

Bitcoins, blockchains et ICO's... Inconnus? Mal aimés? Ou très populaires?

Au cours de ces derniers mois, la presse a relayé le phénomène des «crypto-devises» et de la technologie «blockchain». Succès oblige, on assiste aujourd'hui à une flambée des cours tant pour ces devises que pour les entreprises actives dans ce secteur. Bref aperçu.

Crypto-devises?

Ces crypto-devises (en anglais: cryptocurrency) diffèrent des devises traditionnelles par le fait qu'elles ne sont pas émises ou contrôlées par une instance publique. Ce sont des unités monétaires numériques, basées sur la cryptographie (d'où leur nom de «crypto» devises) ou sur des mécanismes de verrouillage*.

Il est toujours possible de créer une crypto-devise. La façon de procéder varie en fonction du type de crypto-devise. Dans le cas du bitcoin, cela se fait, par exemple, en validant des transactions via la résolution d'algorithmes mathématiques complexes par des ordinateurs spécifiquement conçus à cette fin. Chaque validation est rétribuée par une fraction de bitcoin. Les nouvelles unités de crypto-monnaie sont créées en programmant un bloc de code sécurisé dans des programmes informatiques spécifiquement conçus à cette fin. Dans ce cadre, le nombre d'unités par devise est souvent limité car, dès que toutes celles-ci ont été programmées, il n'est plus possible d'en ajouter. Dans cette optique, on pourrait comparer les crypto-devises à une réserve d'or déterminée. Un exemple de crypto-monnaie est le bitcoin, qui est limité à 21 millions d'unités. À ce jour, la capitalisation de marché totale de toutes les crypto-devises représente 165 milliards de USD, soit 2% des devises mondiales en circulation.

* Chaque «crypto-monnaie» constitue une partie de code informatique verrouillé dans lequel les transactions sont sauvegardées. Chaque fois qu'une transaction a lieu, elle est vérifiée par un réseau décentralisé d'ordinateurs et verrouillée de cette manière dans un nouveau bloc. Actuellement, un tel bloc de transactions est créé toutes les 10 minutes, ce qui génère une chaîne de blocs. D'où le terme «blockchain».

Blockchain?

Les crypto-devises utilisent la technologie blockchain: des registres numériques ouverts partagés entre les utilisateurs, où les transactions entre 2 parties peuvent être enregistrées et vérifiées par l'ensemble du réseau.

Pour voler 1 unité («coin») d'une crypto-devise, il faut reprogrammer entièrement son historique dans la blockchain. Faute de puissance informatique suffisante, c'est impossible actuellement. Tout comme il n'est pas possible de dissimuler des transactions. De ce fait, des systèmes basés sur la technologie blockchain, comme les crypto-devises, sont transparents et faciles à tracer, ce qui offre des avantages considérables en termes de sécurité.

Grâce à l'utilisation de blockchain, les crypto-devises offrent différents avantages.

- **Lutte contre la fraude:** il est impossible de falsifier des crypto-monnaies, contrairement aux billets de banque. Les banques classiques utilisent une base de données centrale qui, dans le pire scénario, pourrait être «hackée» en dépit des systèmes de sécurité très performants. Avec les crypto-devises, il n'existe pas de base de données centrale, de telle sorte que le système est beaucoup plus difficile à attaquer par des hackers.
- **Protection de l'identité:** les crypto-devises fonctionnent avec un mécanisme «push» qui envoie le montant souhaité. Cela permet un meilleur contrôle que les cartes de crédit, qui fonctionnent avec un mécanisme «pull» (un commerçant impute unilatéralement un montant, qui est retiré de votre compte).
- **Décompte immédiat:** pas besoin d'institutions intermédiaires, qui génèrent des ralentissements et/ou des frais.

La technologie blockchain ne constitue dès lors pas un service ou un produit commercial. Il s'agit d'un protocole pour mener à bien des transactions entre de nombreuses parties sans qu'un intermédiaire central ne soit nécessaire. De ce fait, les réseaux sont décentralisés et les utilisateurs sont propriétaires tant du réseau et des données que des bénéfices (et non des géants de l'internet, comme Facebook ou Amazon). Cette technologie est non seulement pertinente dans le contexte financier, mais elle peut enregistrer tout ce qui a une valeur et qui doit être conservé à long terme: certificats de naissance et de décès, droits de propriété intellectuelle, dossiers médicaux, assurances, titres de propriété, etc. Tout cela peut être converti en code informatique et partagé dans un réseau blockchain, ce qui offre les avantages susmentionnés. Et ce contrairement à la conservation centrale de ces informations, dont il n'existe généralement qu'une seule version sécurisée (ou 1 back-up). Si ces bases de données centrales classiques sont «hackées», ces versions seront perdues. Si on recourt à un réseau blockchain, ce risque est réduit, voire inexistant.

C'est pourquoi 6 des plus grandes banques du monde se sont lancées ces derniers mois dans un projet de blockchain pour accroître la rapidité de traitement des transactions et résoudre les discordances dans les registres d'actionnaires.

Bitcoin?

Il s'agit de la première crypto-monnaie qui ait été conçue. Elle est disponible depuis 2008. L'an dernier, sa valeur a augmenté de 700%, ce qui amène la valeur totale de tous les bitcoins existants à 88 milliards de USD. Les autres crypto-

devises par ordre décroissant de capitalisation de marché sont:

- l'ethereum (28 milliards de USD)
- le ripple (9 milliards de USD)
- le bitcoin cash (8 milliards de USD)

Le bitcoin se base sur la technologie blockchain. Les transactions entre les différentes personnes doivent être vérifiées. Cette opération se fait en résolvant un algorithme mathématique qui demande une énorme puissance de calcul. Actuellement, il existe des milliers d'ordinateurs de par le monde qui ne font rien d'autre que résoudre ces puzzles mathématiques et qui vérifient ainsi les transactions entre les personnes. Celles qui mettent leurs puissants ordinateurs à disposition à cette fin reçoivent une fraction d'un bitcoin à titre de rémunération et sont dénommés «miners». Le «mining» constitue dès lors une part importante et intégrante du bitcoin, qui garantit le déroulement correct et la stabilité et la sécurité du réseau. Par le biais de ces miners, de nouveaux bitcoins sont mis en circulation et ce, à un rythme parfaitement prévisible. D'ici 2140, 99,99% de tous les bitcoins auront été créés, ce qui fait que l'offre est limitée sur le plan mathématique.

Pas sans risque

Le monde des investisseurs suit le bitcoin avec intérêt. Mais aussi avec beaucoup de scepticisme. Dans quelle mesure la devise virtuelle est-elle durable? Les nouvelles technologies pourraient-elles à terme menacer la devise? Vu la structure mathématique de l'exploitation du bitcoin (à l'instar du fonctionnement des systèmes de sécurisation des applications bancaires), on peut supposer que ces systèmes ne sont pas près d'être piratés, même avec la progression de l'intelligence artificielle.

L'inconvénient est la grande volatilité et la faible liquidité, deux phénomènes dont tout investisseur doit tenir compte. Actuellement, le prix du bitcoin est uniquement déterminé par l'offre et la demande. Il n'est dès lors pas question d'une activité économique sous-jacente (p. ex. la croissance d'un pays déterminé) ou d'une matière première (p. ex. l'or ou l'argent). Provisoirement, le bitcoin est surtout utilisé comme instrument pour thésauriser ou spéculer. De même, l'absence de cadre fiscal formel et d'encadrement légal (p. ex. l'absence de prospectus) accroît l'incertitude et l'insécurité de celui-ci.

Il serait prématuré de déjà parler d'une nouvelle catégorie d'investissement. Et bien que des trackers soient déjà disponibles, il ne faut pas oublier la volatilité élevée de ce marché. De même, l'investissement dans des entreprises liées au bitcoin (p. ex. des entreprises actives dans le «mining» des transactions et qui investissent dès lors surtout dans des ordinateurs dotés de puissantes capacités de calcul) est très risqué. En effet, leurs revenus sont liés au prix de marché volatile du bitcoin.

Il est possible d'acheter le bitcoin via internet et mieux vaut le conserver dans un «hardware wallet», une portefeuille numérique physique. Il est également possible de le conserver sur des plateformes intermédiaires en ligne, à condition de faire preuve d'une prudence extrême en termes de sécurité et de conservation. Il n'est actuellement pas encore possible d'acheter des bitcoins par l'intermédiaire de Belfius. De nombreuses questions ouvertes sèment aujourd'hui la confusion. Certains chefs d'entreprises ou régulateurs parlent de fraude, tandis que d'autres sont plus prudents et s'abstiennent de faire des commentaires trop rigoureux. Mais ils étudient tous les phénomènes avec attention.

ICO?

L'objectif des ICO's (Initial Coin Offerings) est identique à celui des recapitalisations classiques par des «venture capitalists» (VC's): récolter des capitaux pour des start-ups ou des entreprises existantes. Mais il existe néanmoins des différences notables:

- Lors d'un appel aux marchés des capitaux, un venture capitalist souscrit aux actions et, avec le produit de la transaction, l'entreprise finance ses activités.
- Avec une ICO, on n'émet pas d'actions, mais bien des tokens, que l'on offre au public en échange de crypto-devises (p. ex. des bitcoins). L'entreprise peut financer ses activités avec les bitcoins, qui ont une valeur monétaire. Et le public reçoit les «tokens», qui augmentent avec la valeur réseau de la technologie inhérente au token.
- Dans le cas d'une ICO, tout le monde a en outre accès au marché et pas uniquement les riches venture capitalists.

De telles ICO's ont déjà récolté 1,8 milliard d'USD auprès de développeurs de logiciels. Elles vont actuellement de pair avec des valorisations beaucoup plus élevées que via la structure classique de venture capitalist. Ce «pari» sur les ICO's pourrait être une conséquence du climat actuel de taux bas et de recherche de rendements plus élevés. Tout comme l'industrie du venture capitalist, les ICO's comportent beaucoup de risques et il faut être prêt à perdre l'entièreté de sa mise.

Actuellement, les obstacles à la création des ICO's sont peu nombreux, parce qu'il suffit de créer un «white paper» (une description sur la manière dont la technologie permet de résoudre un problème spécifique) et un code informatique. Ce seuil bas constitue le principal argument des ICO-bulls: liberté d'investissement et quasi aucune barrière à la récolte de capitaux. Il existe pour le moment plus de 1.100 crypto-devises différentes à vendre.

L'inconvénient est que les ICO's ne sont soumises à aucune forme de réglementation. Alors qu'en cas de faillite, un venture capitalist a droit aux actifs restants, c'est difficile à définir dans le cas d'une ICO. Et cela peut générer des abus. Les

autorités essaient de combler cette «lacune» dans la réglementation. La «Securities and Exchange Commission» aux US est convaincue que de nombreuses ICO's sont dans la pratique assimilées à une forme d'actions ou d'obligations et va essayer de les réglementer en ce sens. Entre-temps, la Chine a interdit ces ICO's et veut interdire toutes les transactions avec des crypto-devises.

Rage financière ou innovation en profondeur?

L'an passé, le bitcoin a fortement augmenté et les crypto-devises avaient généralement des valorisations élevées. Il en va ainsi, par exemple, de la crypto-entreprise «Ripple»: initialement valorisée à 500 millions, ensuite à 35 milliards et enfin, à 19 milliards d'USD. Il n'est pas difficile dans ce cadre de faire le lien avec la dotcom-bubble: des valorisations élevées pour une technologie qui n'a pas (encore) fait ses preuves.

Mais ce qui constitue une innovation en profondeur pour ceux qui y croient représente pour d'autres une façon de créer de la «funny money», car on investit uniquement sur la base de la promesse d'un marché futur. Les autres dangers sont la fraude internet, les phishing scams et le hacking des logiciels sous-jacents.

L'avenir nous le dira.

Sources

To coin a craze (FT big read over cryptocurrencies 14-09-2017)

<https://www.ft.com/content/2b0d8926-96d9-11e7-b83c-9588e51488a0>

In cryptocurrencies, tech and speculation meet (FT 14-09-2017)

<https://www.ft.com/content/83a496fe-995b-11e7-b83c-9588e51488a0>

Blockchain pour débutants

- <https://www.tijd.be/dossier/blockchain/Blockchain-voor-beginners/9930650>
- <http://uk.businessinsider.com/cryptocurrency-market-coin-trends-cap-value-2017-9?r=US&IR=T>
- <https://decentralize.today/5-benefits-of-cryptocurrency-a-new-economy-for-the-future-925747434103>

'Realizing the potential of blockchain' du World Economic Forum

BCA research

You Tube.be / GKC2oell878

Jan Vergote – Head of Investment Strategy
Belfius Banque & Assurances