Rapport stratégique

Bureau du chef des placements | Juin 2022

Actifs numériques : bulle spéculative ou véritable révolution? Partie 1/3.
Les principes fondamentaux

Les cryptomonnaies, comme le bitcoin, constituent la plus célèbre catégorie d'actifs numériques. Leur capitalisation boursière a explosé au cours des dernières années pour atteindre une valeur d'environ deux mille milliards de dollars canadiens, soit environ l'équivalent de la totalité du marché boursier canadien. Leur popularité qui était autrefois contrainte aux investisseurs particuliers s'est étendue à certains gouvernements et investisseurs institutionnels. Plusieurs sceptiques soutiennent que ce marché présente des caractéristiques irrationnelles, notamment en raison du nombre d'actifs numériques qui connait une croissance ahurissante. S'agit-il d'une bulle spéculative ou d'une véritable révolution ? Pour tenter d'éclaircir la situation, trois rapports stratégiques seront dédiés aux actifs numériques.

Ce premier rapport présente un sommaire des principes fondamentaux derrière les actifs numériques. Le deuxième rapport mettra en évidence les méthodes d'évaluation qui ont été proposées jusqu'à présent pour les cryptomonnaies. Finalement, le troisième rapport étudiera l'impact de ces actifs dans un processus de construction de portefeuille.

Faits saillants

- Les cryptomonnaies sont nées d'un désir d'améliorer l'efficacité des transactions entre les individus en décentralisant les bases de données. Pour garantir l'intégrité du réseau, deux composantes sont nécessaires.
- Premièrement, une série d'étapes mathématiques doit permettre de prouver l'identité de l'auteur d'une transaction. Deuxièmement, l'historique des transactions (la chaîne de blocs ou *blockchain*) doit être partagé par tous les membres du réseau. Ce registre partagé est mis à jour par un mécanisme de validation qui peut prendre la forme d'une preuve de travail ou une preuve d'enjeu. C'est cette deuxième composante qui est la principale innovation associée aux actifs numériques. En effet, la chaîne de blocs est perçue par certains comme une technologie pouvant avoir des impacts majeurs dans plusieurs domaines.
- Bien qu'il y ait désormais une grande variété de réseaux avec divers mécanismes et actifs numériques associés, leurs caractéristiques par rapport aux systèmes conventionnels se résument généralement en trois catégories: (1) la capacité de régler rapidement et à moindre coût des transactions complexes; (2) la rareté numérique; (3) la possibilité de créer des contrats intelligents.

Christophe Faucher-Courchesne
Associé, stratégie quantitative
Bureau du chef des placements

Nicolas Charlton
Associé, stratégie quantitative
Bureau du chef des placements

BANQUE NATIONALE
INVESTISSEMENTS

Une croissance phénoménale

Les plus vieux actifs numériques n'ont pas encore célébré leur quinzième anniversaire. Pourtant, les cryptomonnaies qui constituent la plus célèbre catégorie d'actifs numériques dont fait partie le Bitcoin représentent aujourd'hui une valeur marchande combinée d'environ 1,6 milliard de dollars canadiens, ce qui est environ équivalent à la moitié de la totalité du marché boursier canadien. Leur popularité qui était autrefois limitée aux investisseurs particuliers s'est étendue à certains gouvernements et investisseurs institutionnels. Les républiques du Salvador et de Cuba ont d'ailleurs conféré le statut de cours légal au bitcoin 2021.

Or, l'engouement pour ces actifs ne fait pas l'unanimité. Certains pays comme la Chine ont tout simplement banni les cryptomonnaies. Plusieurs sceptiques soutiennent que ce marché présente des caractéristiques irrationnelles, notamment en raison du nombre d'actifs numériques et de leur capitalisation boursière qui connait une croissance ahurissante (**graphique 1**). Il y a maintenant plus de 19 000 cryptomonnaies en circulation[1] et de nombreux autres types d'actifs numériques comme les jetons non fongibles (JNF, traduction de *non-fungible token*, NFT) qui continuent de voir le jour. S'agit-il d'une bulle spéculative ou d'une véritable révolution ?

1 | Croissance fulgurante des cryptomonnaies

Bureau du chef des placements (données via coinmarketcap.com)

Pour tenter d'éclaircir la situation, trois rapports stratégiques seront dédiés aux actifs numériques. Ce premier rapport présente un sommaire des principes fondamentaux derrière les actifs digitaux. Le second sera consacré à l'évaluation de leur valeur fondamentale, tandis que le troisième étudiera la question d'inclure de tels actifs dans un processus de construction de portefeuille.

Les débuts du Bitcoin

En 2008, un article intitulé *Bitcoin: A Peer-to-Peer Electronic Cash System* a décrit un programme qui permettrait aux utilisateurs de procéder à des transactions financières sans intermédiaire grâce à une base de données robuste et décentralisée : la chaîne de blocs (*blockchain*). Quelques semaines plus tard, en 2009, le programme a été rendu disponible et le Bitcoin[2] est né.

L'objectif de cet article était de proposer une méthode pour moderniser la façon de procéder à des transactions. En effet, malgré les nombreux progrès technologiques des dernières décennies, l'exécution des transactions entre des clients de différentes banques, ou encore, de différents pays n'est pas instantanée. Encore de nos jours, ces transferts monétaires peuvent nécessiter des délais ou des frais non négligeables. Pour illustrer la situation traditionnelle et mieux comprendre l'innovation proposée par l'article original, considérons deux personnes, Alice et Bob, désirant effectuer une transaction. Alice est cliente de la Banque A, tandis que Bob est client de la Banque B.

Supposons qu'Alice désire envoyer 5 000$ par chèque[3] à Bob. Lorsque Bob encaisse le chèque, la Banque B doit s'assurer qu'Alice dispose bien de la somme promise avant d'ajouter le montant au compte de Bob. Or, la base de données de la Banque B n'est constituée que de ses propres clients. Comme la Banque B n'a pas accès aux

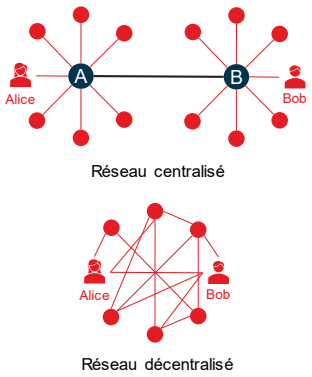
[1] Données via https://coinmarketcap.com/.
[2] Le Bitcoin, avec une lettre majuscule, désigne le réseau sur lequel la devise, le bitcoin avec une lettre minuscule, est transigée.
[3] Notons que l'utilisation du chèque ne sert qu'à imager l'exemple sans en réduire sa pertinence, car des processus similaires sont impliqués pour les transferts électroniques usuels.

informations nécessaires concernant Alice, elle doit contacter la Banque A pour que celle-ci procède à la vérification dans sa propre base de données et lui transmette l'information. Une fois la confirmation effectuée, la Banque B peut rendre la somme disponible auprès de Bob. Ce processus nécessite un certain temps et explique une bonne partie du délai ainsi que des frais exigés.

Le Bitcoin, un réseau décentralisé

L'innovation proposée par l'article repose sur une base de données partagée par l'ensemble d'un réseau (**graphique 2**). En effet, si tous les membres d'un réseau pouvaient vérifier qu'Alice possède les 5 000$ et qu'elle est bien l'instigatrice de la demande de transfert vers Bob, la vérification s'en trouverait accélérée.

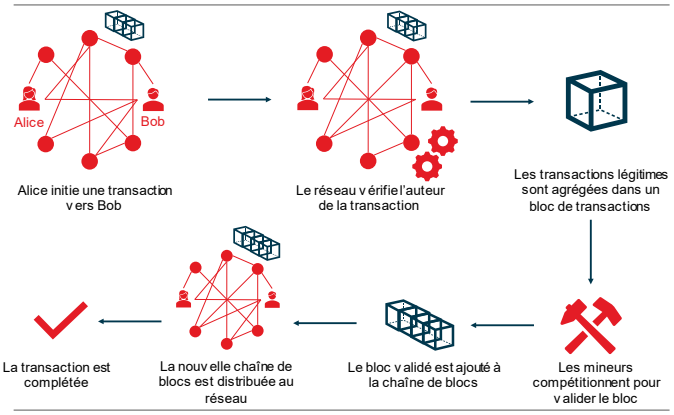
2 | Centralisé vs décentralisé



Bureau du chef des placements

Pour ce faire, deux défis doivent être relevés. Le premier défi est un problème d'authentification. Alice doit pouvoir prouver au réseau qu'elle désire bien effectuer une transaction, sans quoi un autre utilisateur pourrait falsifier une transaction au nom d'Alice. Le second défi concerne le consensus du réseau. Tous les membres du réseau doivent continuellement parvenir à un consensus sur le solde de chacun des comptes des membres du réseau afin de prévenir une situation où un utilisateur tenterait de transférer une somme qu'il ne possède pas. Les concepts mathématiques et informatiques derrière la technologie permettant de relever ces deux défis sont complexes. Leur compréhension n'est certes pas requise pour détenir et échanger des actifs numériques, au même titre qu'il n'est pas nécessaire de comprendre les rouages du système bancaire pour détenir un compte dans une institution financière. Il est toutefois pertinent de brosser un portrait simplifié du fonctionnement d'une transaction (**graphique 3**) avec cette technologie afin de mieux comprendre les innovations proposées et l'intérêt pour les actifs numériques.

3 | Processus de transaction



Bureau du chef des placements

Le premier problème, soit l'authentification de l'auteur d'une transaction, est résolu par l'utilisation de paires de clés uniques. Chaque membre du réseau de la chaîne de blocs possède deux clés : une clé privée et une clé publique. La clé privée fonctionne comme un mot de passe et ne doit donc jamais être révélée au réseau. Elle permet à son détenteur d'effectuer des transactions de son compte vers d'autres comptes. À l'inverse, la clé publique est accessible à tous les membres du réseau. Elle est générée à partir de la clé privée et permet aux autres utilisateurs de transférer des sommes vers le compte de son détenteur. L'algorithme de cryptographie utilisé pour générer la clé publique fait en sorte qu'il est facile pour le détenteur de la clé privée de générer sa clé publique, mais qu'il est impossible en pratique pour les autres utilisateurs de deviner la clé privée à partir de la clé publique. Ces concepts de cryptographie ne sont pas propres à la chaîne de blocs ou aux actifs numériques. Au contraire, ils sont couramment utilisés sur Internet, notamment

par les pages web de type HTTPS depuis les années 90.

Afin de comprendre comment ces clés permettent d'authentifier l'auteur d'une transaction sur la chaîne de blocs, revenons à l'exemple d'Alice et de Bob. Alice désire envoyer 5 000$ à Bob. Pour ce faire, elle crée un fichier informatique contenant le destinataire, c'est-à-dire la clé publique de Bob, ainsi que le message stipulant le montant devant être transféré. Afin d'authentifier la provenance du message, Alice appose une signature électronique sophistiquée qui dépend du message, mais aussi de sa clé privée. Or, cette clé privée ne doit évidemment pas être rendue publique. Pour protéger la clé privée, une série d'opérations mathématiques sont utilisées pour créer une signature. La séquence combine puis transforme le message et la clé privée en une valeur unique qui accompagne le message original. Alice peut donc signer grâce à sa clé privée sans la révéler. De plus, comme la signature d'Alice est unique à chacune des transactions (car le contenu du message change), il est impossible pour un autre utilisateur de tenter de falsifier une transaction en réutilisant la même signature que celle fournie par Alice dans la transaction avec Bob. Dans ce contexte, comment le réseau peut-il reconnaître qu'il s'agit bien d'une signature d'Alice si elle ne révèle pas explicitement sa clé privée?

Une seconde séquence d'opérations, de vérification cette fois, est utilisée par le reste du réseau pour confirmer l'authenticité de la signature. La fonction de vérification combine la clé publique d'Alice (qui, rappelons-le, est liée à la clé privée), sa signature et son message. Toujours grâce à des opérations mathématiques, il est possible de déterminer si la signature produite est bien liée à la clé publique d'Alice et indirectement à sa clé privée. Bref, ces deux fonctions permettent à Alice de masquer sa clé privée tout en prouvant à l'ensemble du réseau par l'entremise de sa clé publique qu'elle détient la clé privée ayant servi à générer la signature. Le problème d'authentification est ainsi solutionné à l'aide de techniques de cryptographie connues. Le second défi précédemment mentionné consiste à s'assurer que tous les acteurs du réseau parviennent à un consensus du solde des différents comptes. Autrement dit, il est nécessaire que chaque participant possède une copie identique du registre de l'historique des transactions afin d'éviter qu'un participant tente de transférer une somme qu'il ne possède pas. C'est ici que l'innovation de la chaîne de blocs entre en œuvre.

Des mineurs ~~d'or~~ de bitcoin

Quel protocole permet de garantir que tous les participants du réseau possèdent la même version du registre ? Voilà la question à laquelle l'article original du Bitcoin répond en proposant de faire confiance au registre ayant nécessité le plus grand effort de calcul. Retournons à l'exemple d'Alice et Bob pour illustrer l'effort mentionné. Précédemment, Alice a envoyé un message au réseau transmettant son intention de transférer 5 000$ à Bob. Le réseau a ensuite procédé à la vérification de sa signature. Après cette opération, la transaction proposée par Alice est mise en attente de validation. La validation est effectuée par des membres particuliers du réseau qui se nomment « mineurs ». Ces participants agrègent les différentes transactions proposées dans un « bloc ». Ce bloc contient aussi une copie de la plus récente version du registre ce qui permet de conserver l'historique des transactions antérieures.

Les différents mineurs entrent alors en compétition pour tenter de résoudre un problème cryptographique complexe qui est lié au bloc de transaction en question. Ce problème ne se résout que par essai-erreur et requiert un effort computationnel important. En revanche, la conception du problème fait en sorte qu'il est banal de valider la réponse une fois qu'elle est découverte par un des mineurs. Ce mécanisme de validation se nomme *preuve de travail* (*proof of work*). Lorsqu'un mineur trouve la réponse et qu'elle est validée par les autres mineurs, le bloc de transactions est ajouté au registre et transmis à l'ensemble des participants. Ce registre est donc une succession de blocs approuvés : la fameuse chaîne de blocs.

Le niveau de complexité du problème s'adapte en fonction du nombre de mineurs, de sorte qu'un bloc nécessite toujours une dizaine de minutes en moyenne pour être approuvé. Ce même mécanisme offre une bonne protection contre de potentiels mineurs malveillants qui tenteraient de faire approuver des blocs frauduleux. En effet, comme le registre officiel est celui ayant nécessité le plus grand effort de calcul (donc le plus de blocs approuvés), les mineurs malveillants devraient réussir à faire approuver plus de blocs sur leur version parallèle du registre que le registre officiel, ce qui est improbable si le nombre de mineurs malveillants ne représente pas la majorité des mineurs.

La résolution du problème pour fournir la preuve de travail nécessite des coûts informatiques et énergétiques. Le premier mineur réussissant à trouver la solution qui entraîne la validation du bloc reçoit une compensation sous forme de nouveaux actifs associés à cette chaîne de blocs, par exemple des bitcoins. Ces participants sont donc appelés des mineurs par analogie avec l'or : leur participation fait augmenter le nombre de pièces émises. En 2022, les mineurs de bitcoins qui parviennent à trouver la solution à un bloc reçoivent 6,25 nouveaux bitcoins, ce qui signifie environ 250 000 dollars canadiens[4]. Or, le cours du bitcoin n'est pas le seul facteur qui influence la récompense puisque le nombre de pièces obtenues par minage est programmé pour diminuer au fil du temps. Le nombre total de bitcoins sera limité à 21 millions et 90% de ceux-ci ont déjà été produits. Les derniers bitcoins devraient être produits vers l'an 2140. Ce fonctionnement entraîne un concept inédit: la rareté numérique.

Les cryptomonnaies se multiplient

La combinaison des mécanismes associés aux paires de clés et de la preuve de travail permet de créer le réseau décentralisé et sans intermédiaire. Cela ne signifie pas pour autant que la solution est parfaite. Le mécanisme de validation par preuve de travail est très énergivore et limite le nombre de transactions pouvant être validées. Le réseau Bitcoin peut supporter moins de 10 transactions par seconde. En comparaison, Visa estime pouvoir supporter jusqu'à 24 000 transactions par seconde grâce à son système centralisé. Ces limites techniques ont donné naissance à une multitude de réseaux différents et à leur cryptomonnaie associée. Par exemple, l'Ether – la deuxième cryptomonnaie la plus importante en termes d'actifs – devrait remplacer cette année son mécanisme de validation. Plutôt que d'utiliser la preuve de travail comme le Bitcoin, l'Ether utilisera un mécanisme nommé *preuve d'enjeu* (*proof of stake*). Dans ce mécanisme, le mineur ne doit pas résoudre un problème mathématique complexe à haute consommation énergétique, mais plutôt présenter une certaine quantité de cryptomonnaie en dépôt. Le mineur peut alors valider la transaction à l'aide d'une tâche simple et récupérer son dépôt ainsi qu'une rémunération supplémentaire sous forme de nouvelles pièces d'Ether. Toutefois, si une tentative de fraude de la part du mineur est détectée, celui-ci perd son dépôt.

La présence d'autres cryptomonnaies s'explique aussi par les fonctionnalités supplémentaires. Plusieurs actifs numériques permettent d'implémenter des *contrats intelligents*, c'est-à-dire des transactions qui sont programmées pour s'exécuter automatiquement dès que certaines conditions sont remplies.

Conclusion

En résumé, les actifs numériques, dont les cryptomonnaies sont les composantes les plus connues, sont nés d'un désir d'améliorer l'efficacité des transactions entre les individus en décentralisant les bases de données. Pour garantir l'intégrité du réseau, deux composantes sont nécessaires.

Premièrement, il faut une série d'étapes mathématiques permettant de prouver l'identité de l'auteur d'une transaction. Deuxièmement,

[4] En date du 1 juin 2022, un bitcoin s'échangeait contre environ 40 000 dollars canadiens.

l'historique des transactions, la chaîne de blocs, doit être partagé par tous les membres du réseau. Ce registre est mis à jour par un mécanisme de validation qui peut prendre la forme d'une preuve de travail ou une preuve d'enjeu. C'est cette deuxième composante qui est la principale innovation associée aux actifs numériques. En effet, la chaîne de blocs est perçue par certains comme une technologie pouvant avoir des impacts majeurs dans plusieurs domaines.

Bien qu'il y ait désormais une grande variété de réseaux avec divers mécanismes et actifs numériques associés, leurs caractéristiques par rapport aux systèmes conventionnels se résument généralement en trois catégories: (1) la capacité de régler rapidement et à moindre coût des transactions complexes; (2) la rareté numérique; (3) la possibilité de créer des contrats intelligents. Ces caractéristiques permettent de se pencher sur l'évaluation de la valeur fondamentale. Ce sujet sera abordé dans le prochain rapport stratégique dédié aux actifs numériques.

Bureau du chef des placements
CIO-Office@nbc.ca

Martin Lefebvre
Chef des placements
martin.lefebvre@bnc.ca

Louis Lajoie
Directeur
Stratégie d'investissement
louis.lajoie@bnc.ca

Simon-Carl Dunberry
Directeur
Stratégie de portefeuille
simon-carl.dunberry@bnc.ca

Nicolas Charlton
Associé
Stratégie quantitative
nicolas.charlton@bnc.ca

Mikhael Deutsch-Heng
Associé
Stratégie d'investissement
mikhael.deutschheng@bnc.ca

Zaid Shoufan
Associé
Stratégie de portefeuille
zaid.shoufan@bnc.ca

Christophe Faucher-Courchesne
Associé
Stratégie quantitative
christophe.faucher-courchesne@bnc.ca

Général

Le présent document a été élaboré par Banque Nationale Investissements inc. (BNI), filiale en propriété exclusive de la Banque Nationale du Canada. La Banque Nationale du Canada est une société ouverte inscrite à la cote de la Bourse de Toronto (TSX : NA).

Les renseignements et les données fournis dans le présent document, y compris ceux fournis par des tiers, sont considérés exacts au moment de leur impression et ont été obtenus de sources que nous avons jugées fiables. Nous nous réservons le droit de les modifier sans préavis. Ces renseignements et données vous sont fournis à titre informatif uniquement. Aucune représentation ni garantie, explicite ou implicite, n'est faite quant à l'exactitude, la qualité et le caractère complet de ces renseignements et de ces données. Les opinions exprimées ne doivent pas être interprétées comme une sollicitation ou une offre visant l'achat ou la vente des parts mentionnées aux présentes et ne devraient pas être considérées comme une recommandation. Les points de vue exprimés ne visent pas à prodiguer des conseils de placement ni à faire la promotion de placements en particulier et aucune prise de décision de placements ne devrait reposer sur ces derniers. Banque Nationale Investissements inc. a pris les moyens nécessaires afin de s'assurer de la qualité et de l'exactitude des informations contenues aux présentes à la date de la publication. Cependant, Banque Nationale Investissements inc. ne garantit ni l'exactitude, ni l'exhaustivité de cette information et cette communication ne crée aucune obligation légale ou contractuelle pour Banque Nationale Investissements inc.

BNI ou ses sociétés affiliées peuvent intervenir comme conseillers financiers, placeurs pour compte ou preneurs fermes pour certains émetteurs mentionnés dans les présentes et recevoir une rémunération pour ces services. De plus, BNI et ses sociétés affiliées, leurs dirigeants, administrateurs, représentants ou adjoints peuvent détenir une position sur les titres mentionnés dans les présentes et effectuer des achats ou des ventes de ces titres à l'occasion, sur les marchés publics ou autrement.

Le présent document ne peut être distribué qu'au Canada et qu'aux résidents du Canada que dans les cas permis par la loi applicable. Le présent document ne s'adresse pas à vous si BNI ou toute société affiliée distribuant le présent document fait l'objet d'interdiction ou de restriction de le mettre à votre disposition par quelque loi ou règlement que ce soit dans quelque territoire que ce soit. Avant de lire le présent document, vous devriez vous assurer que BNI a l'autorisation de vous le fournir en vertu des lois et règlements en vigueur.

Un placement dans un fonds d'investissement (« Fonds ») peut donner lieu à des frais de courtage, des commissions de suivi, des frais de gestion et d'autres frais. Veuillez lire le prospectus des Fonds avant de faire un placement. Les titres des Fonds ne sont pas assurés par la Société d'assurance-dépôts du Canada ni par un autre organisme public d'assurance-dépôts. Les Fonds ne sont pas garantis, leur valeur fluctue souvent et leur rendement passé n'est pas indicatif de leur rendement dans l'avenir.