GUIDE DES CRYPTO MONNAIES POUR INVESTISSEURS

CRYPTO FINANCE ANALYSIS CONSULTING

Votre partenaire dans le monde de la cryptofinance

BESOIN DE CHANGEMENT

Le monde de la finance est sur le point de changer drastiquement.
Un nouvel arrivant vient de pénétrer ce gigantesque marché de plusieurs milliers de milliards de dollars* et il entend s'imposer.

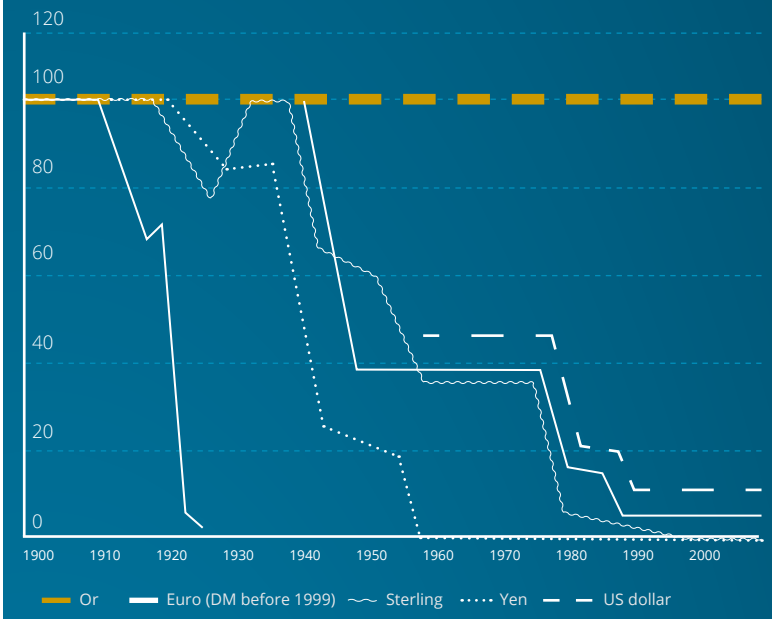
Les monnaies du monde entier, et avec elles le reste du système financier, ont été réglementées et gérées de façon centralisée depuis bien longtemps. Cependant, là où étaient attendues stabilité économique et prospérité, on a trop souvent vu naître des crises économiques, des cracks boursiers, voire même des guerres.

Durant les périodes de crise, les gens se sont généralement tournés vers l'or pour son utilité en tant que réserve de valeur, bien qu'il présente des inconvénients majeurs : il est lourd, coûteux à stocker, son marché est manipulé, et son achat est en plus réglementé dans de nombreux pays.

Mais quoi d'autre à part l'or ? Le besoin d'un refuge capable de soutenir les futurs chocs économiques se fait clairement sentir : la récupération de la crise globale de 2007/2008 reste fragile, et, compte tenu des problèmes futurs consécutifs au *quantitative easing* et aux déficits croissants de nombreux pays, il y a de nombreuses raisons de se questionner sur la stabilité et la santé de l'économie mondiale dans les années à venir.

La demande croissante de transactions à la fois plus rapides et plus sécurisées pourrait bien, à l'heure d'Internet, trouver sa réponse dans les crypto monnaies comme le Bitcoin.

Monnaies en termes d'or



* *Les trois réseaux de paiement principaux (MasterCard, Visa, et American Express) traitent ensemble plus de 3000 milliards de dollars de paiements, générant un chiffre d'affaire annuel de plus de 30 milliards de dollars. La capitalisation boursière totale des compagnies de cartes de crédit est de presque 400 milliards de dollars. Les banques américaines facturent à elles seules plus de 250 milliards de dollars de frais par an. Les magasins en ligne ont un chiffre d'affaire de plus de 1 000 milliards de dollars annuel. Plus de 30 000 milliards de dollars sont mis à l'abri dans des comptes en banque offshore. Les entreprises d'envoi de fonds gèrent des échanges se montant à 500 milliards de dollars tous les ans. 500 autres milliards de dollars sont dépensés annuellement en frais de transaction. Enfin, la capitalisation de l'or est d'environ 8 000 milliards de dollars.*

La dernière version de ce document est téléchargeable ici :
http://cfa-consulting.ch/dlfiles/Crypto_Guide_For_Investors_FR.pdf

DES MONNAIES RAPIDES POUR UN MONDE RAPIDE

Qu'est-ce que le Bitcoin ?

Bitcoin est un système de paiement électronique de pair à pair, ou ***peer to peer*** en anglais. Il permet aux transactions entre personnes d'avoir lieu sans passer par une autorité centrale ou par des intermédiaires. Bitcoin est donc un réseau de terminaux individuels. Les transactions ont lieu en informant les autres pairs du transfert d'argent d'un "*wallet*" (l'équivalent d'un compte en banque) à un autre. Le système impose un standard de cryptage de très haute qualité pour protéger l'expéditeur, le récepteur, et le système global. C'est pour cette raison que Bitcoin et les autres monnaies numériques sont souvent appelés des "monnaies cryptographiques".

Que sont les Bitcoins ?

Les paiements ayant lieu au sein du réseau Bitcoin sont enregistrés dans un livre de comptes public et sous forme d'une unité de compte spécifique : les Bitcoins.

Les utilisateurs peuvent envoyer et recevoir électroniquement des Bitcoins simplement en utilisant un logiciel de gestion de "*wallet*" via un ordinateur, un appareil mobile, ou une application Web, moyennant des frais de transaction optionnels.

La capitalisation boursière actuelle du système Bitcoin est de plus de 8 milliards de dollars (Juillet 2014).

Fonctionnalités économiques :

- Il y a de faibles frais pour chaque transaction (quelques centimes au prix actuel) [1].
- La masse monétaire du Bitcoin est programmée pour progresser à une allure modérée, puis s'arrêter. L'effet de cette inflation[2] contrôlée est montré grâce au graphique 1.
- La monnaie Bitcoin est faiblement inflationniste. Il y a en 2014 12 millions de Bitcoins en circulation ; ce nombre s'accroîtra lentement jusqu'à atteindre 21 millions en 2140. A partir de cette date, plus aucun Bitcoin ne sera créé, et la nature du Bitcoin en tant que monnaie changera pour devenir légèrement déflationniste. Ce qui veut dire que, toutes choses égales par ailleurs, la valeur de chaque Bitcoin augmentera avec le temps.

> *Bitcoin est le début de quelque chose de formidable : une monnaie sans gouvernement, quelque chose de nécessaire et d'impératif*
>
> Nassim Taleb
> philosophe, écrivain, statisticien
> auteur de La théorie du Cygne Noir (2013)

- Contrairement aux transactions avec cartes de crédit, celles avec les Bitcoins sont définitives dès qu'elles touchent le réseau Bitcoin. S'il devait y avoir un marché pour un service de remboursement, il pourrait être offert par des tierces parties.
- Il n'y a pas de banque centrale. Au contraire, les décisions sont prises par le marché ou définies dès le départ au coeur du système : taux d'intérêts directeur, masse monétaire, taux d'inflation, monnaie non falsifiable, etc. Bienvenue dans un système monétaire en bonne santé !

[1] Ces frais dépendent d'aspects techniques qui sortent du cadre de ce document. Pour plus de détails techniques, veuillez vous référer à l'article suivant (en anglais) : https://en.Bitcoin.it/wiki/Transaction_fees
[2] Tout au long de ce document, quand il sera question d'inflation, c'est de l'augmentation de la masse monétaire dont il s'agira, et non de celle des prix.

- La possession décentralisée et le possible anonymat de ce moyen de paiement et de réserve de valeur place le Bitcoin et les autres crypto monnaies en général dans la même catégorie que l'or.

- Comme le Bitcoin est miné (voir la section des fonctionnalités techniques pour plus de détails), c'est une monnaie légèrement inflationniste : la masse monétaire va donc s'accroître d'environ 10% en 2014. Mais cette inflation est programmée pour diminuer : il y a une fin au minage, et à partir de ce moment, l'inflation s'arrêtera (voir *graphique* 1).

- La valeur du Bitcoin est, pour le moment, très volatile. Elle dépend beaucoup d'annonces publiques comme, par exemple, lorsque la Banque Populaire de Chine a publié une note interdisant aux banques de travailler avec des plateformes d'échanges Bitcoin sur le territoire chinois. Même si le réseau Bitcoin est très souple et peut, techniquement, résister à une telle interdiction, le prix du Bitcoin s'en ressent néanmoins, tendant à chuter brusquement avant de retrouver sa tendance long terme. Voir le *graphique 2* pour une évolution de la volatilité du Bitcoin, et le *graphique 3* pour l'évolution de son prix et de sa volatilité.

- Les Bitcoins sont de plus en plus acceptés comme moyen de paiement pour des biens et des services, comme réserve de valeur, et même comme garantie.
Bloomberg a récemment ajouté un ticker Bitcoin

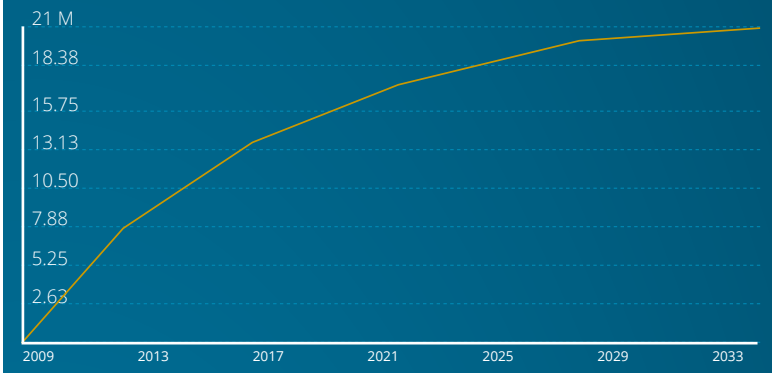
à son terminal d'échange professionnel, tout comme Google Finance et Yahoo Finance.

- De plus en plus de gens s'intéressent aux Bitcoins. Avec plus de 60 000 transactions journalières (voir

graphique 4) et un volume de transactions estimé de plus de 45 millions de dollars, la liquidité des Bitcoins ne pose plus beaucoup de problème, rendant la monnaie de moins en moins risquée.

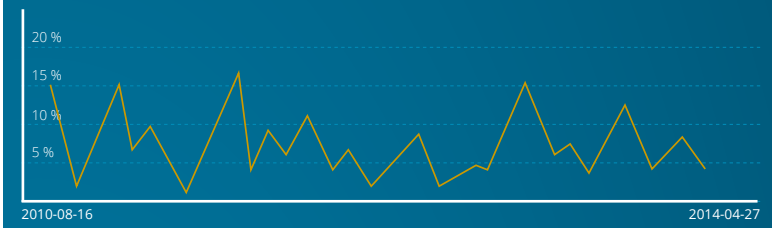
Total des Bitcoins en circulation

Graphique 1



Volatilité du Bitcoin %

Graphique 2

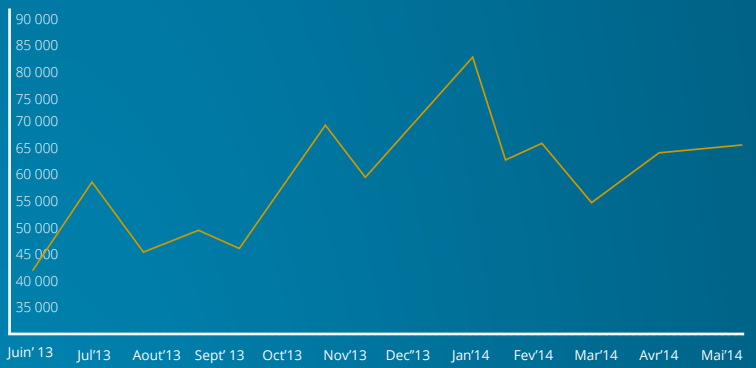


Volatilité et prix du Bitcoin

Graphique 3

Bitcoin transaction / jour

Graphique 4



Fonctionnalités techniques :

- Pour maintenir l'intégrité de la blockchain Bitcoin (un livre de comptes numérique et public), des gens utilisent du matériel informatique sophistiqué pour "miner" des Bitcoins, en compétition les uns avec les autres, pour ajouter des "*blocks*" à la "*blockchain*". Ces blocs sont comme des pages d'un livre de comptes, chaque bloc contenant les transactions réalisées depuis le bloc précédent. Etant donné que tout ceci est public et partagé par un grand nombre d'ordinateurs, tricher et modifier les transactions du passé est considéré comme impossible. Une transaction est généralement admise comme parfaitement sûre après six confirmations, ce qui veut dire que six blocs ont été "minés" depuis qu'elle a eu lieu. Ce processus prend environ une heure (chaque bloc prend en moyenne 10 minutes pour être "miné"). Cependant, la plupart des gens jugent inutile d'attendre les six confirmations et se contentent de moins pour considérer les fonds comme bien transférés.

> *Je pense que Bitcoin est un tour de force technologique.*
> Bill Gates, Fondateur de Microsoft (2013)

- Les mineurs minent pour gagner une récompense : quand un mineur résoud une équation algorithmique spécifique, des Bitcoins sont créés et envoyés sur le compte dudit mineur, en venant s'ajouter au nombre total de Bitcoins en circulation. En 2014, 25 Bitcoins seront créés de cette manière toutes les 10 minutes en moyenne (voir *graphique* 1 pour l'inflation du Bitcoin.) Cette méthode permettant la maintenance de la blockchain s'appelle la Preuve de Travail (*Proof of Work*, ou PoW) : le "travail" étant la résolution de l'équation et la "preuve" étant l'annonce au réseau Bitcoin de la solution trouvée.

> *Bitcoin est une réalisation cryptographique remarquable et la possibilité de créer quelque chose qui n'est pas duplicable dans le monde numérique a une valeur énorme.*
> Eric Schmidt, PDG de Google (2013)

- Implications : pour cette raison, une course à la puissance informatique fait rage : les mineurs dépensent de plus en plus d'argent pour acheter du matériel dédié afin de miner plus vite, c'est-à-dire pour avoir plus de chances de gagner la récompense de 25 Bitcoins.

Comment acheter des Bitcoins ?

Aujourd'hui la vaste majorité des achats de Bitcoins est réalisée via des plateformes d'échanges centralisées. Une certaine quantité est également échangée de la main à la main ou encore via des "distributeurs" de Bitcoin (ATM). Plusieurs ont d'ailleurs été installés dans différents pays comme le Canada, la Nouvelle Zélande, la Suisse... Il existe de tels distributeurs sur le marché (d'un coût d'environ 1000 dollars), permettant aux propriétaires de Bitcoins d'installer leur propre point de vente automatique (en juin 2014, 220 avaient déjà été vendus).

http://projectskyhook.com/

Bitcoin: de nouveaux services pour des marchés existants

En tant que nouveau système de paiement, de tenue de comptes et de réserve de valeur, le Bitcoin entre en compétition avec d'autres systèmes préexistants, comme :

- **Les cartes de crédit et Internet** : Bitcoin a été développé dans l'optique de payer via Internet : comme c'est un système de pair à pair (*peer to peer*), il ne nécessite pas l'usage d'une tierce partie pour gérer le paiement, ce qui est le cas pour une compagnie de cartes de crédit ; par ailleurs, étant donné que les paiements en Bitcoins sont irréversibles, il n'y a pas de possibilité de remboursement. Des entreprises dont le coeur de métier repose sur Internet ainsi que certains magasins en ligne acceptant déjà le Bitcoin, ont annoncé qu'ils allaient offrir cette possibilité. (Overstock, CVS, Sears, Home Depot, Kmart, Amazon, Shopify, TargetDirect, Virgin Galactic, Dish Networks, C7 Data Centers, Expedia, Newegg.com, Dell, Monoprix, etc.).
  En juillet 2014, plus de 60 000 commerces dans le monde acceptaient des paiements en Bitcoins, il est même probable que ce nombre monte à 100 000 avant la fin de l'année.

- **Les cartes de crédit dans les magasins physiques** : l'utilisation de cartes de crédit (en ligne ou hors ligne) est coûteuse, alors qu'un simple code QR est suffisant pour payer en Bitcoin, à l'aide d'un appareil connecté à Internet, et ce de façon instantanée et complètement sécurisée (voir *Infographique* 1).

- **Paypal et d'autres systèmes de paiement** : ceux-ci coûtent de l'argent à l'utilisation, alors qu'un paiement en Bitcoin est presque gratuit. Cependant Bitcoin peut également supporter des services supplémentaires, comme une assurance ou un "programme de protection de l'acheteur", ce qu'offre déjà Paypal, par exemple.

- **Envoi de fonds** : Western Union et MoneyGram sont des cibles claires : Bitcoin fait gratuitement ce qu'ils facturent (une moyenne de 9% par transaction).

> *Virgin Galactic est une entreprise technologique audacieuse en train de conduire une révolution et Bicoin est en train de faire quelque chose de similaire en inventant une nouvelle monnaie.*
>
> Sir Richard Branson, Fondateur de Virgin Records, Virgin Galactic, et de plus de 400 autres entreprises (2013)

> *Je pense réellement que Bitcoin est la première monnaie cryptographique qui a le potentiel de changer le monde.*
>
> Peter Thiel, Co-Fondateur de Paypal (2014)

- **Liquide** : les Bitcoins fonctionnent comme du cash électronique. C'est rapide et les petits paiements sont aisément réalisés.

- **Sexe** : L'industrie du sexe a toujours été à la recherche de nouvelles technologies pour satisfaire ses nombreux consommateurs. Le relatif anonymat des paiements en Bitcoins peut être attirant pour ces clients, et c'est pourquoi cette industrie est déjà en train de migrer vers le Bitcoin.

- **Le jeu** : les casinos en ligne ont déjà commencé à accepter les Bitcoins. C'est une monnaie internationale qui est à la fois pratique et rapide pour de telles entreprises avec des clients provenant de nombreux pays. Ce marché est estimé à 30 milliards de dollars.

- **Crowdfunding** : la disponibilité globale des Bitcoins, les faibles frais de transferts, et leur instantanéité ouvrent la porte à de nombreux efforts de crowdfunding en ôtant les barrières géographiques et les coûts de transactions.

> *Je pense qu'Internet va devenir une des forces majeures qui va diminuer le rôle des gouvernements. La seule chose qui manque, mais qui sera développée bientôt, est une solution fiable de cash électronique*
>
> Milton Friedman,
> prix Nobel d'économie (1999)
>
> *Ca y est, Mr Friedman, le cash électronique fiable est arrivé ! Les peuples de pays comme l'Argentine, Chypre, ou la Grèce par exemple, commencent à s'intéresser aux Bitcoins à cause du manque de confiance dans leur propre monnaie ou gouvernement.*

Infographique 1

Systèmes de paiement

Transaction inefficace
(Intermédiaires : banque, carte de crédit, etc)

Vous achetez votre repas 20€

La carte de crédit vérifie avec votre banque

La carte de crédit envoie de l'argent à la banque du restaurant et **facture 3%**
(le commerçant obtient 19.40€)

La carte de crédit vous facture des intérêts ou des frais annuels.

Transaction efficace
(Aucun intermédiaire)

Vous achetez un repas pour 0.03 BTC

Les Bitcoins vont directement au vendeur et la transaction est vérifiée par le réseau

Le commerçant obtient 0.03 BTC
(l'acheteur paie aussi 0,0001 BTC de frais aux mineurs qui gèrent la transaction)

Dans ce cas les frais se montent à 0,3%

10X PLUS EFFICACE

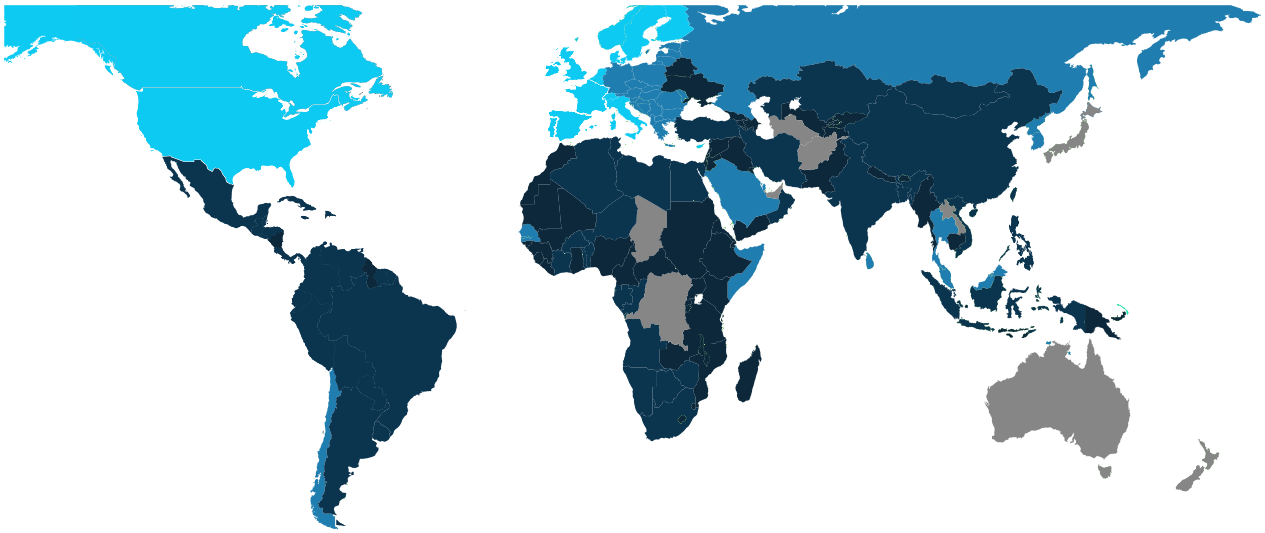
Kashmir Hill a publié un livre électronique dans l'édition *Forbes Signature Series*, intitulé *Monnaie Secrète, Vivre Avec Des Bitcoins Dans Le Monde Réel (Secret Money, Living On Bitcoin In The Real World)*. Il y explique comment il a vécu une semaine à San Francisco en ne dépensant que des Bitcoins.

Bitcoin : de nouveaux services pour de nouveaux marchés

Les fonctionnalités particulières du Bitcoin en font un outil formidable pour le développement de nouveaux marchés :

- Micropaiements : le champ d'application potentiel des tout petits paiements (<$0.1) est énorme : des pourboires en ligne à la possibilité de se faire payer pour des sondages ou regarder des publicités, des jeux en ligne (Zynga accepte déjà les paiements en Bitcoins) au paiement via des "j'aime" sur des sites comme Facebook, ou du paiement d'informations en ligne aux messageries sans spam, les possibilités sont sans limite. Les crypto monnaies, avec les frais de transaction avoisinant le zéro, sont idéalement placées pour jouer un rôle prépondérent sur ce marché.

Carte 1 : Pourcentage de la population adulte totale qui n'utilise pas de service financier formel ou semi formel



Total

53%

de la population adulte mondiale sans accès à des services financiers

0 - 25% 26 - 50% 51 - 75% 76 -100%

Pourcentage de la population adulte avec peu ou pas d'accès à des services financiers

Estimations utilisées pour calculer des moyennes régionales

- Pays sous-développés / en voie de développement. Hernando de Soto, un économiste péruvien connu pour son travail sur l'économie informelle, a identifié certaines des causes du sous-développement des pays pauvres. L'une d'elles est le manque d'un système de paiement sûr ("Le mystère du capital" -*The Mystery of Capital*-, H. De Soto, 2000). Sans Bitcoin, le choix est restreint à soit un système coûteux comme les cartes de crédit, soit un système non sécurisé : l'argent liquide. Le Bitcoin va révolutionner les micro crédits et l'infrastructure financière d'une partie du monde qui a le potentiel de croître exponentiellement durant les 25 prochaines années : l'Afrique (voir carte 1).

Chiffres-clés du marché Bitcoin, en Juillet 2014 :

- Les investissements de capital-risque dans le monde Bitcoin viennent de franchir les 285 millions de dollars. Afin de mettre ce chiffre en perspective, il faut le comparer aux 250 millions en 1995 pour l'ensemble de l'industrie Internet.
- 63 000 commerçants acceptent les Bitcoins dans le monde.
- Le FBI a vendu 30 000 Bitcoins à un capital-risqueur (Tim Draper). Il n'y a pas de retour arrière possible : maintenant, les Etats-Unis se sont fermés la porte de l'interdiction légale du Bitcoin, et ne peuvent plus que le réglementer.
- La Californie a spécifiquement légalisé le Bitcoin en juin 2014.
- Benjamin Lawsky, superintendent du Département des Services Financiers (*Department of Financial Services*) de la ville de New-York, a proposé en juillet 2014 un ensemble de règles à suivre pour les entreprises travaillant dans le domaine des crypto monnaies.
- Apple a commencé à accepter des applications Bitcoin dans son App Store, après une période d'interdiction qui n'a duré que quelques mois. 340 applications y sont maintenant disponibles, et 250 sont téléchargeables dans l'Android Store.

Les limites du Bitcoin

- La plupart des gens ne comprennent pas ce qu'est Bitcoin ni ne savent comment l'utiliser. Cependant, d'importants efforts sont faits pour créer les outils qui permettront à tout le monde de profiter de cette nouvelle technologie, de la même façon qu'il fut fait avec Internet. On peut espérer qu'avec l'introduction de tels outils, la complexité technique liée à l'utilisation du Bitcoin ne posera plus de problème et sera aussi simple que l'utilisation d'autres moyens de paiement, tels que les cartes de crédit ou les virements bancaires internationaux. Les clients se fichent de savoir si leurs outils sont complexes tant que cette complexité est tenue loin d'eux et que la maintenance est gérée par quelqu'un d'autre.
- Le manque de confidentialité. Le système Bitcoin s'appuie sur la blockchain publique qui fonctionne comme un livre de comptes géant. Comme tout est public, il est simple de retracer toutes les transactions réalisées par un compte en particulier. Un client payant un fournisseur connaît nécessairement le numéro de compte vers lequel l'argent est envoyé. A partir de là, il peut, par exemple, calculer le chiffre d'affaire du fournisseur. Ce manque d'intimité inhérent au Bitcoin fait qu'il peut difficilement devenir un moyen de paiement majeur, bien que le risque de divulguer involontairement des informations commercialement sensibles puisse en partie être réduit, par exemple en utilisant plusieurs comptes Bitcoin.

> *Je suis très intrigué par Bitcoin. Il y a tous les signes. Changement de paradigme, les hackers l'adorent, et pourtant il est tourné en dérision comme étant un jouet. Comme les micro ordinateurs.*
>
> Paul Graham, Créateur de Yahoo Store (2013)

- Il y a un risque technique au système de Preuve de Travail (PoW) : il est théoriquement possible d'attaquer le réseau Bitcoin, à condition que l'attaquant dispose de plus de 50% de la puissance informatique utilisée par le minage de Bitcoins. Ceci s'appelle le risque d'attaque à 51%. Des solutions sont en train d'être développées pour limiter ce risque.
- Parmi les autres limites du Bitcoin se trouvent les délais de transaction et le nombre total de Bitcoins (rendant le prix d'un Bitcoin assez élevé, et ainsi décourageant inutilement le consommateur moyen).

LE MONDE DES CRYPTO MONNAIES : L'ARBRE BITCOIN QUI CACHE UNE FORÊT

Le Bitcoin a ouvert une porte

En trouvant un moyen de décentraliser la gestion d'une monnaie, Satoshi Nakamoto a ouvert une boîte de Pandore. Il a créé un outil qui est sur le point de révolutionner la finance, comme Internet a révolutionné l'industrie informatique, avec beaucoup d'effets de bord dans les industries connexes.
Mais Satoshi Nakamoto a créé Bitcoin tout seul et, même si une importante communauté de développeurs s'est réunie autour depuis, il demeure techniquement difficile de modifier les bases du système.

C'est la raison principale pour laquelle de nombreux développeurs, utilisant un nombre varié de techniques, se sont mis à créer d'autres crypto monnaies. Entre 2013 et 2014, des centaines de monnaies ont ainsi vu le jour. Elles peuvent être placées dans deux catégories : les clones Bitcoin et les crypto monnaies de seconde génération.
Généralement, le développeur d'un clone de Bitcoin prend le code de Bitcoin et modifie un ou plusieurs paramètres existants (nombre total de pièces, taux d'inflation, vitesse de transaction, etc.).

> *Il sera partout et le monde devra s'adapter. Les gouvernements du monde devront se réadapter.*
> John McAfee, Fondateur de McAfee (2013)

Cependant, le développeur de clone n'ajoute pas de fonctionnalité complètement nouvelle au code.
Ceci veut dire que sa valeur aura tendance à être parfaitement liée à celle du Bitcoin. Le seul autre facteur influançant la valeur d'un quelconque clone pour une courte période de temps est le degré de confiance qu'il peut donner (nouveauté, marketing agressif, impression du marché...)

Le clone de Bitcoin avec la capitalisation boursière la plus importante est le Litecoin, et c'est essentiellement dû au fait qu'il fut un des premiers à apparaître sur le marché après le lancement de Bitcoin.

Alors que beaucoup de développeurs se sont contentés d'ajuster quelques paramètres du protocole Bitcoin, d'autres ont essayé de developer des solutions pour faire face aux faiblesses principales de Bitcoin (voir page 9).
Le développement et l'implémentation de ces solutions - certaines d'entre elles impliquant la réécriture complète du code - a donné naissance à une seconde génération de crypto monnaies.

Changements d'approches

- **Manque de confidentialité** : une des principales limites du Bitcoin est la traçabilité des transactions. Plusieurs solutions ont été imaginées pour y remédier, comme l'inclusion d'une tierce partie permettant le "mélange"[3] ou le développement de crypto monnaies totalement nouvelles qui intègrent directement ce genre de fonctionnalité au sein de leur protocole, comme Darkcoin et AnonCoin.

- **La Preuve de Travail** *(Proof of Work ou PoW)* : la plupart des crypto monnaies utilisent le même mécanisme de PoW qui est détaillé plus haut. Ce système a trois inconvénients majeurs :

  - Le risque d'attaque 51% décrit page 10.
  - Les systèmes PoW sont coûteux à maintenir, et les mineurs dépensent une fortune pour faire tourner leurs programmes (en matériel et en électricité). La maintenance du système Bitcoin coûtera 130 millions de dollars en 2014, et ce coût augmentera en proportion de l'accroissement du prix du Bitcoin[4].
  - Ce mécanisme génère de l'inflation au travers du minage. (voir *graphique* 1)

- En conséquence, d'autres solutions ont été développées :

  - **La Preuve d'Enjeu** (*Proof of Stake ou PoS*) : finis les mineurs, voici les forgeurs. La probabilité qu'un compte puisse forger (c'est-à-dire parvienne à confirmer le block suivant de transactions à ajouter à la blockchain et ainsi à gagner la récompense) est proportionelle à la quantité de monnaie PoS présente sur ledit compte, d'où le nom : Preuve d'Enjeu. Ce système élimine le risque d'une attaque 51% car, pour mener une telle attaque, il faudrait posséder au moins 51% de la masse monétaire.
    De plus, les mécanismes PoS ne nécessitent pas de matériel informatique puissant et onéreux pour la maintenance de la blockchain et ne consomment pas beaucoup d'électricité. Les systèmes PoS peuvent être maintenus pour moins d'un millième de ce qui est nécessaire pour les systèmes PoW. C'est pourquoi on les considère comme une technologie verte.
    Enfin, il n'y a absolument aucune inflation. La masse monétaire est créée au début, et c'est pourquoi un système PoS garantit qu'une monnaie sera déflationniste dès le premier jour. NXT est la monnaie principale utilisant un mécanisme PoS. Mintcoin et Communitycoin en sont deux autres.

  - **Preuve de Transaction** (*Proof of Transaction ou PoT*) : le système s'appuie sur la génération de transactions. Encore une fois, pas de matériel spécifique de minage nécessaire : la blockchain est maintenue par ceux-là même qui utilisent la monnaie. Le défaut de ce système est que la blockchain est difficile à maintenir au début de la vie de la monnaie, ce qui veut dire qu'il est moins probable que ceux qui l'utilisent la voient un jour adoptée de façon générale.
    La blockchain inclut un mécanisme d'équilibrage de façon à ce que personne ne puisse prendre le contrôle via une attaque 51% simplement en générant des transactions factices.
    La PoT requiert très peu de matériel informatique pour être maintenue. Sous cet angle, c'est un système encore plus écologique que le PoS.

  - **Systèmes mixtes** : certaines monnaies mélangent ces mécanismes, comme Peercoin (PoW & PoS) ou Fluttercoin (les trois systèmes). Les développeurs travaillant sur ces monnaies pensent qu'en mélangeant les technologies, ils limitent les risques associés à chacune d'entre elles.

[3] Les clients envoient leurs Bitcoins à la même tierce partie avec les détails concernant la destination finale de l'argent, puis toutes ces transactions sont mélangées ensemble avant que les transactions de sortie ne soient réalisées vers les adresses de destinations finales.
[4] Analyse comparative détaillée de l'efficacité énergétique et de la rentabilité de Bitcoin et NXT (en anglais) :
http://cfa-consulting.ch/dlfiles/NxtEnergyandCostEfficiencyAnalysis.pdf

Le résultat de tous ces développements et innovations est une industrie nouvelle, la crypto finance. L'ampleur des implications, en termes de capacité à révolutionner la société de cette industrie, commence à peine à être reconnue. Cela rappelle les débuts d'Internet, notamment parce qu'il est important d'identifier les start-up les plus prometteuses dans ce qui est un marché évoluant extrêmenent rapidement.

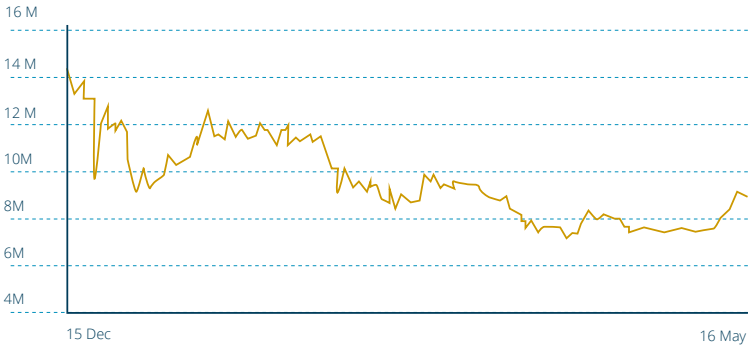
Quelles sont les meilleures crypto monnaies ? Ce sont celles qui améliorent ce qui existe déjà et qui disposent d'une communauté active. La communication, la publicité, et le développement de nouveaux outils et fonctionnalités dépendent de ces communautés.

C'est pourquoi, pour identifier les meilleurs investissements moyen et long termes dans ce domaine, les clones de Bitcoin doivent être ôtés du tableau à cause de leur manque d'innovation, tout comme la plupart des autres monnaies qui ont une capitalisation boursière ou un volume d'échanges trop faibles pour des investissements conséquents.

Cela laisse les monnaies suivantes :

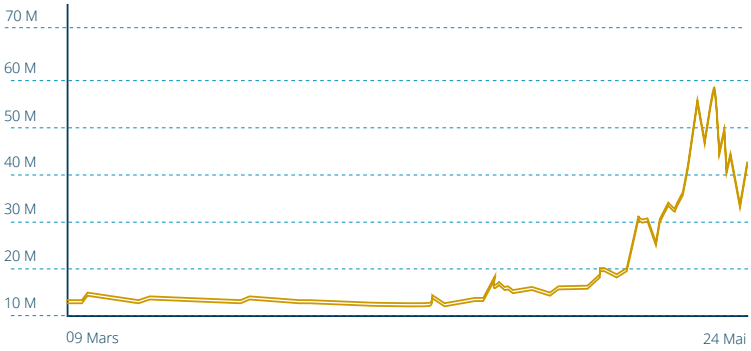
> *Si une entreprise est bonne, sa valeur boursière finira par augmenter.*
> Warren Buffet

Graphique 5 : Bitcoin sur 180 jours



Bitcoin : la première et (pour l'instant) la plus importante de toutes. Pour le moment, le Bitcoin est aux crypto monnaies ce que le dollar est à la finance classique. Quand la valeur du Bitcoin augmente, celle de la plupart des autres monnaies suit le mouvement, et vice-versa. Ceci est dû au fait que la plupart des crypto monnaies ne peuvent s'acheter qu'avec des Bitcoins.

Graphique 6 : Darkcoin sur 90 jours



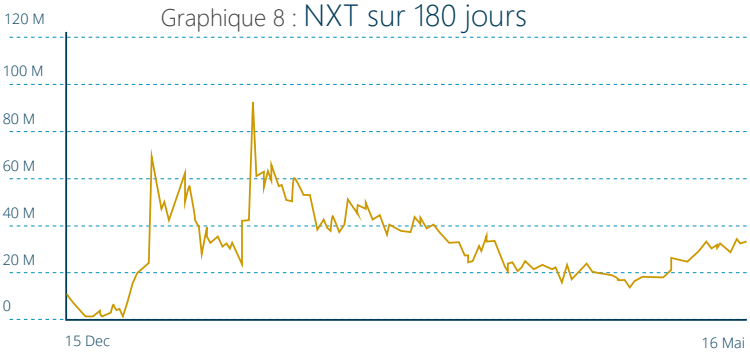
Darkcoin. Une monnaie PoW qui ajoute la confidentialité. Très volatile.

Graphique 7 : Peercoin sur 180 jours

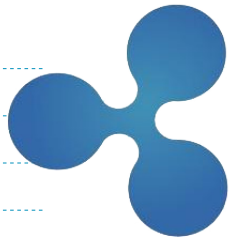
Peercoin. Une combination de PoS et PoW. En diminution régulière, faible communauté.

NXT. Une véritable monnaie de seconde génération et la monnaie PoS la plus importante. Communauté très active. De nombreux développements en cours. Le seul marché décentralisé sans frais au monde (hors frais de transactions). NXT est une des très rares monnaies à pouvoir être achetées via des monnaies fiat. (https://www.ccedk.com/ and https://bter.com/). En train de croître.

Graphique 8 : NXT sur 180 jours



Graphique 9 : Ripple sur 180 jours



Ripple. Non décentralisée. Créé par une compagnie qui possède toujours une majeure partie de la masse monétaire et agit comme autorité centrale. Décroît.

YOUR FUTURE IS NXT

Vous voulez que les choses aillent vite ? Elles iront plus vite que vous n'y comptiez.

20 développeurs, 150 participants actifs, une communauté estimée à environ 45 000 utilisateurs NXT, incluant des économistes, conseillers financiers, traders, programmeurs, mathématiciens, cryptographes, gestionnaires de projets, chefs d'entreprises, professeurs, etc. Actifs 24 heures sur 24, 7 jours sur 7, avec des dizaines de projets en cours, les choses avancent vite.

De toutes les crypto monnaies, NXT est la seule à mener le concept de décentralisation aussi loin. En effet, la plupart des autres monnaies offrent peu de foncionnalités de plus que Bitcoin. La communauté NXT, en revanche, a créé un environnement technique avancé et un ensemble d'outils financiers qui placent le NXT clairement en tête de la compétition.

Fonctionnalités techniques actuelles :

- **Preuve d'Enjeu** (*Proof of Stake*) : comme expliqué précédemment, le système PoS est non seulement un moyen efficace économiquement de maintenir la blockchain, mais il est également immunisé contre les attaques 51%.

- **Porte-monnaie dans la tête** (*brain wallet*) : NXT, contrairement aux autres crypto monnaies, ne nécessite pas un fichier (porte-monnaie) sur un ordinateur local afin d'enregistrer les informations d'identification. Ce fichier est considéré par la communauté NXT comme étant un risque : si le fichier est perdu pour une raison quelconque, il n'y a plus moyen de récupérer les informations contenues dedans, et donc l'argent de l'utilisateur est définitivement perdu. C'est pourquoi il est fortement recommandé de sauvegarder ces fichiers de façon sécurisée. NXT, en revanche, utilise un brain wallet. Les utilisateurs doivent juste imaginer une passephrase (un mot de passe long, comme "J'ad0re les crypt0 monnaies, et j'aimerais avoir pl3in de NXT"). Cela s'appelle un brain wallet car, de n'importe où, la seule chose nécessaire pour accéder à son compte est la passephrase à taper dans un logiciel client. C'est une méthode à l'épreuve des voleurs et des pirates, qui permet de traverser aisément les frontières, et aucun fichier ne peut être perdu.

- **Les pièces teintées** : c'est une méthode pour suivre l'origine des pièces NXT, de façon à ce qu'il soit possible de mettre de côté un certain nombre de pièces, permettant à certaines personnes de les utiliser d'une manière particulière. De telles pièces peuvent représenter des jetons numériques, comme des actions, obligations, *smart property* (propriété dont la possession est contrôlée via une *blockchain*), etc. Ces jetons peuvent même représenter des objets physiques.

- **Beaucoup plus d'adresses que Bitcoin** : il y a 2^{160} adresses possibles avec Bitcoin, tandis que NXT en a 2^{256} (c'est 100 millions de milliards de milliards de fois plus que Bitcoin). Le résultat est qu'il est beaucoup moins probable d'avoir des doublons d'adresses.

Usages économiques et financiers :

NXT, en tant que crypto monnaie, peut et sera probablement utilisée de la même façon que le Bitcoin. Sur ce point, les deux monnaies sont des concurrentes directes. Mais NXT, grâce à son architecture technique et à sa communauté dévouée, offre beaucoup plus :

- NXT est la seule monnaie à avoir implémenté une plateforme d'échanges décentralisée, appellée Asset Exchange (AE). Contrairement aux bourses classiques, l'Asset Exchange n'est pas "géré" par qui que ce soit. Il est totalement décentralisé, basé sur la blockchain de NXT, et les frais sont limités (1 NXT par transaction, 1000 NXT pour créer un *asset*).

  Cet Asset Exchange, lancé le 11 mai 2014, a rapidement vu de nombreux assets mis à disposition et échangés, tells que des fonds communs de placement, des matières premières (argent, autres crypto monnaies), des introductions en bourse de start-ups, etc. C'est un endroit où les idées d'entreprises peuvent facilement trouver financement.
  Cela fonctionne beaucoup comme une place boursière classique, moins les lourds frais de transaction et la réglementation. En effet, l'AE étant décentralisé, il n'y a pas moyen de lui imposer une réglementation. Cela peut être vu comme un point négatif par les investisseurs académiques, mais c'est une assurance de qualité pour le capital risque et les premiers utilisateurs. Les "assets" sont mis sur le marché comme des pièces teintées, comme expliqué ci-dessus.

- La communauté NXT a organisé un système de subvention pour start-up pour aider au développement d'activités commerciales autour de NXT. Cela garantit qu'il y aura du financement pour participer à la croissance de NXT.

- Des fonds communs de placements sont créés pour investir dans le monde des crypto monnaies. Ceci étant un domaine particulièrement technique, des spécialistes, tout comme dans le monde classique de la finance, investissent l'argent de leurs clients en s'appuyant sur leurs connaissances du milieu, afin de pouvoir payer des dividendes proportionnellement aux gains réalisés. Le premier à avoir vu le jour est jl777hodl, bientôt suivi par Sharkfund0, CryptoCoins, SuperNet, etc.

- MultiGateway : cet outil va bientôt permettre aux utilisateurs de l'Asset Exchange d'échanger d'autres crypto monnaies, soit au travers de NXT, soit directement entre elles. Les plateformes d'échanges classiques ne permettent l'échange que d'un nombre limité de paires de monnaies (l'une des plus populaires, BTer, maintient 30 paires basées sur Bitcoin, et 7 sur Litecoin), tandis que le système MultiGateway permettra à terme à n'importe quelle paire d'être créée et échangée. Cela ne nécessitera qu'un acheteur et un vendeur.
  De plus, les nouvelles monnaies qui ont toujours besoin de se battre pour être ajoutées à ces plateformes d'échanges pourront être directement échangées via ce système.

Projets en cours :

- Confidentialité : en juillet 2014, Bitcoin et la plupart des autres crypto monnaies manquent de confidentialité. Les développeurs NXT travaillent sur une solution pour permettre d'effectuer des transactions sûres et confidentielles avec NXT.
- NXTHaus sera le lien direct entre le monde fiat et NXT. De cette manière, NXT sera la première crypto monnaie à avoir son propre échange fiat-crypto. Les utilisateurs de Bitcoins doivent s'appuyer sur une plateforme tierce. Les utilisateurs NXT pourront s'en passer.
- InstantDex : ce service construit sur le service MultiGateway et l'Asset Exchange permettra l'échange direct en temps réel entre différents assets de l'Asset Exchange.
- VCorp : la communauté NXT est en train de developper un cadre de travail de façon à ce que des entrepreneurs avec des idées de business à developer dans le monde virtuel puissent le faire directement dans ce monde. Le système de livre de comptes public de NXT sera utilisé pour stocker des rapports financiers destinés aux investisseurs de telles entreprises.
- Marketplace : des développeurs on créé un magasin décentralisé pour biens numériques. Ce service est en concurrence directe avec Amazon et iTunes. Il est également prévu de créer un site décentralisé d'enchères en ligne, en concurrence directe avec Ebay qui, au contraire, est centralisé.
- NXTStudios : il s'agit du premier studio de divertissement et de média décentralisé, reposant sur la communauté NXT. Le but principal est d'apporter du support à NXT pour le lancement sur le marché de son écosystème, de ses services financiers et de ses produits logiciels grâce à des équipes créatives.
- NXT Legal : c'est un projet à but non lucratif pour apporter une aide juridique aux possesseurs de NXT à propos de leurs besoins légaux concernant NXT et son utilisation. L'objectif est le développement d'un ensemble de bonnes pratiques dans différentes juridictions dans le monde.
- Cryptamail : avec Edouard Snowden révélant au monde à quel point la NSA envahissait la spère privée, le besoin de plus de confidentialité est devenu particilièrement évident. Cryptamail est la réponse à ce besoin en ce qui concerne la messagerie électronique, en combinant une communication sûre et le pouvoir de la décentralisation (ce qui implique qu'il n'y a pas de localisation centralisée, pas de serveur central, et aucune tierce partie en qui faire confiance).

Entreprises :

- Gocoin : cette entreprise de traitement de paiements est une tierce partie permettant aux commerces d'accepter facilement les paiements en Bitcoin et d'autres crypto monnaies, parmi lesquelles NXT.

- De plus en plus de magasins en ligne se sont mis à accepter NXT en plus de Bitcoin, comme BitcoinBazaar, Coinverted, NXTShop.eu, ArbilnnovateID, BrieHost, Crypto Jeweler, Bitezze, etc.

- NXTVenture : c'est une compagnie virtuelle pésente sur l'Asset Exchange qui vise à devenir un hybride Capital Risque / Banque d'investissement. Elle investit dans des entreprises et ensuite offre des assets basés sur ces investissements via l'Asset Exchnage.

- Lith, le MMO NXT : ce jeu multijoueur en ligne (*Massive Multiplayer Online game*), comme tous les jeux de ce type, offrira une monnaie en ligne. Contrairement aux monnaies virtuelles d'autres jeux similaires comme Diablo ou World of Warcraft, cette monnaie est une vraie monnaie, NXT, créant ainsi un lien entre le monde du jeu et le réel. Lith est un jeu développé par DORCS, une compagnie présente sur l'Asset Exchange.

- NXT Mania Games : cette compagnie développe des jeux pour les smartphones. Les joueurs pourront entrer en compétition les uns contre les autres et parier avec des NXT sur le résulat. Cette entreprise est également présente sur l'Asset Exchange.

- LocalNXT : ce site Web permettra à ses utilisateurs d'acheter et vendre des NXT sans intermédiaire, via le moyen de paiement qu'ils choisiront (Cash, Paypal, virement bancaire, etc.)

- NXTStore : ce projet prévoit d'offrir une plateforme pour héberger des "magasins" indépendants, à l'image de ce qui se fait sur Ebay.

- NXTKey : il s'agit d'une clé USB capable de contenir la ou les passephrase(s) de l'utilisateur, permettant d'accéder aux NXT présents sur les comptes correspondants sans avoir à taper les passephrases.

- NXTSafe : c'est un "crypto coffre-fort" analogique qui peut stocker la passephrase de quelqu'un sans aucun lien avec le monde numérique.

Non seulement NXT en tant que monnaie a beaucoup d'avantages sur sa concurrence, mais un nouveau cadre économique est en train d'être développé, ce qui pousse beaucoup d' observateurs à penser que le futur de NXT est très prometteur.
De plus, le fait que la plupart des projets NXT soient encore en développement signifie que la valeur du NXT est amenée à augmenter une fois que les services constitutifs de ce cadre de travail seront ouverts au public.

QUESTIONS FRÉQUEMMENT POSÉES :

1. *Les crypto monnaies peuvent facilement être utilisées pour des activités illégales, blanchiment d'argent, traffic d'armes et de drogues, terrorisme, etc. Les gouvernements ne vont-il pas tout faire pour empêcher cela ?*

Aucune de ces activités n'a attendu l'arrivée des crypto monnaies pour être pratiquée. Si la potentielle utilisation illégale était un argument valide contre l'adoption des crypto monnaies, alors le dollar américain, en tant que moyen de paiement principal pour nombre d'activités illégales de par le monde, devrait être bani également. Les crypto monnaies ne peuvent pas être rendues plus responsables de ce que les criminels font avec elles que les monnaies fiat ne le sont aujourd'hui.
De plus, les crypto monnaies sont basées sur des organisations décentralisées. Elles ne peuvent pas être "arrêtées". Elles existent parce que des gens partout dans le monde veulent qu'elles existent. Une banque peut être fermée. Pas une crypto monnaie. A titre de comparaison, une interdiction de partage de fichiers de musique et de films a été tentée par certains gouvernements dans le monde, sans aucun succès.

2. *Les crypto monnaies ne s'appuient sur rien. Leur valeur n'est-elle pas seulement spéculative ?*

Depuis 1971, le dollar ne s'appuie plus sur rien. En fait, depuis cette date, il a perdu 73% de sa valeur à cause de l'inflation. La valeur des crypto monnaies vient de leurs réseaux d'échanges et des services qu'elles offrent. Certaines d'entre elles, comme NXT, ne peuvent même pas être inflationnistes.

3. *Les crypto monnaies ne sont pas réglementées. Cela ne constitue-t-il pas un risque ?*

Cela peut être considéré comme un risque pour ceux ne comprenant pas comment les utiliser. Mais les monnaies fiat ont été non réglementées pendant la majeure partie de l'Histoire, et il semblerait aujourd'hui qu'une part considérable du risque vienne de la réglementation elle-même, surtout des changements de réglementation.
L'industrie financière est l'une des plus réglementées au monde. Malgré cela, les crashs et les crises surviennent régulièrement, appellant à encore plus de réglementation.

4. *N'est-il pas possible que Bitcoin soit cracké ? N'est-ce pas là ce qui s'est produit avec Mt Gox ?*

Le réseau Bitcoin existe depuis 2009. Des millions de dollars y sont échangés tous les jours, en dehors du contrôle d'une quelconque autorité centrale. Bien qu'il soit impossible de dire que Bitcoin ne sera jamais cracké, les chances que cela se produise s'amenuisent chaque jour qui passe.
Selon la rumeur, MT Gox fut victime d'un tel crack. En fait, ce n'est pas ce qu'il s'est produit. Le problème principal avec Mt Gox était lié à de mauvaises procédures internes. Tout comme Lehman Brothers, par exemple.

> *Il existe une chose plus puissante que toutes les armées du monde, c'est une idée dont l'heure est venue.*
> Victor Hugo

Les crypto monnaies sont arrivées et, tout comme Internet, le partage de fichiers, et l'information libre, elles ne peuvent être arrêtées. Le monde de la finance est sur le point de changer drastiquement, la tempête arrive.
Comme d'autres industries qui ont eu à faire face à des changements disruptifs, l'industrie de la finance (dont les banques, la gestion de fonds, les assurances, la gestion de fortune, les organismes de crédit, etc.) devra s'adapter. Ceux qui ne le feront pas vont vite se trouver remplacés par ceux qui l'auront fait.

En tant qu'acteur important de ce monde, vous vous devez de prendre part à la révolution des crypto monnaies qui est sur le point de frapper l'industrie de la finance.
Mais la concurrence, déjà intense, va s'intensifier beaucoup plus avec de nombreux nouveaux arrivants dans une industrie offrant des services sur mesure touchant aux crypto monnaies.

Ces nouveaux arrivants ne se contenteront pas de prendre part à la révolution des crypto monnaies. Ils vont, en fait, la mener. A moins d'être parmi eux, vous ne serez nulle part.

Alors, soyez là...

Crypto
Finance
Analysis
Consulting

Crypto Finance Analysis Consulting, votre partenaire dans le monde de la crypto finance.

CFA Consulting aide les entreprises à mettre un pied dans le secteur de la crypto finance. Que ce soit avec le Bitcoin, NXT, Darkcoin, ou toute autre crypto monnaie ou investissement dépendant du secteur de la crypto finance, CFA Consulting est là pour vous aider à comprendre les enjeux et à tirer profit de ces technologies révolutionnaires.

Banques, assurances, gestionnaires de fonds et de fortune, entreprises du Net, petites capitalisations nécessitant plus d'investissements, capital risqueurs, entreprises ayant besoin de levées de fonds, crowdfunding... Vous êtes tous invités à découvrir avec nous quelles sont vos options.

Nous vous accompagnerons dans le monde des crypto monnaies en adaptant vos stratégies à leurs possibilités et limites, en gérant leurs aspects technique, sécuritaire, et économique, et en créant un environnement dynamique, de façon à ce que votre entreprise puisse surfer sur la vague crypto, en laissant vos concurrents loin derrière.

Nous pouvons participer à la définition de votre business plan, vous fournir des experts entraînés tels qu'avocats, fiscalistes, traders, analystes informatiques, web designers et développeurs, puis vous accompagner tout au long de votre expérience crypto.

Nous offrons également des sessions de formation certifiantes ainsi que des solutions informatiques sur mesure, de façon à ce que vous puissiez vous appuyer sur du matériel et logiciel sécurisés.

CFA Consulting, une entreprise suisse pour un monde de la finance sans frontière.

Florine Oury,
Head of Marketing and Communication

Jean-Laurent Tari,
Chief Executive Officer

Yann Wahli,
Chief Financial Officer