#

Bitcoins & Blockchains : petits blocs décryptés

#

Cette Lettre Digitale propose une approche de décryptage des Bitcoins et Blockchains : elle ne se veut pas une énième digression sur l'intérêt ou la dangerosité supposés des cryptomonnaies en général et du Bitcoin en particulier ; loin de nous l'idée de contester à Nabila son statut d'experte sur la question ou de commenter la dernière saillie de Warren Buffet ou de Jamie Dimon sur l'éventualité d'un krach à venir… Nous ne chercherons pas plus à deviner qui est Satoshi Nakamoto, l'inventeur réel ou mythifié de l'algorithme sous-tendant le Bitcoin…

La vitesse de développement des cryptomonnaies, les technologies et pratiques qui les permettent ainsi que les révolutions qu'elles annoncent interpellent les investisseurs de la digitalisation que nous sommes. Ces cryptomonnaies ne sont pas seulement les devises de choix du Dark Web ; certains usages, certaines de leurs technologies et de leurs applications se développeront. Toutes les autorités nationales ne suivront pas l'interdiction édictée par les chinois, qui y voient pèle mèle "une incitation à la spéculation pouvant perturber le système financier, un mécanisme de fuite des capitaux et un instrument d'activités criminelles"[1].

Par l'exemple du Bitcoin, dont l'évolution de la valorisation frappe les imaginations, nous traiterons quelques questions usuelles et rappellerons certaines définitions clefs : blockchains, bitcoins, altcoins, tokens, wallets, mining et autres ICO's.

Nous proposerons également quelques pistes de réflexion pour les investisseurs sur :

- les opportunités et risques afférents aux cryptomonnaies et de leurs applications, qu'il s'agisse d'achats de cryptomonnaies – sans évoquer à ce stade leurs dérivés financiers tout juste naissants – ou leur application au crowdfunding : les ICO's
- les opportunités d'investissement sur les technologies sous-jacentes aux cryptomonnaies et les actions de quelques entreprises en pointe sur ces sujets en évolution très rapide.

A bit about Bitcoins…

Le *Bitcoin* est une *cryptomonnaie*, ce qui ne n'est pas nécessairement une monnaie, comme nous le verrons. Le Bitcoin est 100% *numérique* : il n'en existe aucune expression fiduciaire, donc aucune pièce

[1] Source : https://qz.com/1174091/china-wants-an-orderly-exit-from-bitcoin-mining/

ou billet le matérialisant… en dehors d'illustrations d'artistes agrémentant les nombreux articles le concernant.

Le Bitcoin fonctionne en *peer-to-peer*, de manière décentralisée, les transactions se déroulant sans *tiers de confiance*, rôle dévolu à une Banque Centrale – la FED, la BCE, la BoE, etc… – pour "gérer la monnaie d'un pays ou d'un groupe de pays et contrôler la masse monétaire, c'est-à-dire la quantité de monnaie en circulation. Le principal objectif de nombreuses banques centrales est la stabilité des prix. Dans certains pays, elles sont tenues par la loi d'agir en faveur du plein emploi"[2]. Le système est ouvert à tous ceux qui veulent participer, d'où le terme *public* pour le caractériser.

Une transaction de Bitcoins est validée avec l'aide des *miners*, ces derniers gagnant de l'argent en renforçant le système : ils sont parties prenantes du processus de validation d'une transaction, qui consiste en un challenge informatique complexe à résoudre, nommé *mining*. Les gagnants du challenge sont récompensés directement en Bitcoins.

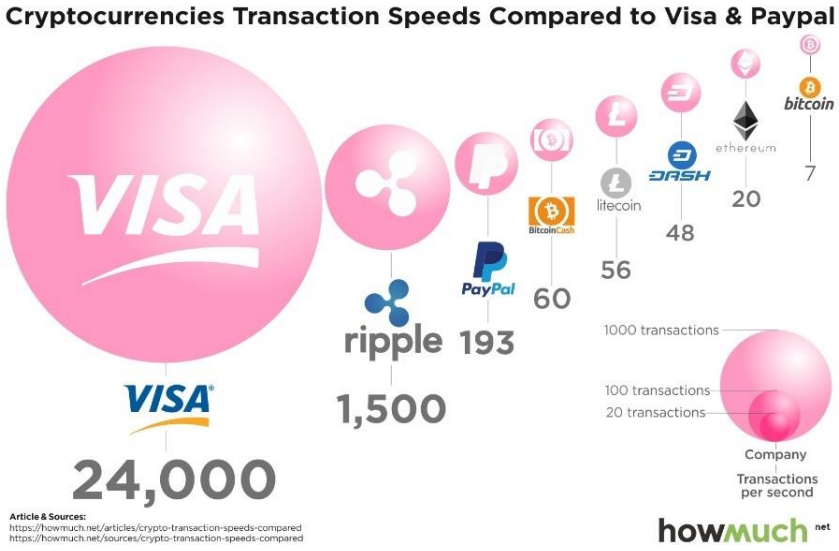
Les transactions sont regroupées et chainées dans ce qu'on appelle une blockchain (littéralement une "chaine de blocs"), assurant la *sécurité* : chaque nouveau maillon (le "bloc") vient se greffer à la chaine déjà existante. Le fait que la chaine, ainsi que le processus d'ajout d'un nouveau maillon, soient visibles par tous à tout moment fait que la "blockchain" est très difficile, voire impossible, à falsifier. L'historique de toutes les transactions est accessible par tous à tout moment, assurant de fait une *traçabilité* totale du système.

Le nombre de Bitcoins émis ou à émettre est limité par construction à 21 millions[3]. L'émission programmée de nouveaux Bitcoins est divisée par deux tous les quatre ans environ, afin que le nombre total de bitcoins converge vers ce chiffre sans pouvoir le dépasser. Cette *rareté* structurellement organisée est un facteur d'appréciation dans le temps. Elle est aussi facteur de *confiance*, laquelle est la base, y compris étymologiquement[4], de tout système fiduciaire… et qui peut parfois manquer justement aux monnaies dites fiduciaires lorsque les autorités monétaires succombent à la tentation de la "planche à billet", sapant la confiance des acteurs économiques dans la monnaie. Le document original décrivant les principes du Bitcoin date de 2008, alors que la confiance dans les banques centrales et le système financier était au plus bas, ce qui explique sans doute sa structure.

A côté du Bitcoin, les "Altcoins"

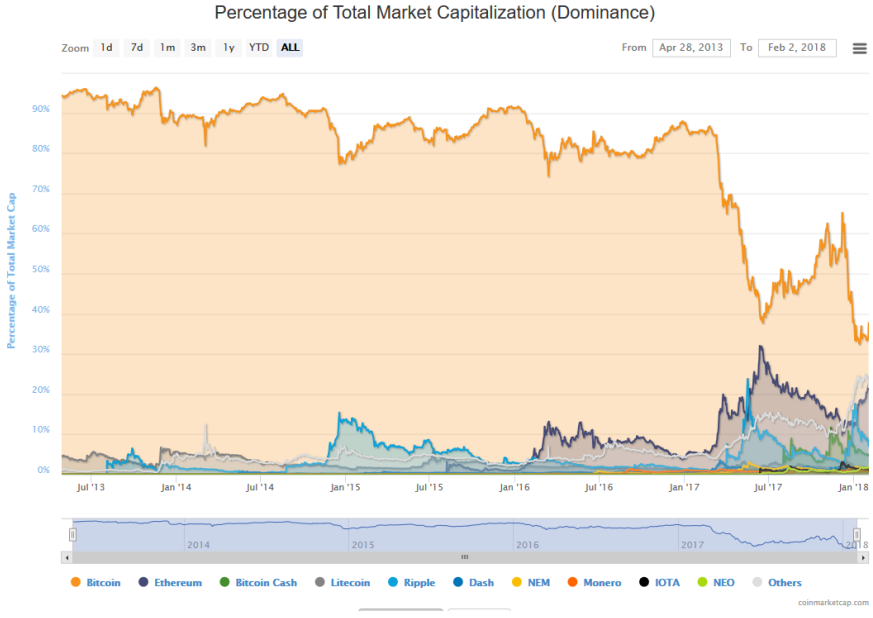
Le Bitcoin n'est pas exempt de critiques. Ainsi, sa vitesse de traitement est faible, freinant son développement : 7 transactions de Bitcoin par seconde, quand Visa en gère 24 000 (cf. graphique ci-dessous). La volonté d'avoir un système inviolable explique un processus de "mining" très complexe et donc long.

[2] Source : https://www.ecb.europa.eu/explainers/tell-me/html/what-is-a-central-bank.fr.html
[3] Au 21 janvier 2018, il y avait 16,8 millions de bitcoins en circulation.
[4] *fiducia* : nom féminin désignant la confiance en latin



L'enrichissement des participants originels au Bitcoin[5] suscite des convoitises et des imitateurs qui créent leur propre cryptomonnaie, censée combler telle ou telle limite du Bitcoin, appelée génériquement *Altcoin*. Le logiciel assurant le fonctionnement du Bitcoin étant accessible à tous en *open source*, il est aisé de copier, modifier et redistribuer ce logiciel sans risque de violation de droits ou paiement de redevances.

Le nombre d'"Altcoins" a ainsi proliféré : au 7 janvier 2018, il y avait 1 384 Altcoins référencées[6], dont les plus répandues, Ethereum, Bitcoin Cash, Litecoin, Ripple, Dash… se développent comme l'illustre le graphique suivant[7] :



[5] La fortune de l'inventeur du bitcoin est estimée à 600 millions de dollars US : http://www.lemonde.fr/festival/article/2016/08/01/satoshi-nakamoto-l-inventeur-du-bitcoin_4977101_4415198.html

[6] Pour connaitre la liste officielle des cryptomonnaies, se référer notamment à https://en.wikipedia.org/wiki/List_of_cryptocurrencies

[7] Source : https://coinmarketcap.com/

Les cryptomonnaies sont-elles des monnaies ?

Les cryptomonnaies sont des actifs numériques dont la définition et le cadre juridique sont encore en gestation ; le degré d'avancement en la matière varie considérablement d'un pays à l'autre. La première question est bien entendu de savoir si on peut les qualifier de monnaie.

La BCE[8] distingue la *monnaie fiduciaire*, émise par une banque centrale, acceptée en échange de biens et de services, "car la population fait confiance à la banque centrale en ce qui concerne le maintien de la stabilité de la monnaie sur la durée", des "nouvelles monnaies numériques décentralisées comme le Bitcoin pour lesquels il n'y a pas de point de contrôle central (tel qu'une banque centrale), qui ne sont pas considérées *juridiquement* comme de la monnaie". La même BCE définit trois rôles pour une monnaie, "quelle que soit sa forme" : un *moyen d'échange*, à savoir un moyen de paiement ayant une valeur, fiable aux yeux de tous ; une *unité de compte* permettant d'établir le prix des biens et des services et une *réserve de valeur*.

Comme il est difficile d'anticiper l'évolution de la jurisprudence et donc le droit qui reste à écrire sur les cryptomonnaies, concentrons-nous sur les besoins sous-tendant les cryptomonnaies. A cette aune, le Bitcoin et l'Ethereum sont clairement des moyens d'échange. En effet, le Bitcoin est la monnaie de base (quoiqu'elle pourrait être concurrencée par le Monero[9]) des échanges sur le *Dark Web*, cet espace de l'Internet, non-indexé donc invisible aux moteurs de recherche, où tout peut être échangé, surtout le plus illégal : cette "économie souterraine" est estimée à 10% de la richesse légale[10]. Cette "popularité" pourrait fortement inciter les autorités à surveiller, contraindre, voire interdire et criminaliser la détention ou l'usage des cryptomonnaies au motif qu'elles facilitent le blanchiment et le développement d'activités illicites. Certains pays, Chine et Corée du Sud, ont d'ores et déjà fait le choix de l'interdiction.

Les cryptomonnaies, notamment l'Ethereum et le Bitcoin sont les monnaies de prédilection des opérations d'IPO numériques que sont les ICOs (voir paragraphe ci-après). Quant aux 1382 autres *altcoins*, les transactions sont souvent faibles et il conviendrait de débattre plutôt de leur nature d'actifs que de monnaies.

Les cryptomonnaies sont-elles sûres ?

La blockchain du Bitcoin est, par conception, très difficile, voire impossible à falsifier. Si de nombreux hackers s'y essaient, que ce soit par goût de la publicité ou intention malveillante, il semble que personne n'ait encore réussi à casser l'algorithme.

Cependant, la sécurité d'un système est, par définition, celle de son maillon le plus faible. L'accès aux transactions de cryptomonnaies implique de nombreux intermédiaires qui sont non-régulés (il n'y a personne vers qui se retourner en cas de fraude ou de faillite) et vulnérables[11]. En bout de chaine, il y a l'utilisateur qui se déclare par le biais d'un numéro connu de tous - la *clef publique* - et s'authentifie grâce à sa *clef privée* qu'il est le seul à connaitre. Quiconque réussit à récupérer une clef privée peut accéder au *wallet* (compte de cryptomonnaies) et en voler le contenu, sans aucun recours pour son propriétaire. Le droit de propriété n'existe pas en outre pas pour les cryptomonnaies, empêchant tout

[8] https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.fr.html
[9] https://edgylabs.com/monero-to-replace-bitcoin-as-currency-of-criminals-in-dark-web
[10] https://www.lesechos.fr/idees-debats/cercle/0301121797996-la-vraie-valeur-du-bitcoin-2143724.php#hKCwI4LmbGAjmu24.99
[11] La liste des plateformes d'échange se faisant hacker voire faisant faillite est déjà longue : https://www.bloomberg.com/news/articles/2018-01-29/how-to-launder-500-million-in-digital-currency-quicktake-q-a

recours légal. On estime ainsi que 14%[12] de l'offre Bitcoin et Ethereum a été dérobée d'une manière ou d'une autre, ce qui n'est pas surprenant : (i) tout système non-stabilisé est plus vulnérable et les cryptomonnaies sont immatures ; (ii) une crypto-monnaie est "du logiciel" et tout logiciel est sujet à attaque(s) ; (iii) avec 1 384 crypto-monnaies, cela fait 1 384 failles potentielles de sécurité.

Investir dans la technologie sous-jacente au Bitcoin, la Blockchain ?

Comme précisé précédemment, le cœur du Bitcoin est une Blockchain, réceptacle inviolable et inaltérable des transactions passées, appelé *public ledger*. Le Bitcoin est la preuve que la Blockchain n'est pas juste un concept, mais un mécanisme crédible qui peut fonctionner à grande échelle : la valorisation totale des Bitcoins est de 150 milliards de dollars US. On évoque près de 400 milliards pour l'ensemble des cryptomonnaies[13].

Depuis 2014, l'intérêt pour les Blockchains grandit rapidement, le Bitcoin constituant un laboratoire à grande échelle de l'élimination concrète du tiers de confiance, au cœur de nombreux métiers, trop souvent facteur de lourdeurs administratives, de surcoûts et sujet à des tendances monopolistiques peu compatibles avec l'ère numérique.

Technologiquement, il est probable que les projets de Blockchain futurs n'auront plus grand-chose à voir avec la Blockchain d'origine, celle du Bitcoin. Les Blockchains publiques, plus ambitieuses mais plus futuristes et les Blockchains privées, plus adaptées à un besoin spécifique, et plus faciles à mettre en œuvre, présentent déjà une démarcation de plus en plus marquée.

Les mécanismes de règlement-livraison des marchés financiers, les processus de dédommagement des sinistres dans l'assurance, les transferts monétaires, les systèmes de preuve de propriété (immobilier, voiture, brevets), d'identification ou de traçabilité (exemple : certifier l'origine de tous les composants d'une "supply chain" ou lutter contre la contrefaçon) sont tous susceptibles d'être réinventés à une échéance plus ou moins proche par la blockchain.

Pour avoir un bon aperçu de ce qu'imaginent les entrepreneurs les plus visionnaires, un nouvel Internet, nous conseillons par exemple cet excellent article du New York Times[14].

Le potentiel disruptif est évident et les annonces de nouvelles Blockchains se multiplient. Néanmoins, la grande majorité sont encore des projets ("*proof of concept*") destinés à convaincre un écosystème de franchir le pas vers la Blockchain, ce qui heurte certaines positions établies. En tant qu'opportunité d'investissement, et notamment d'investissement coté s'agissant de Finaltis Digital Leaders, c'est encore prématuré, mais assurément à surveiller.

Bitcoin et blockchain comme moyen d'investir : les ICOs

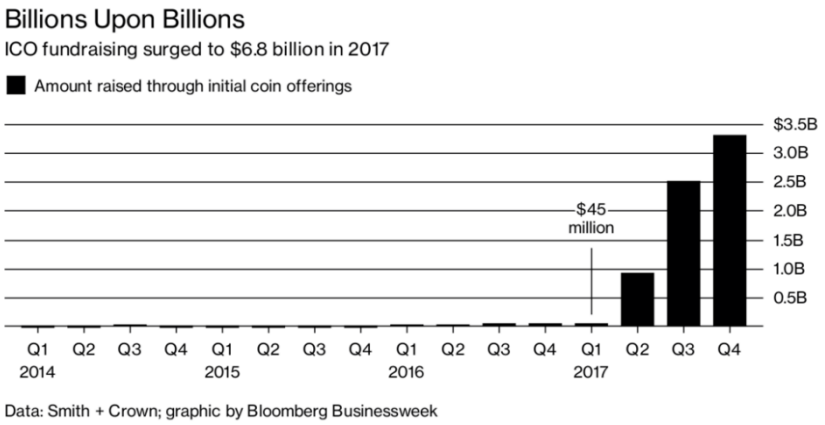
Une *Initial Coin Offering* (ICO) relève du *crowdfunding*, donc une levée de fonds nécessaires au lancement d'un projet sans emprunt bancaire, et sans appel aux marchés financiers ou à un fonds de "private equity".

Toutefois, dans le cas d'une ICO, il n'y a pas d'émission ou de cession de parts ou d'actions d'une société ; des *jetons* ("tokens") sont émis. Ce "token", payé en général en Bitcoin ou Ethereum, donne

[12] https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies
[13] Au 2 février 2018, source : www.coinmarketcap.com
[14] https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html

droit à une conversion dans la cryptomonnaie associée à l'ICO ou à d'autres privilèges (droits d'usage, priorités, gratifications, dividendes, droits de vote particuliers…). Le cadre juridique est en cours de définition par les autorités des différents pays : la SEC a émis un "avertissement" concernant les ICOs le 1er août 2017 et n'a pas hésité à intervenir sur certaines ICOs, voire à en interdire, essentiellement pour non-conformité avec la législation des… placements de titres. De nombreuses autorités nationales, dont l'AMF en France, réfléchissent aux règles à appliquer à ces opérations ; la Chine les a interdites.

6,8 milliards de dollars US ont été levés sous la forme d'ICOs[15] depuis leur création, la quasi-totalité sur la seconde moitié de 2017, principalement aux Etats-Unis.



L'ambition d'une ICO peut aller bien au-delà de la levée de fonds : Telegram est à ce titre emblématique. Pour mémoire, Telegram est une messagerie créée en 2013 par deux opposants à Vladimir Poutine : Telegram chiffre de bout en bout ses échanges, ce qui en fait malheureusement une des applications préférées des djihadistes. Son usage est aussi très répandu dans l'écosystème des ICOs ; elle devrait prochainement atteindre les 200 millions d'utilisateurs. Telegram a annoncé vouloir lancer en 2018 l'ICO la plus importante à ce jour, visant une levée d'1,2 milliard de dollars US[16] pour financer le développement d'une plateforme décentralisée (avec Telegram néanmoins aux commandes…), le Telegram Open Network (TON) offrant un ensemble de services (communication, hébergement de fichiers, navigation anonymisée…), payables avec les "tokens" émis lors de l'ICO, appelés "Grams".

En synthèse, pour investir…

Acheter une cryptomonnaie en convertissant une monnaie bien réelle est assez aisé pour un particulier. La performance spectaculaire du Bitcoin et d'autres altcoins, malgré la forte volatilité qui les caractérise, alimente espoirs et fantasmes : +256% annualisés pour les Bitcoins en comparaison au dollar US sur trois ans (2015-2017) dont… +1 403% en 2017 ! La dimension spéculative est évidente : même la célèbre experte financière Nabila en vante les mérites sur Internet[17] sans toutefois préciser l'extrême volatilité à en attendre : à l'heure où nous rédigeons (2 février), le Bitcoin a perdu plus de 15% lors des dernières 24 heures, l'Ethereum -21%, le Cardano -36%... La liquidité de ces marchés, fragmentés et immatures, reste à tester lorsque tout le monde voudra vendre des Bitcoins et autres cryptomonnaies au même moment. Les variations des devises fiduciaires sont difficiles à anticiper alors

[15] https://www.forbes.com/sites/outofasia/2017/12/18/icos-in-2017-from-two-geeks-and-a-whitepaper-to-professional-fundraising-machines/#37b7b4e6139e
[16] https://techcrunch.com/2018/01/15/inside-telegrams-ambitious-1-2b-ico-to-create-the-next-ethereum/
[17] Voir la vidéo sur YouTube : https://www.youtube.com/watch?v=9Eys7uaZOvw

que leurs sous-jacents sont accessibles à tous, reposant sur la santé économique d'un pays ou d'une zone et sur la politique monétaire de sa banque centrale. Rien de cela pour les cryptomonnaies, qui présentent de surcroît des risques quant à la notion même de leur propriété, leur licité fluctuante selon les pays et le traitement fiscal qui est réservé aux transactions réalisées.

Si peu de gouvernements ont adopté des positions définitives, il est impensable que des sujets aussi régaliens et sensibles que la monnaie ou les levées de fonds (par le biais d'ICOs) ne soient pas encadrés.

Quant aux projets liés à la technologie Blockchain, ceux-ci gagneront probablement progressivement l'ensemble de l'espace économique. Néanmoins, si on peut citer AXA et son service Fizzy, une plateforme d'assurance paramétrique 100% automatisée, 100% sécurisée, permettant de couvrir les retards d'avion, combien de temps faudra-t-il pour que cela agisse de manière significative sur sa valorisation ?

Parmi les accélérateurs digitaux chers à Finaltis Digital Leaders, IBM, **Accenture** et **Microsoft** sont très actifs sur le sujet de la Blockchain ; de nombreux contrats de conseil sont signés. En matière d'infrastructure, la demande en serveurs et *in fine* le volume d'affaires de **TSMC**, en bout de chaine, est également mesurable. Leur poids pour autant dans leur chiffre d'affaires global est encore minime.

Pour ceux qui seraient tentés par une sensibilisation à l'évolution du cours et des volumes des crypto-monnaies, le *proxy* le plus intuitif est Nvidia ou AMD. Gardons toutefois en tête que toute baisse sensible du cours du Bitcoin modifie en profondeur le marché du "mining", faisant sortir les mains faibles et diminuant d'autant la demande auprès de ces sociétés. L'effet peut jouer dans les deux sens, d'autant plus que leur communication nous semble minimiser l'impact potentiel du marché des cryptomonnaies sur leur chiffre d'affaires pour ne pas effrayer les investisseurs.

Quel que soit le vecteur envisagé pour s'exposer à la thématique bitcoin/altcoin, blockchain et ICO, qu'il s'agisse de positions en cryptomonnaies, en technologies sous-jacentes, en applications dérivées, en infrastructure ou en disruptions à venir, il nous semble toutefois indispensable de bien mesurer l'immaturité générale de la thématique et les grandes incertitudes inhérentes de toutes natures : absence de cadres juridique, réglementaire et fiscal clairs ; risques opérationnels, technologiques et réputationnels au plus haut.

Pour les investisseurs de la digitalisation que nous sommes, la thématique doit être scrutée avec attention. Elle doit cependant rester à ce stade sous le microscope, en laboratoire. Outre une veille très active sur ce sujet très dynamique, pour préparer les investissements d'après-demain, seuls quelques accélérateurs digitaux ou entreprises d'infrastructure digitale nous semblent adaptés à ce stade.

La phase actuelle de la thématique est celle de la "soupe quantique", juste après le Big Bang… dont la vie naîtra… longtemps après.

A suivre donc…

Les sociétés soulignées en gras sont détenues par le fonds au 31 janvier 2018.

Benoît Flamant
bflamant@finaltis.com

Leslie Griffe de Malval
lgriffedemalval@finaltis.com

Co-gérants du fonds Finaltis Funds Digital Leaders