CRYPTOMONNAIES et BLOCKCHAIN

Innovations – Open and user innovations

Résumé (abstract)

Après la crise des subprimes, de nombreuses voix se sont élevées pour dénoncer la responsabilité des institutions bancaires et financières lors de cette période. En réponse à cela, un homme dénommé Satoshi Nakamoto, s'est servi d'une technologie appelée blockchain pour créer une monnaie virtuelle, une cryptomonnaie, dont l'essor se fait aujourd'hui sentir : le Bitcoin. La création de cette monnaie, si on peut l'appeler comme telle, avait un objectif clairement défini. Il fallait que le pouvoir qu'octroie le contrôle de la monnaie ne soit plus entre les mains des banques mais entre celles de chaque individu possédant cette monnaie. Depuis 2010 et dans le sillage du Bitcoin, de nombreuses autres cryptomonnaies furent crées. Mais ces monnaies décentralisées suscitent de nombreuses questions quant à leur régulation, leur réglementation, ou alors leurs usages inappropriés. Cette innovation, reposant sur la volonté de pouvoir se passer de tout intermédiaire conventionnel, se retrouve de plus en plus prisée par grandes institutions traditionnelles. Ainsi, ces monnaies créées par et pour les utilisateurs pour ôter le pouvoir qu'octroie le contrôle de l'argent aux institutions politiques, financières et bancaires ne seraient-elles pas maintenant la chasse gardée d'une élite technologique et, à nouveau, financière ?

Technologie – Cryptomonnaies – Blockchain – Innovation de rupture – Innovation ouverte – Décentralisation – Révolution – Bitcoin – Régulation

Table des matières

Introduction générale

Les cryptomonnaies, à l'origine, furent crées à cause de la responsabilité des institutions bancaires et financières dans la crise de 2007. L'impopularité des banques depuis a ensuite permis l'essor des cryptomonnaies grâce à une technologie révolutionnaire : la blockchain.

Mais que signifie les termes cryptomonnaie et blockchain ?

Il nous faut d'abord définir le terme « cryptographie » qui nous permettra ensuite de définir la cryptomonnaie de manière précise.
De manière générale, la cryptographie est une technique d'écriture qui vise à rédiger un message crypté, via l'utilisation de codes secrets ou de clés de décryptage. La cryptographie est principalement utilisée pour protéger un message jugé confidentiel. On l'emploie dans des domaines très divers, comme le monde militaire, l'informatique, la protection de la vie privée, etc.
Il existe de nombreux algorithmes de cryptographie « qui permettent de coder (et de décoder pour le destinataire) le message. Certains sont considérés comme basiques (on décale par exemple la lettre de l'alphabet d'un nombre déterminé de rang vers la droite ou vers la gauche), d'autres proposent un niveau de sécurité presque absolu. »[1]
Ainsi, la cryptomonnaie ou monnaie cryptographique est une monnaie 100 % électronique et magnétique.
Sa valeur fluctue en fonction de l'offre et de la demande et certaines sont utilisables pour réaliser divers achats ou opérations.
La cryptomonnaie s'échange de personne à personne (particulier ou entreprise) sur internet contre d'autres devises monétaires (euro, dollar, yen…) c'est-à-dire en dehors des réseaux bancaires traditionnels. La crypto-monnaie a été créée à partir de la technologie informatique appelée blockchain. Il s'agit d'une technologie de stockage et de transmission d'informations sécurisées.
Elle s'apparente à un immense registre virtuel public et anonyme regroupant toutes les transactions effectuées par des utilisateurs.
Plus précisément, c'est *« un fichier informatique composé de pages (ou blocs) ordonnées, Page 0, Page 1, ..., Page n, évoluant par addition de nouvelles pages, une à une, sans que ne s'opère jamais aucun retrait, effacement ou modification. Ce fichier, concaténation dans l'ordre de toutes les pages, [Page 0, ..., Page n] à l'instant n, est le fichier blockchain. Chaque page du fichier blockchain est en partie constituée de transactions, c'est-à-dire de séquences d'informations — des chaînes de caractères — qui*

[1] D'après Lejournaldunet

ont circulé sur le réseau blockchain {et ont été certifiées par les mineurs}. Ces transactions respectent un certain format et suivent certaines règles de construction. Le respect du format et des règles est contrôlé par chaque nœud du réseau blockchain à chaque fois qu'il reçoit une transaction. »[2]

Pour vérifier les informations émises par la blockchain, des « mineurs » emploient leur matériel informatique pour résoudre des algorithmes extrêmement complexes pour certifier ces informations. Pour les récompenser, des tokens que l'on peut assimiler à des jetons numériques de chaque cryptomonnaie leur sont attribués. Or avec l'essor de cette technologie, la quantité d'informations à traiter est de plus en plus importante et par conséquent, les moyens matériels pour miner sont de plus en plus coûteux et énergivore. On remarque ici à l'une des premières impasses liées aux cryptomonnaies : elles semblent réservées aux personnes ayant les moyens et les connaissances technologiques nécessaires à son exploitation. Ce problème nous renvoie à vers une seconde impasse : les entités les plus à même de posséder les moyens matériels, financiers et intellectuels pour exploiter des cryptomonnaies semblent être les banques et autres institutions financières classiques. Autrement dit, d'ici quelques années, les cryptomonnaies crées par et pour des personnes lambda désireuses d'avoir un contrôle direct sur leur argent pourraient se retrouver sous le contrôle des institutions qu'elles combattaient à l'origine. D'autant plus que ces monnaies étant décentralisées, leur valeur ne peut, pour l'instant, être régulée par des mesures gouvernementales. Leur valeur ne repose en effet que sur l'estimation, l'offre et la demande qu'en font leurs utilisateurs. Dès lors, il est certain que les institutions politiques ne peuvent conserver dans leur environnement un tel électron libre qui pourrait potentiellement déstabiliser tout un système. Plusieurs tentatives de régulations ont-été émises mais aucune n'est aujourd'hui réellement parvenu à réglementer cette technologie.

La question de recherche est donc la suivante : Cette innovation technologique sera-t-elle prise dans un cercle vicieux qui la positionnera sous l'égide des institutions qu'elle tentait de fuir, ou pourrait-elle parvenir à s'en émanciper et à révolutionner un système économique et bancaire dont beaucoup doute ?

Dans notre recherche, la difficulté, mais aussi l'opportunité, aura principalement été de trouver des articles pertinents sur une thématique au final extrêmement récente, dont la littérature n'était pas nécessairement abondante. Nous sommes finalement parvenus à progresser vis-à-vis de notre question de recherche dans le sens où une réponse semble se dessiner. Cependant il est important de mentionner que le sujet évolue plus rapidement que jamais ces derniers temps. Dès lors, même si

[2] D'après Jean-Paul Delahaye pour Scilogs

notre réponse s'appuie sur plusieurs éléments de recherche, celle-ci ne représente en aucun cas une certitude.

Ainsi, comme vous le découvrirez rapidement, la tendance semble être pour le moment toujours en faveur des cryptomonnaies grâce à la ferveur qui entoure le phénomène, mais aussi à leur technologie que peu sont en mesure de réellement comprendre et donc de réguler. Une régulation qui nécessiterait par ailleurs un consensus international qui est loin d'être acquis. C'est cependant dans ce sens que se réunissent les puissances du G20, en Avril prochain. Ils y débattront pour la première fois de la position officielle à adopter face aux cryptomonnaies.

Glossaire : quelques outils de compréhension

Bitcoin (BTC) : monnaie électronique décentralisée conçue en 2009 par un développeur non identifié utilisant le pseudonyme Satoshi Nakamoto.

Blockchain : la blockchain est une technologie de stockage et de transmission d'informations à coût minime, sécurisée, transparente, et fonctionnant sans organe central de contrôle.
Par extension, une blockchain (littéralement une « chaîne de blocs ») désigne une base de données sécurisée et distribuée (car partagée par ses différents utilisateurs), contenant un ensemble de transactions dont chacun peut vérifier la validité. Une blockchain peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable.

Cryptomonnaie : monnaie électronique et peer-to-peer, se basant sur les principes de la cryptographie pour valider les transactions et la génération de la monnaie elle-même.

Peer to peer : de pair à pair, sans tiers ou intermédiaire

Ethereum : plateforme décentralisée, basée sur une blockchain, permettant à son réseau d'utilisateurs de créer des smart contracts. La blockchain d'Ethereum fonctionne avec la monnaie Ether. Contrairement à la blockchain du bitcoin, focalisée sur l'aspect monétaire, la blockchain d'Ethereum a vocation à accueillir des programmes très divers, qui sortent du cadre purement monétaire.

Smart contract : "contrat intelligent". Les smart contracts sont des programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

Microtransaction : transaction de quelques centimes. Dans un circuit "classique", via une banque par exemple, les micro-transactions sont trop coûteuses à réaliser (les frais sont en effet supérieurs au montant des transactions). La blockchain apporte une solution à ce problème.

Minage : utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés.

Mineur : personnes (particuliers ou sociétés) qui connectent sur le réseau une ou plusieurs machines équipées pour effectuer du minage. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau.

Proof of work : "preuve de travail" ou "preuve de calcul". Il s'agit du traitement cryptographique permettant la validation des blocs de transactions. Effectuer ce traitement requiert du temps de calcul : en général, un seul ordinateur du réseau y parvient en environ dix minutes. La difficulté est régulièrement adaptée pour maintenir cet intervalle.

La blockchain, par le biais des cryptomonnaies, c'est la fin des tiers de confiance. C'est un système en peer-to-peer où les ordinateurs des pairs communiquent entre eux pour se partager des fichiers, se répartir des calculs et créer une base de données communes d'eux-mêmes, sans la moindre institution externe. C'est bien l'ensemble de la communauté qui s'occupe des transactions. Ainsi, les cryptomonnaies s'affranchissent des règles bancaires en vigueur tout en étant très sécurisées car il est impossible de modifier une transaction une fois faite (pas de parties lésées à la suite d'un contrat de vente) et le serveur d'horodatage (enregistrement de la date et de l'heure) empêche l'utilisation simultanée d'un bitcoin vers deux directions ou adresses différentes.