qu'il désire.

Les opérations en bitcoin sont sécurisées grâce à la technologie de la chaîne de blocs ou *blockchain*. La chaîne de blocs est une base de données électronique publique contenant toutes les transactions en bitcoin validées depuis la création de la cryptomonnaie, le 3 janvier 2009. Les transactions du système sont regroupées en blocs et validées. Un bloc est validé toutes les dix minutes environ et ajouté à la suite du dernier bloc de la chaîne de blocs.

La validation du bloc est appelée minage. De nos jours, elle est effectuée par des systèmes très puissants et consiste en la résolution d'un problème mathématique complexe basé sur la cryptographie et relié au bloc. Le problème change tous les quinze jours et son niveau de difficulté augmente. Le premier mineur qui résout le problème est gratifié d'un certain nombre de nouveaux bitcoins générés automatiquement

---

[2] https://www.coinbase.com/

[3] Il existe 2 à la puissance, 256 possibilités de clés privées différentes, soit 1,16 x 10^{77}. Il est donc improbable de générer deux fois de façon aléatoire la même clé privée. Pour la même raison, générer et tester un grand nombre de clés privées aléatoires dans l'espoir de tomber sur un compte contenant des bitcoins est totalement vain. La fabrication d'une clé privée ne nécessite donc pas la vérification et l'enregistrement sur le réseau, ce qui permet à Bitcoin de fonctionner de façon décentralisée. On calcule la clé publique à partir de la clé privée. L'inverse est évidemment impossible.

[4] La signature des transactions Bitcoin et leur vérification utilisent la cryptographie asymétrique et plus précisément l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm) qui assure aussi la génération des paires de clés (privée et publique) nécessaire aux signatures.

par le réseau : 50 bitcoins en 2009, 25 en 2013, 12,5 en 2017, 6,25 en 2021 et ainsi de suite. Les ordinateurs ou les systèmes des mineurs doivent être équipés d'un logiciel de minage. Il existe actuellement quelque 200 systèmes de minage dans le monde.

L'incorruptibilité de la chaîne de blocs est garantie par la puissance de calcul phénoménale qui serait nécessaire pour la corrompre. On estime que, pour falsifier un bloc donné, il faudrait une puissance égale à la totalité de celle utilisée pour valider tous les blocs précédents de la chaîne. En 2017, la puissance du réseau Bitcoin dépassait les 10 exaflops par seconde[5]. En comparaison, l'ordinateur le plus puissant sur la planète en 2016 avait une puissance de 125 pétaflops par seconde[6].

Il existe aujourd'hui des centaines de variantes du modèle bitcoin s'appuyant sur la chaîne de blocs de cette cryptomonnaie. Mais la technologie peut être utilisée dans toute application de transfert et de stockage distribué. Aussi, les banques, les compagnies d'assurance, les bureaux de notaires et d'avocats, etc. cherchent-ils à développer leur propre chaîne de blocs, distincte de celle du bitcoin.

3 / Mignot, Sylvain, « Dossier Bitcoin : Le bitcoin : nature et fonctionnement », *Banque & Droit*, nº 159, janvier-février 2015.

Le bitcoin a été développé à partir de technologies de plusieurs autres monnaies électroniques beaucoup plus primitives. Il importe de distinguer le bitcoin, la devise, du Bitcoin, le système ou le réseau.

Les cryptomonnaies donnent lieu à des frais de transactions extrêmement faibles. Au cœur des méthodes de validation des transactions et de la génération des cryptomonnaies est le concept de « preuve de travail ». Il s'agit de la résolution du problème informatique qui atteste de la validation d'un bloc.

Le bitcoin, comme toutes les cryptomonnaies, n'est émis, contrôlé ou garanti par aucune autorité centrale dans aucun pays. Son émission est prédéterminée dans un code informatique consultable par tous (*open source*) et l'évolution de sa quantité dans le temps est prévisible. Les transactions sont validées par des mineurs sélectionnés au hasard, et à intervalles réguliers.

Dans le système Bitcoin, les seules données chiffrées ou cryptées sont les clés privées et publiques. Les transactions ou messages ne le sont pas. Tout utilisateur peut ainsi consulter toutes les transactions ayant eu lieu. Par ailleurs, la clé publique d'un utilisateur est semblable à une adresse électronique permettant à son propriétaire d'effectuer et de recevoir des paiements. Elle figure dans la chaîne de blocs et peut être connue de tous. La clé privée est comparable à un mot de passe et est utilisée pour signer chaque dépense de bitcoins à partir d'une clé publique définie. La clé privée donne le contrôle des bitcoins contenus dans la clé publique qui lui est associée.

Chaque bitcoin est divisible jusqu'à la 8e décimale. La plus petite subdivision du bitcoin (le cent millionième) est appelée satoshi. Un satoshi vaut 100 microbitcoin ou $100*10^{-6}$ bitcoin.

[5] Un flop par seconde désigne le nombre d'opérations sur les nombres réels qu'un ordinateur peut effectuer par seconde. Le préfixe exa signifie, quant à lui, un milliard de milliards, soit 10^{18}.

[6] 125 pétaflops= 125 millions de milliards ou $125*10^{15}$ opérations par seconde.

Un individu voulant se connecter doit obtenir l'adresse Internet (adresse IP) d'un ordinateur du réseau et télécharger la chaîne de blocs. Celle-ci vient avec le logiciel client. Le nouveau membre est alors en échange permanent avec les autres membres du réseau et peut effectuer des transactions.

Une transaction consiste toujours en un transfert de bitcoins du compte d'un utilisateur à un autre. Elle doit être signée numériquement par le payeur, diffusée à l'ensemble du réseau et validée par un des mineurs, le premier qui y parvient. La transaction validée est ensuite stockée dans un ensemble d'autres transactions appelé bloc que le mineur a déjà validé. Le mineur en question ajoute alors au bloc la date, l'heure et un identifiant cryptographique unique, le hash, qui rend le bloc non modifiable.

Selon l'auteur, l'apposition du hash présuppose la résolution d'un problème informatique dont la difficulté augmente automatiquement tous les 15 jours. Ce problème s'adapte aussi automatiquement d'une validation à l'autre de façon à ce que celle-ci se produise toutes les dix minutes. Elle est coûteuse en temps et en consommation d'énergie en raison de la difficulté du problème. Le bloc validé est diffusé sur le réseau et les utilisateurs essaient de l'intégrer à la copie de la chaîne de blocs présente sur leur ordinateur. Si au moins six y parviennent, alors les transactions sont considérées comme nouvelles et cohérentes avec les précédentes. Dans le cas contraire, le bloc n'est pas valide et est rejeté.

Comme la validation est au cœur du système Bitcoin, afin de maintenir ce dernier en fonction, deux systèmes de rémunération des mineurs sont incorporés au protocole. Le premier est la création de nouveaux bitcoins à chaque validation. C'est l'unique façon de créer de nouveaux bitcoins. À l'origine, en janvier 2009, la rémunération par validation de bloc était de 50. Ce nombre diminue de moitié tous les quatre ans et tombera pratiquement à 0 en 2140. Cette année-là, le plafond de 21 millions de bitcoins fixé par Nakamoto sera atteint et il n'y aura plus de création de bitcoins d'aucune manière[7]. Alors commencera le deuxième mode de rémunération, des frais de transaction. Les utilisateurs seront alors tenus de payer les frais de transaction qu'ils voudront, mais ils doivent être suffisamment élevés pour intéresser et inciter les mineurs à les valider.

La majorité des articles sur le bitcoin s'intéresse à ses risques liés à la volatilité du cours, à l'anonymat et à l'utilisation illicite de la devise. Ici, l'auteur se penche plutôt sur les risques techniques du bitcoin. Ceux-ci sont les bogues éventuels, la taille toujours croissante de la chaîne de blocs, la possibilité de collusion entre des mineurs pour décider des transactions à inclure dans les blocs et finalement le délai nécessaire à la validation (assez long en informatique!). Selon l'auteur, le premier risque est faible. En effet, les membres actifs du réseau *open source* sont assez nombreux pour que le bogue soit réparé rapidement. Le second risque est aussi faible en raison de la puissance toujours croissante des ordinateurs. Quant aux deux derniers risques, ils sont réels, même s'ils ne se sont pas encore avérés.

[7] On estime que 99 % des 21 millions de bitcoins seront déjà créés en 2035, et le solde pendant les 105 autres années. Cela tient de la division de la rémunération par deux tous les quatre ans.

4 / Chelet, Jonathan, « Bitcoin : bientôt une bourse pour échanger la monnaie virtuelle, Capital.fr et Brecht, Somers, la bourse ne veut pas du bitcoin », *Data News*, 13 mars 2017.

En 2013, les frères Cameron et Tyler Winklevos ont déposé une demande pour créer un fonds indiciel à être négocié en bourse et qui reflétera les variations du bitcoin. Ce fonds, le Winklevos bitcoin trust, pourra être acheté par les investisseurs traditionnels des marchés boursiers. Les deux frères qui possédaient alors 1 % des 13,8 millions de bitcoins en circulation visaient notamment à : (1) offrir une plateforme d'échange de bitcoins plus fiable que la cinquantaine de sites d'échange existants en juillet 2015; (2) protéger les utilisateurs contre la fraude et les attaques informatiques; (3) stabiliser le cours du bitcoin et rendre la cryptomonnaie plus liquide; (4) soumettre les bitcoins négociés en bourse à la Security Exchange Commission (SEC) afin d'éliminer l'anonymat qui entoure leur utilisation. Selon eux, ces quatre objectifs permettront de diminuer sensiblement l'utilisation du bitcoin pour le blanchiment d'argent et les activités illicites.

La réalisation de ces objectifs comporte deux défis majeurs. Premièrement, il faudra convaincre les utilisateurs de laisser un de leurs principes de base, soit l'absence d'intermédiaire dans le processus d'échange des bitcoins. En effet, la bourse sera un intermédiaire. Deuxièmement, il sera nécessaire d'obtenir la permission de l'autorité des marchés financiers des États-Unis, la SEC. Cela n'est pas pour le court terme.

En effet, le 11 mars 2017, la SEC a décidé d'interdire la création du fonds négocié en bourse. Les motifs à la base du refus sont la très grande volatilité du bitcoin et la faible protection du système Bitcoin contre la manipulation, la fraude ou les attaques informatiques. Cela étant, l'organisme fédéral américain ne ferme pas à tout jamais la porte. Il souligne que le bitcoin est encore trop jeune et qu'il n'est pas exclu que des marchés réglementés qui lui sont liés se développent à terme.

5 / Fabien Major,« Attention aux cryptomonnaies », *Le Journal de Québec*, 4 juillet 2017.

Fabien Major, conseiller en épargne collective, répond aux lecteurs désireux d'investir dans les cryptomonnaies. Il reconnaît que la tentation est forte. En effet, selon lui, 10 000 dollars investis en bitcoins en 2010 valent maintenant plus de 200 millions de dollars. Toutefois, ces monnaies sont plus volatiles que les actions. En effet, si de janvier à juillet 2017 le bitcoin a augmenté de 137 %, il a perdu 25 % du 12 juin au 29 juin.

L'auteur souligne que le principe de ces monnaies électroniques repose sur une technologie complexe, la *blockchain*. Cette technologie assure une si grande sécurité des transactions que des institutions, telles Fidelity, J.P. Morgan, RBC, et TD, veulent l'utiliser pour protéger davantage les opérations interbancaires.

De l'avis de M. Major, malgré leur popularité, l'achat des cryptomonnaies ne peut être considéré comme un investissement, mais plutôt comme de la spéculation. Il les compare même aux chaînes pyramidales des années 1980 qui enrichissaient quelques personnes et lessivaient de nombreuses autres. Il cite l'exemple de Mt Gox, une plateforme d'échange de bitcoins de Tokyo qui a fait faillite en 2014 et a fait perdre 300 millions de dollars à des particuliers.

Selon certains, cette somme a été dérobée par des pirates informatiques. D'autres ont accusé le fondateur du site d'avoir détourné la somme. Quoi qu'il en soit, l'auteur invite les lecteurs à la prudence. Les motifs de cet appel résident dans les caractéristiques suivantes du marché des cryptomonnaies :

- L'absence de cours légal et des risques de vol et de fraude importants.
- L'absence de réglementation et de cadre juridique protégeant les utilisateurs.
- La non-reconnaissance par la Banque du Canada comme un moyen d'échange.
- L'attrait pour toutes sortes d'activités illégales en raison de l'anonymat qu'elles garantissent.
- La perte irrécupérable du contenu du portefeuille virtuel en cas de perte du code associé.

ET CINQ AUTRES LECTURES (POUR ALLER PLUS LOIN)

1 / Brito, Jerry; Castillo, Andrea, *Bitcoin: A Primer for Policymakers*, Arlington, Virginia: Mercatus Center, George Mason University, 2016. 109 p.

2 / Cryptos.net, *Comment installer un mineur de bitcoin?*

3 / European Central Bank, *Virtual currency schemes, a further analysis*, Frankfurt : European Central Bank, 2015. 37. p.

4 / Murphy, Edward V, Murphy, M. Maureen, Seitzinger, Michael V, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, *Congressional Research Service*, 2015. 32 p.

5 / Vachon, Hendrix, « Les limites des monnaies du type bitcoin », *Point de vue économique*, 21 novembre 2013, 5 p.

Préparé par Samuel Houngué, Service de recherche, mai 2018.