2

L'écosystème des cryptomonnaies

Qu'est-ce qu'une cryptomonnaie ?

Une cryptomonnaie, ou monnaie cryptographique, monnaie numérique ou encore monnaie virtuelle (dénomination *a priori* péjorative), est une monnaie dont le fonctionnement et la sécurité sont fondés sur la cryptographie.

Elle remplit les trois fonctions essentielles de la monnaie :

- une réserve de valeur : quand je possède un bitcoin, je possède de la valeur car je peux la vendre ou l'échanger ;
- une unité de compte permettant le calcul économique ou la comptabilité : on peut déjà acheter certains produits ou services avec des cryptomonnaies, des bitcoins notamment ;
- un intermédiaire : les cryptomonnaies sont faites pour être échangées, pour le moment essentiellement à des fins de spéculation, et sur des places de marché particulières.

Le fonctionnement et la sécurité d'une cryptomonnaie s'appuient sur la cryptographie asymétrique.

Les cryptomonnaies sont régies par un protocole qui définit des fonctions cryptographiques permettant l'échange de la monnaie dans un réseau mondial sécurisé et sans contrôle. Contrairement aux monnaies fiduciaires (euro, dollar, won, etc.), une monnaie cryptographique n'est

pas nécessairement créée par une banque centrale à l'initiative d'un État ou d'un groupe d'États, mais peut l'être par un ou des individus, une organisation ou une entreprise, avec presque toujours la décentralisation comme principe de fonctionnement. Une cryptomonnaie n'existe que sous forme électronique et n'est pas rattachée à un territoire.

La plus connue des cryptomonnaies est le bitcoin, qui a lancé le mouvement en 2009 en introduisant la technologie de la blockchain. Toutes les cryptomonnaies se distinguent les unes des autres essentiellement par leur valeur (déterminée par la loi de l'offre et de la demande et relativement volatile), leur rythme de création (de nouvelles unités monétaires sont créées à une fréquence prédéfinie), le fonctionnement de leur blockchain et leur projet.

Chaque cryptomonnaie est utilisable sur un réseau informatique et est caractérisée par un symbole (ticker) généralement de trois lettres majuscules (BTC pour bitcoin). La cryptomonnaie est couplée à un système de paiement qui permet de régler des transactions de pair à pair. Elle a un fonctionnement décentralisé (sauf rares exceptions) et est régie par un protocole initial qui stipule le rythme et les règles de création et d'attribution de nouveaux coins.

À noter que vous verrez apparaître de plus en plus le terme « crypto-actif » (*cryptoasset* en anglais). Ce terme donne une dimension plus grande aux cryptomonnaies. La plupart n'ont pas pour but d'être simplement une monnaie. Elles constituent à la fois un actif financier reflétant la valeur de la société émettrice et un outil permettant d'utiliser un service, comme un réseau d'ordinateurs pour faire tourner des contrats intelligents. Je continuerai à utiliser le terme « cryptomonnaie » par souci de simplification.

Résumé

- Les cryptomonnaies sont des monnaies dématérialisées dont le fonctionnement est décentralisé et basé sur la cryptographie asymétrique.
- Elles n'ont pas besoin d'un État ou d'une quelconque autorité régalienne pour être émises et ne sont pas encore reconnues par les grands États comme des moyens de paiement légaux.
- Leur valeur est déterminée uniquement par la loi de l'offre et de la demande.
- Elles remplissent les rôles d'une monnaie et sont toujours couplées à un système de paiement.

Le bitcoin

Origines

Nous l'avons vu, les cryptomonnaies sont à la fois des monnaies et des systèmes de paiement. Cependant, les deux n'ont pas forcément le même nom. Avec le bitcoin, la différence est assez subtile : le bitcoin est une cryptomonnaie et le Bitcoin un système de paiement. C'est la première cryptomonnaie à avoir été créée (fin 2008) et la plus emblématique. C'est elle qui a introduit le principe du paiement de pair à pair sans organe de contrôle ni système centralisé (autrement dit sans banque ni compte en banque), mais aussi la technologie de la blockchain et l'algorithme de consensus « Proof of Work », repris par de nombreuses cryptomonnaies. Elle représente à elle seule plus de 40 % de la capitalisation boursière des cryptomonnaies (en avril 2018). Initialement, le bitcoin se voulait être LA monnaie numérique (digital cash) et le Bitcoin un système de paiement

rapide, peu onéreux, efficace, anonyme, décentralisé et modulable, mais d'autres monnaies remplissent ces fonctions mieux qu'elle, si bien qu'elle s'est trouvée une autre vocation.

Le bitcoin a été créée par une personne, un groupe de personnes ou une entité dénommée « Satoshi Nakamoto » fin 2008. Même s'il y a de nombreuses rumeurs qui circulent sur la véritable identité de ce Satoshi Nakamoto, personne (ou presque !) ne sait qui est ce mystérieux personnage, qui pourrait être décédé ou être en fait un groupe de personnes. Le fait que son nom soit typiquement japonais explique peut-être le succès du bitcoin et des cryptomonnaies dans ce pays. Ce qu'on sait en revanche, c'est que ce Satoshi Nakamoto a miné les premiers bitcoins pendant presque deux ans et qu'il en détiendrait environ un million, ce qui fait de lui, au cours actuel, un homme très riche. L'activité du wallet bitcoin de Satoshi Nakamoto est suivie de près par plusieurs personnes ; il continuerait à être alimenté en bitcoins mais aucune n'en sort…

Apports du bitcoin

Le succès du bitcoin tient au fait que c'est la première cryptomonnaie à avoir vu le jour : elle a apporté la technologie de la blockchain et le concept même de cryptomonnaie. Aujourd'hui, le bitcoin est la monnaie des cryptomonnaies : toutes les autres cryptomonnaies sont cotées en bitcoin, et vous finirez par avoir du bitcoin entre les mains à un moment ou un autre si vous voulez acheter d'autres cryptomonnaies. Le bitcoin est la porte d'entrée vers le trading de cryptomonnaies. Du fait de sa célébrité et de son poids financier (plus de 40 % de la capitalisation boursière des cryptomonnaies à elle seule en mai 2018), c'est la monnaie que regardent tous les investisseurs, notamment professionnels, et c'est donc elle qui donne la tendance du marché. Le « Quand le bâtiment va, tout va » de l'économie traditionnelle devient, dans le monde des cryptomonnaies : « Quand le bitcoin va, tout va ». Et inversement. Enfin, le bitcoin est la cryptomonnaie aujourd'hui la plus acceptée par les commerces en ligne et hors ligne. C'est celle qui compte le plus de distributeurs physiques (avec des billets de banque ou carte bancaire), notamment en Asie et en Amérique du Nord.

Le système de paiement Bitcoin a apporté la blockchain et l'algorithme « Proof of Work ». Le Proof of Work, qui permet de parvenir à un consensus sur la blockchain du bitcoin (sur les transactions qui ont bien eu lieu), nécessite des investissements en informatique et des consommations d'électricité phénoménales, ce qui fait l'objet de critiques. En 2018, l'équivalent de la consommation électrique de la Serbie (plus de sept millions d'habitants) est nécessaire pour « miner » le bitcoin et cette consommation a tendance à croître rapidement car, plus vous investissez en matériel informatique et consommez d'électricité, plus vous avez de chances de recevoir des bitcoins pour votre contribution au système.

Limites du bitcoin

Le bitcoin n'est cependant pas, et encore loin d'être, une monnaie utilisée dans la vie de tous les jours pour plusieurs raisons :

- il n'a de cadre légal pour être utilisé comme moyen de paiement dans aucun pays pour le moment ;
- son utilisation pose des problèmes de sécurité ;
- les transactions peuvent durer plusieurs minutes (plusieurs dizaines de minutes fin 2017) ;
- son prix est hautement volatile ;
- ses frais de transaction sont relativement élevés ;
- les systèmes centralisés (banques, cartes de crédit, Paypal…) sont aujourd'hui la norme. Ils proposent des systèmes de protection et de recours relativement efficaces, ont des interfaces pratiques et agréables, des moyens d'innover et de garder une longueur d'avance sur les systèmes décentralisés tels Bitcoin ;
- les entreprises et les commerçants ont besoin de temps pour comprendre et adopter le système.

En outre, comparé à ceux des autres cryptomonnaies, le système Bitcoin est :

- relativement cher, ce qui empêche son utilisation pour des produits ou services de la vie de tous les jours ;

– relativement lent, car le nombre de transactions est limité à environ 200 par minute, insuffisant pour faire du Bitcoin un système de paiement mondial ;
– de moins en moins décentralisé, puisque les cinq plus grands pools de miners représentent les trois quarts de la création de blocs ;
– peu modulable : le nombre de transactions et la taille des blocs sont limités, et la communauté du bitcoin préfère laisser les mécontents faire des hard forks plutôt que changer ces règles ;
– pas forcément anonyme, surtout si vous laissez vos bitcoins sur des exchanges.

Les limitations du système Bitcoin sont en revanche une aubaine pour les créateurs des autres monnaies, qui, chacune à sa manière, apportent des solutions aux défauts de ce système. Litecoin ou Zcash, par exemple, permettent de réaliser des transactions rapidement pour des coûts raisonnables dans le but de détrôner le bitcoin comme monnaie numérique de référence. Monero garantit un plus grand anonymat. Nous le verrons plus tard, la plupart des autres monnaies cryptographiques ne cherchent pas à remplacer le bitcoin. Plusieurs d'entre elles innovent dans leur projet, le fonctionnement de leur blockchain et le degré de décentralisation.

Une monnaie anonyme ?

Contrairement à ce que l'on peut lire ici et là, le bitcoin n'est pas une monnaie anonyme, bien au contraire, sans quoi il n'y aurait pas autant de coins qui mettent l'accent sur l'anonymat. N'importe qui peut suivre l'historique de n'importe quelle transaction en bitcoin (par exemple sur blockchain.info) s'il possède une transaction ID (numéro de transaction) ou une public address (numéro de compte). Il obtiendra des données comme le montant de bitcoin échangé, la public address de la personne qui a reçu ou émis ce montant, le moment où la transaction a eu lieu, etc.

Savoir quelle public address a échangé de l'argent avec une autre que vous connaissez déjà ne vous servira à rien, si vous ne savez pas qui la contrôle. La traçabilité des transactions en bitcoin passe donc par

l'identification des détenteurs de public addresses et les *exchanges* ont ici un rôle important à jouer.

Le Lightning network

Le Lightning network est un protocole de paiement « deuxième couche » qui fonctionne parallèlement à une blockchain (notamment celle de Bitcoin). Il permet des transactions instantanées entre les participants, une solution au problème de scalabilité de Bitcoin. Il propose un système peer-to-peer pour effectuer des micropaiements en cryptomonnaie à travers un réseau de canaux bilatéraux parallèle à la blockchain, tout en maintenant la confiance dans le système afin que deux participants qui ne se connaissent pas puissent s'échanger des fonds en toute sécurité. Il permet d'augmenter la capacité de transactions d'une blockchain tout en maintenant la sécurité de celles-ci. Le Lightning network est actuellement testé sur la blockchain de Bitcoin et semble tenir ses promesses. Il y aurait un millier de participants et une quinzaine de bitcoins sur ce réseau parallèle mi-mai 2018.

Résumé

- Le bitcoin est la première cryptomonnaie à avoir vu le jour en 2009 et le Bitcoin est le système de paiement qui lui est associé.
- Le bitcoin a apporté la technologie de la blockchain et l'algorithme de consensus « Proof of Work », très énergivore.
- Le bitcoin est, plus que toute monnaie fiduciaire, la monnaie de référence pour les investisseurs et le trading de cryptomonnaies : c'est LA monnaie des cryptomonnaies.
- Le bitcoin est largement critiqué car il nécessite des consommations d'électricité phénoménales pour être « miné » et que son système est menacé par la centralisation.

Ethereum

Description

Ethereum est un protocole d'échanges décentralisés de données créé en 2015, ayant pour monnaie l'ether (symbole : ETH), la deuxième monnaie après le bitcoin en terme de capitalisation. Ethereum est tellement différent de ce que propose Bitcoin que ces deux entités illustrent à elles seules la diversité des cryptomonnaies. Le projet d'Ethereum, comme celui de Stratis, Neo, Golem ou EOS, est de créer un « super ordinateur » hyper puissant, toujours en ligne et « invincible », fait de millions d'ordinateurs reliés entre eux grâce à Internet et au protocole Ethereum. Il permet de tester et d'héberger des applications appelées « dapps », basées sur des contrats intelligents et d'effectuer des transactions.

Caractéristiques principales d'Ethereum :

- L'EVM (Ethereum Virtual Machine) est le réseau d'ordinateurs qui constitue le réseau Ethereum en stockant ou transférant des données et en effectuant des calculs.
- La première fonctionnalité principale offerte aux utilisateurs de l'EVM est la création de contrats intelligents qui permettent d'automatiser, en grande partie ou en totalité, des contrats et applications comme des paiements avec contrepartie par exemple. Ces contrats sont écrits dans un langage propre à Ethereum : Solidity.
- La seconde fonctionnalité principale est la mise à disposition de la capacité de stockage et la puissance de calcul du réseau d'ordinateurs à des développeurs de dapps (applications décentralisées). La promesse d'Ethereum est que les applications que vous y hébergez sont invincibles car disséminées sur des ordinateurs répartis sur toute la planète reliés entre eux, et pas sur un serveur central contrôlé par une autorité centrale comme Amazon ou Microsoft.
- La blockchain Ethereum fonctionne avec un algorithme de consensus PoW, qui devrait changer prochainement.
- L'ether, avant d'être la deuxième cryptomonnaie en terme de capitalisation et un vecteur de spéculation majeur dans le marché des

cryptomonnaies, est « le carburant » qui permet d'utiliser ce réseau pour faire tourner des contrats intelligents (simple transfert d'ether ou base d'une application). Donc, dès que j'utilise Ethereum pour faire tourner des contrats intelligents, c'est-à-dire dès que je demande aux mineurs d'effectuer des changements pour moi sur la blockchain Ethereum, je dois les payer en « gas » libellé en ethers et qui évolue en fonction de la loi de l'offre et de la demande.

Ethereum a lancé la blockchain 2.0, une blockchain non seulement capable d'effectuer des transactions, c'est-à-dire des transferts de valeurs entre public addresses, mais aussi de gérer et stocker des contrats intelligents et des données, et d'effectuer des calculs. Si la blockchain 1.0, inaugurée par le bitcoin, est un registre distribué, la blockchain 2.0, initiée par Ethereum, est un registre distribué programmable. C'est devenu un « lieu » incontournable pour tout développeur qui s'intéresse à la blockchain, aux contrats intelligents et aux dapps. Des tokens spécifiques sont inventés au fur et à mesure, comme le ERC20 qui permet de créer de nouvelles monnaies basées sur la blockchain Ethereum, ce que la majorité des monnaies créées *via* des ICO utilisent, ou le ERC777 qui permet de mettre en place des votes ou referendums.

La blockchain Ethereum est un « couteau suisse » très performant avec 18 000 mineurs et de nombreuses applications : elle devient un véritable laboratoire pour les cryptomonnaies. La communauté Ethereum, très internationale et active, se réunit régulièrement lors de conférences comme celle qui a eu lieu au CNAM à Paris du 8 au 10 mars 2018 et à laquelle Vitalik Buterin, créateur d'Ethereum, a assisté. Un des événements importants de 2018 devrait être le passage de la blockchain Ethereum à PoS, contribuant à la réduction des dépenses d'énergie et montrant peut-être la voie à Bitcoin.

Analyse SWOT d'Ethereum

Les principaux avantages d'Ethereum sont :

- ses applications, très nombreuses grâce aux systèmes des contrats intelligents et des tokens spécifiques ;
- la taille de son réseau avec ses 18 000 mineurs et ses centaines de milliers d'ordinateurs ;
- le nombre important de bons développeurs qui créent des contrats intelligents sur Ethereum.

Les principaux désavantages sont :

- la place de son créateur, le jeune Vitalik Buterin, qui fait la pluie et le beau temps dans le développement d'Ethereum ;
- l'extensibilité de la blockchain Ethereum : elle peut gérer moins de 20 instances (transactions) quand Facebook gère près de 200 000 requêtes par seconde. La blockchain Ethereum a déjà du mal à faire face à l'afflux de projets et tokens utilisant son réseau et aura *a fortiori* encore plus de mal à l'avenir étant donné l'engouement pour ce protocole ;
- les frais, qui ont tendance à augmenter au fur et à mesure de la hausse du cours de l'ether (passé d'environ 8 $ début 2017 à plus de 1 000 $ fin 2017).

Ses opportunités principales sont :

- le renforcement de son rôle de laboratoire et de figure de proue des applications de contrats intelligents dans le monde réel, avec un puissant réseau ;
- la venue de mineurs et développeurs nombreux et capables, renforçant sa capacité de développement et son rôle de pionnier ;
- le développement de la capacité de calcul du réseau, afin de mettre en place des applications fiables au niveau mondial.

Ses principales menaces sont :

– l'ether est bien parti pour continuer à monter, et la blockchain Ethereum à attirer de nombreux projets, pouvant en faire une plateforme de développement et d'hébergement de contrats intelligents ;
– la caractérisation d'ether comme titre financier par des autorités de Bourse, qui pourrait affecter le développement d'Ethereum, même si cette caractérisation a été rejetée par l'autorité de la Bourse américaine (SEC) ;
– Ethereum a des concurrents (ex. : Neo et EOS) qui pourraient lui voler la vedette en proposant des frais moins élevés ou de nouvelles fonctionnalités.

Résumé

- Ethereum est un protocole informatique visant à mettre à disposition un « super ordinateur » nommé *Ethereum Virtual Machine* (EVM), formé de millions d'ordinateurs reliés en réseau permettant de faire tourner des applications basées sur des contrats intelligents, sans interruption et de manière décentralisée.
- La monnaie d'Ethereum est l'ether, la deuxième plus grande capitalisation après Bitcoin et la deuxième monnaie universelle du monde des cryptomonnaies.
- La blockchain Ethereum est celle qui est la plus utilisée pour lancer de nouvelles monnaies *via* des ICO.
- Bénéficiant d'une communauté très active et riche en talents et en nombre de développeurs et de mineurs, Ethereum est le véritable laboratoire des applications des cryptomonnaies.