Bitcoin (BTC) : une nouvelle monnaie - 1/7

Le Bitcoin (BTC) est une nouvelle monnaie, totalement décentralisée, dont le but est d'être analogue à de l'or version électronique. Inventée début 2009, ce n'est que depuis 2011 que cette nouvelle monnaie se développe vraiment et promet la richesse aux early adopters.

Qu'est-ce que Bitcoin (BTC) ?

Le Bitcoin (j'utiliserai "BTC" pour désigner la monaie et "Bitcoin" pour désigner le réseau dans la suite – tous deux se prononçant "Bitcoin") est une monnaie virtuelle totalement décentralisée et anonyme, c'est-à-dire qu'il n'y a aucun organe central – comme les banques et les états – pour la contrôler. Ainsi, le réseau est autogéré par les membres de celui-ci, il n'y a aucun serveur central qui gère les transactions ou l'émission de BTC.
Pour faire simple, si vous voulez utiliser des BTC, vous téléchargez un petit logiciel. Après l'avoir lancé, ce logiciel se synchronise avec les autres membres et votre ordinateur fait alors partie du réseau Bitcoin.

Comme il n'y a pas d'organisme central pour gérer les transactions (et savoir qui possède des BTC ou non), tout le monde est en permanence au courant de toutes les transactions qui ont lieu sur le réseau et donc de qui possède des BTC et qui n'en possède pas. C'est aussi pour cela, au contraire des monnaies classiques, les transactions en BTC mettent plusieurs minutes à arriver à leur destinataire : pour qu'une transaction soit considérée comme réelle, il faut qu'un ou plusieurs membres du réseau Bitcoin la confirment.

Bitcoin est une monnaie cryptographique, c'est-à-dire qui s'appuie sur des propriétés mathématiques et cryptographiques assez complexes aussi bien dans la gestion du réseau que dans la génération des Bitcoin. Nous n'aborderons volontairement pas dans le détail ces notions trop complexes pour un article d'introduction.

A quoi servent les BTC ?

Comme toute monnaie, les BTC peuvent être échangés contre des biens, des services ou tradées contre d'autres devises. Vous trouverez une liste de services acceptant les BTC sur le wiki – plus ou moins officiel - https://en.bitcoin.it/wiki/Trade. Plutôt que de parler de monnaie (qui permet de simplifier l'image de Bitcoin), il serait plus approprié de parler d'un bien puisque le BTC s'apparente beaucoup plus à un morceau d'or : vous envoyez quelques grammes – ou milligrammes – de BTC pour payer.

Ainsi, le BTC possède un cours, un peu un comme un cours de bourse, fonction de l'offre et de la demande en achat et en vente de BTC. La plus grosse place de marché est MT.Gox. Le cours du BTC a varié entre $2 et $29 sur l'année 2011.

Comment Bitcoin fonctionne-t-il ?

Conçue pour être analogue à l'or, Bitcoin se décompose en 2 parties bien distinctes :
- Le wallet, c'est-à-dire l'endroit où vous stockez votre "or" et duquel vous pouvez donc envoyer et recevoir des BTC.
- La génération des BTC (mining), c'est-à-dire le programme qui réalise des calculs cryptographiques lourds et qui, en échange, reçoit des BTC lorsqu'il découvre un bloc ayant des propriétés particulières.

Le portefeuille Bitcoin (wallet)
Ce programme est plus ou moins analogue à votre compte bancaire, sauf qu'il n'est pas stocké dans une

Bitcoin (BTC) : une nouvelle monnaie - 2/7

banque mais sur votre ordinateur. Le programme le plus utilisé est le programme originel de Bitcoin.org (open source), mais il en existe de nombreux autres, y compris certains qui s'exécutent en ligne comme https://blockchain.info/wallet ou https://strongcoin.com. Lorsque vous lancez ce programme, vous faites partie du réseau Bitcoin au sens propre, c'est-à-dire que vous êtes tenu au courant en permanence de toutes les transactions, générations de BTC, etc. Vous pouvez alors générer des adresses Bitcoin (exemple : 1NDiQEFjAoyp6Vx7z1tLaJVdNw1hmvS5Mn) : c'est grâce à ces adresses que vous pouvez recevoir des BTC, ce sont en quelques sortes vos identifiants sur le réseau Bitcoin, un peu analogue à votre adresse e-mail pour recevoir des mails. Vous pouvez générer autant d'adresses que vous le souhaitez, c'est totalement gratuit et ça ne prend qu'un clic, par exemple pour garder une trace de qui vous envoie des BTC. De même, si vous souhaitez envoyer des BTC, il vous suffit d'indiquer à quelle adresse vous souhaitez envoyer les BTC et cliquer sur le bouton d'envoi, c'est aussi simple que cela. Le réseau est totalement anonyme et rien ne permet de relier une adresse Bitcoin à quoi que ce soit d'identifiable, sauf si bien sûr vous publiez volontairement cette adresse !

Comme précédemment évoqué, lorsque vous recevez des BTC, ils ne sont pas immédiatement disponibles sur votre compte, vous devez attendre qu'un certain nombre de nœuds ("peers") confirment la validité de la transaction (ce que l'on appelle tout simplement des "confirmations"). Pour accélérer ce processus de validation qui peut prendre plusieurs dizaines de minutes, l'émetteur de la transaction peut "payer" pour s'assurer une validation rapide. Ces frais ("fees") sont ensuite redistribués lors de la génération suivante de BTC.

Attention, toute transaction est définitive, irréversible. Si vous vous faites voler votre wallet, vous ne pourrez pas appeler de banque pour récupérer votre argent. De même, si vous perdez votre wallet (le fichier "wallet. Dat" étant le seul indispensable à sauvegarder), vous n'aurez plus aucun moyen d'accéder à votre argent. AUCUN. Prenez donc bien soin de votre fichier wallet. Dat, encryptez-le (en activant l'option dans le logiciel) et surtout sauvegardez-le régulièrement, notamment chaque fois que vous générez une nouvelle adresse. Vos BTC ne sont pas physiquement contenus dans ce fichier – ils ne sont nulle part et partout à la fois, puisque tout le monde sait à tout moment quelle adresse possède combien de BTC – mais il contient la clé privée associée à chacune de vos adresses, qui seule permet d'utiliser les BTC qu'elle contient.

La génération de Bitcoins (mining)
Rendu à ce stade de la lecture, vous devez vous demandez d'où sortent les BTC, comment en obtenir. La réponse est simple et analogue à ce qu'il se passe avec l'or : en "piochant" !

Commençons par le commencement : l'or est présent en quantité finie sur Terre. Au début de la ruée vers l'or, celui-ci était relativement facile à obtenir puis, de plus en plus de gens partant à sa recherche, il est progressivement devenu de plus en plus difficile d'en découvrir. Et il arrivera un jour où tout l'or de la Terre aura été découvert et mis en circulation.

Pour les BTC, c'est exactement la même chose en version électronique. Vous installez et faites tourner une pioche virtuelle sur votre ordinateur, un programme appelé "miner" (mineur). Il en existe de très nombreux, open-source pour la plupart, on y reviendra tout à l'heure. Ce programme effectue une très grande quantité de calculs cryptographiques pour tenter de trouver un bloc ayant une propriété particulière ("block"). Ce type bloc est très difficile à trouver, cette difficulté étant auto adaptée par le réseau toutes les 2 semaines (2016 blocks) pour qu'en moyenne un bloc soit découvert toutes les 10 minutes. Lorsque vous découvrez un bloc, vous êtes récompensé par un certain nombre de BTC – 50 au moment de l'écriture de cet article. La récompense ("block reward") varie au cours du temps et ne sera plus que de 25 en décembre 2012 par exemple, puisque, tout comme l'or, plus le temps passe et plus il devient difficile de trouver de nouvelles mines. Tous les 4 ans environ (210 000 blocks), cette récompense est divisée par deux. La courbe de

Bitcoin (BTC) : une nouvelle monnaie - 3/7

génération des BTC est d'ores et déjà établie. Ceci assure notamment que l'inflation liée à la génération "spontanée" de BTC est déterminée.

Un difficulté de 1 signifie qu'il faut en moyenne 2^32 (soit 4 294 967 296) calculs (hashs) pour trouver un bloc. Au 26 février 2012, la difficulté est de 1 376 302, soit en moyenne 5.9×10^15 hashs pour trouver un bloc !

Le problème est que la puissance de calcul du réseau est tellement considérable qu'il faut en pratique plusieurs mois, voire plusieurs années, sur un ordinateur actuel pour découvrir un bloc ! C'est pourquoi sont nées les "pools" (exemple : Deepbit, le plus gros pool à ce jour), qui sont des regroupements de mineurs. Lorsque l'un des mineurs découvre un bloc, la récompense est partagée entre tous les membres du pool qui ont participé à son calcul, au prorata de la puissance de calcul fournie (il existe d'autres modes de récompense en fonction des pools, que nous ne développerons pas). En contrepartie, le pool s'attribue une petite partie de la récompense (entre 0 et 5%, 3% en général) pour compenser les frais (serveurs, etc.) engagés.

Terminons cette partie par le fait que miner sur un processeur, même très puissant, est très fortement inefficace et vous coûtera bien plus cher en électricité que la récompense en BTC. Pour miner avec un bilan économique positif, vous devez miner sur votre carte graphique ou sur un matériel spécialisé (FPGA ou autre). La page https://en.bitcoin.it/wiki/Mining_hardware_comparison vous permettra de savoir quoi acheter pour miner efficacement, les cartes AMD (ex ATI) étant beaucoup plus efficace dans ce travail que les cartes nVidia. En effet, les cartes graphiques sont équipées d'un très grand nombre de processeurs de flux ("stream processors", 3200 par exemple sur une AMD Radeon 5970) qui exécutent chacun les calculs en parallèle. Pour donner un ordre d'idée, un processeur type Core i7 960 (3,2 GHz) va miner à environ 20 MH/s (ie 20 000 000 de tentatives par seconde), tandis qu'une carte AMD Radeon 5970 va miner à un minimum de 650 MH/s, soit plus de 30 fois plus vite.

Comment miner pour obtenir des BTC ?
Inscrivez-vous tout d'abord sur un pool, par exemple Slush's pool ou Deepbit. Une fois identifié, renseignez votre adresse Bitcoin pour recevoir vos récompenses, puis créez un (ou plusieurs) "worker", c'est-à-dire un identifiant que va permettre à votre logiciel de s'identifier sur le pool. Vous devez créer autant de worker que vous allez avoir d'instances de logiciel qui vont s'exécuter en parallèle, si vous avez 2 ordinateurs que vous souhaitez faire miner alors créez 2 workers, par exemple.

Téléchargez ensuite un logiciel mineur, comme par exemple Ufasoft's Bitcoin Miner qui est simple, rapide et surtout très facile à configurer. Quand vous connaitrez mieux Bitcoin, vous découvrirez des logiciels comme CGMiner qui sont très complexes à configurer mais qui permettent également de faire des choses très intéressantes (overclocking, contrôle de la vitesse des ventilateurs, etc.). Enfin, lancez votre mineur avec la ligne de commande suivante :

bitcoin-miner.exe -a 5 -o ADRESSE_DE_VOTRE_POOL -u IDENTIFIANT_DE_VOTRE_WORKER -p MOT_DE_PASSE_DE_VOTRE_WORKER

L'adresse de votre pool est indiquée par le pool, c'est, par exemple, http://pit.deepbit.net:8332 dans le cas de Deepbit. Le logiciel va alors vous indiquez qu'il a généré des "shares", c'est-à-dire des tentatives de résolution du bloc et qu'il les a envoyées au pool qui l'a accepté ou refusé. Si vous minez juste avec votre CPU, la résolution d'une share peut prendre plusieurs minutes ! Vous générez en moyenne une share tous les 2^32 tentatives, et donc il faut en moyenne générer autant de share que la difficulté du moment pour trouver un bloc.

Bitcoin (BTC) : une nouvelle monnaie - 4/7

Comment obtenir des Bitcoins sans miner ?

Vous pouvez acheter des BTC sur une place de marché telle que MT.Gox. Vous pouvez également obtenir quelques fractions de BTC gratuitement sur des services comme Free Bitcoins (il en existe de nombreux autres).

Le système Bitcoin possède-t-il des failles ?

En l'état des connaissances mathématiques et cryptographiques, le système Bitcoin est totallement sécurisé. Néanmoins, il possède quelques faiblesses potentielles inhérentes à sa nature distribuée sans organe de contrôle central, notamment :

- Si un attaquant possède plus de 50% de la puissance de calcul du réseau Bitcoin, il pourrait notamment inverser ses transactions ou interdire les autres participants de générer des BTC en minant. La puissance de calcul du réseau Bitcoin est actuellement tellement importante que la réalisation de cette attaque est proche de l'impossible et surtout très loin d'en valoir le coût.
- L'attaque "double dépense" (double-spending attack) : comme son nom l'indique, un utilisateur dépense plusieurs fois ses BTC. Cette attaque est théoriquement possible car il n'y a pas d'établissement central permettant de valider les transactions, mais, à la place, il y a des millions de peers qui jouent ce rôle ! C'est pour prévenir cette attaque que vous devez attendre des confirmations avant de pouvoir considérer des BTC comme vous appartenant. Nous considérons que 6 confirmations permettent d'assurer la validité du transfert en raison de la décroissance exponentielle de la possibilité de fraude avec le nombre de confirmations. Lisez cet article pour les détails : http://bitcoin.stackexchange.com/questions/1170/why-is-6-the-number-of-confirms-that-is-considered-secure
- La plus grosse faille concerne la perte du wallet. Considérez que si vous perdez les clés de votre maison, vous perdez votre maison. Si vous vous faites voler vos clés, vous perdez votre maison également. Vos clés sont donc extrêmement précieuses ! Je vous conseille fortement d'utiliser un service comme https://blockchain.info/wallet ou https://strongcoin.com qui vont stocker vos clés – dont vous pourrez faire un backup crypté sur votre compte Dropbox ou votre E-mail, "au cas où" le service que vous utilisiez disparaissait. Grâce à ce backup, vous pourrez alors récupérer votre accès à vos BTC :) De même que des tonnes d'or sont perdues chaque année, il en va de même avec les BTC : des milliers sont perdus chaque année par des gens perdant leurs clés. N'en faites pas partie ! Inversement, sans vos clés, PERSONNE ne peut toucher à vos BTC, pas même un état ou une banque.
- N'importe qui pouvant tracer l'intégralité des transactions, il est parfois possible de relier des adresses à des identités réelles (par exemple telle personne a acheté sur tel site via telle adresse, donc je sais que cette adresse appartient à telle personne) et ainsi remonter, de fil en aiguille, les identités.

Il existe également d'autres faiblesses, listées sur cette page, mais qui sont trop techniques pour être dans le champ de cet article.

Existe-t-il des alternatives à Bitcoin ?

Il est très facile de créer une monaie alternative "comme Bitcoin" (mais incompatible), en modifiant le bloc initial. De nombreuses devises ont ainsi vu le jour, comme Namecoin, Litecoin, Devcoin, etc. Mais elles sont toutes très loin d'avoir l'aura de Bitcoin... Et sa valeur d'échange ! Par exemple, au jour de la rédaction de cet article, 300 NMC (Namecoin) valent environ 1 BTC, alors qu'un NMC est seulement 10 fois plus simple à miner qu'un BTC.

Bitcoin (BTC) : une nouvelle monnaie - 5/7

Comment accepter les paiements en Bitcoins ?

Pour recevoir des BTC, rien de plus simple, il vous suffit d'installer un wallet.
Pour accepter les paiements en BTC sur votre site Internet, il existe plusieurs services permettant de le faire facilement comme BitcoinPayFlow ou Bit-Pay. Si vous êtes un peu plus pointu et que vous ne souhaitez pas vous appuyer sur un prestataire externe, la page http://bitcoin.stackexchange.com/questions/126/how-can-i-accept-bitcoins-on-my-website vous intéressera certainement.

J'ai lu/vu/entendu que Bitcoin pouvait être utilisé pour du blanchiment d'argent ou de la pédophilie, est-ce vrai ?

Bitcoin fonctionne à l'inverse du système monétaire classique : toutes les transactions sont connues de tous, mais les "comptes bancaires" (les adresses Bitcoin) sont anonymes. Ainsi, il est facile, pour n'importe qui, "d'écouter" le réseau à la recherche de transactions anormales (en nombre ou en montant) et, plus ou moins facilement, de remonter jusqu'à une ou plusieurs identités réelles (par exemple grâce aux places de marché permettant de convertir les BTC en devise) par corrélation.

Malheureusement, il existe des services permettant de brouiller les pistes – dont je ne fournirai pas les adresses – en transférant les BTC d'une adresse vers une ou plusieurs autres en suivant – ou non – un planning pré-établi. Le fait qu'il est possible de se générer autant d'adresses que nécessaires (plusieurs milliards si vous le souhaitez... Mais votre wallet. Dat risque alors d'être "un peu" lourd...), permet de brouiller les pistes facilement.

Comment Bitcoin peut-il évoluer puisqu'il n'y a personne pour le réguler ?

Par vote, comme en démocratie. Si vous êtes d'accord avec une fonctionnalité, utilisez un logiciel qui la supporte, et, si vous n'êtes pas d'accord, un logiciel qui ne la supporte pas. L'implémentation du système fait que si une fonctionnalité est "votée" (donc implémentée) par plus de 50% de la puissance de calcul alors elle peut être utilisée.

Est-il possible de détruire le réseau Bitcoin ?

Théoriquement oui, mais en pratique non, Bitcoin est indestructible. Il est impossible détruire le réseau lui-même, car il n'est basé sur AUCUN organe central et un réseau comme Tor (anonymisateur) permettrait de l'utiliser même si le protocole était interdit dans un pays donné. Pour que le système Bitcoin continue de fonctionner, il suffit que le protocole soit autorisé dans au moins 1 pays. Nous pouvons donc considérer cette situation comme impossible, d'autant plus que le réseau n'est pas figé et le protocole peut évoluer.

Un autre risque est que le Bitcoin devienne trop peu utilisé et qu'une entité malveillante possède plus de 50% de la puissance de calcul. Si cette attaque réussi, alors le réseau perdurerait mais deviendrait de fait inutile, l'attaquant ayant tué l'intérêt de son attaque.

Si les algorithmes mathématiques et cryptographiques sous-jacents au réseau devenaient un jour faillibles, la preuve mathématique serait très probablement réalisée bien avant la réalité pratique de l'attaque.
Rappelez-vous 2 choses :

Bitcoin (BTC) : une nouvelle monnaie - 6/7

- Le cœur de Bitcoin est basé sur de la cryptographie, les développeurs des clients Bitcoin et la communauté se doivent donc être au top de l'état de l'art de la recherche en la matière.
- Bien que ça remettent en cause beaucoup de chose, Bitcoin peut changer d'algorithmes (lisez https://bitcointalk.org/index.php?topic=191.msg1585#msg1585 pour en savoir plus).

Conclusion

Totalement analogue à l'or, la valeur d'un BTC est purement spéculative. Il est aujourd'hui relativement facile d'obtenir des BTC et la difficulté va s'accentuer, et donc sa valeur (normalement) décoller. De même, plus le système sera utilisé et plus la valeur d'un BTC augmentera. Les early adopters devraient donc devenir riches et le méritent pour avoir joué un rôle clé dans le développement de Bitcoin :)

Miner sur un CPU est inefficace et présente un bilan économique négatif. Vous devez miner sur votre carte graphique ou sur un hardware spécialisé pour espérer tirer profit. Si vous croyez en Bitcoin, vous pouvez également acheter des BTC sur un exchange tel que MT.Gox. Néanmoins, la difficulté s'adaptant automatiquement, plus il y a de personnes qui minent et plus la difficulté pour obtenir un BTC augmente. Mais, parallèlement, plus la valeur d'un BTC augmente.

Si vous souhaitez vous amuser avec l'histoire de Bitcoin, je vous conseille l'épisode 13 de la saison 3 de la série The Good Wife intitulé "Bitcoin for Dummies", qui reprend des éléments réels (par exemple, personne ne sait qui se cache derrière le pseudonyme de Satoshi Nakamoto, le créateur de Bitcoin, et la communauté essaie de faire comprendre aux autorités qu'un BTC est un bien – comme l'or – et non une monnaie).

Un peu comme le poker, il faut 5 min pour comprendre les règles générales de Bitcoin, mais beaucoup plus de temps – une vie entière ? – pour en comprendre en détail le fonctionnement :)

Liens utiles

Attention, quasiment toutes les resources disponibles relatives à Bitcoin sont en anglais ! Il n'y a aucun site officiel, Bitcoin étant, par nature, P2P, à l'exception du site bitcoin. Org qui héberge le programme "originel" et opensource. La communauté Bitcoin fonctionne sur le même principe, avec des sites qui sont des standards "de facto".

http://bitcoin.org : le programme "originel" vous permettant de gérer vos Bitcoin
http://www.weusecoins.com : le "comment ça marche" du Bitcoin
https://en.bitcoin.it : le wiki qui répondra à toutes vos questions – posez les à Google, le site étant très bien référencé les pages les plus pertinentes remonteront automatiquement dans vos recherches
https://bitcointalk.org : le forum de facto officiel de Bitcoin
http://fr.wikipedia.org/wiki/Bitcoin : la page Wikipedia, si vous voulez en savoir plus
https://blockchain.info/charts : plein de graphiques sur Bitcoin

http://owni.fr/2011/06/15/bitcoin-revolution-monetaire-ponzi/ : article – en français – si vous voulez aller plus loin

1NDiQEFjAoyp6Vx7z1tLaJVdNw1hmvS5Mn : mon adresse Bitcoin, si vous voulez me faire un don :)

Bitcoin (BTC) : une nouvelle monnaie - 7/7

Excusez-moi pour les raccourcis et approximations faites dans un but de simplification dans cet article qui s'adresse en priorité aux personnes ne connaissant pas du tout Bitcoin

Posez vos questions dans les commentaires, j'essaierai d'y répondre dans la mesure de mes connaissances