Bitcoin : comment fonctionne la 1ère monnaie numérique décentralisée

Chronique de Pirmin Lemberger
Weave Business Technology

30/10/13 16:14

Bitcoin constitue la première expérience de monnaie virtuelle à l'échelle du Web. Quelles ont été les motivations pour créer un tel système ? A qui profite-t-il ? Quels impacts bitcoin peut-il avoir à moyen terme sur nos moyens de paiement ?

Bitcoin : un premier essai de monnaie numérique décentralisée

Tentons une définition : « Bitcoin désigne à la fois une monnaie électronique et un système de paiement sécurisé et anonyme entre particuliers. Son infrastructure est décentralisée[1] et comparable au système de partage de fichiers BitTorrent. »

Bitcoin n'est ni la première **monnaie virtuelle**, ni le premier **système de paiement anonyme** en ligne. Dans l'univers virtuel Second Life par exemple, le Linden Dollar permet à ses « habitants » d'acheter des biens et des services. Le service Paypal offre quant à lui la possibilité de régler ses achats en devises sans avoir à communiquer de coordonnées bancaires.

L'ambition de bitcoin cependant est d'une tout autre ampleur : (1) elle se veut monnaie universelle permettant de payer des biens dans le monde réel et (2) elle doit être échangeable contre des devises sans pour autant être adossée à aucune institution financière ou bancaire. Bitcoin cherche donc, en principe, à jouer dans la cours des grands, sur un pied d'égalité avec le dollar et l'euro.

Mais avant de poursuivre, posons la question fondamentale : **pourquoi diable inventer une nouvelle monnaie ?** Le dollar, l'euro et le yen ne suffisent-ils donc pas ? Très schématiquement, on peut considérer que deux courants de pensées soutiennent la création de nouvelles monnaies, virtuelles ou non, qui ne soient pas soumises à la tutelle d'aucune banque centrale. D'un côté nous avons les libertaires, dans la mouvance de l'école économique autrichienne, dont faisait partie F. Hayek grand chantre du libéralisme et digne héritier d'Adam Smith, le père du fameux concept de « main invisible ».

Pour eux, les interventions des organismes centraux sont la source de tous les maux de l'économie et notamment de la spirale inflationniste. La solution, pensent-ils, réside dans la libre compétition entre monnaies au sein d'un écosystème monétaire. De l'autre, nous avons les contempteurs du système financier actuel, écologistes et autres altermondialistes, qui fustigent les profits faramineux d'une petite oligarchie financière au détriment de l'intérêt général. Contourner les services financiers des banques et se réapproprier le droit de créer de la monnaie sont leurs principaux crédos.

Bitcoin en pratique

Pour envoyer ou recevoir des bitcoins, il vous faudra un porte-monnaie numérique (ou **wallet**). Vous aurez à choisir entre deux types de solution. Soit vous ne faites confiance à personne, ce qui bien dans l'esprit de bitcoin, auquel cas vous installez une petite application gratuite sur votre machine. Il vous incombera alors d'assurer la sécurité de votre porte-monnaie. Soit vous décidez d'accorder votre confiance à un prestataire en ligne qui prétend prendre en charge

la sécurisation de votre pécule numérique. Dans les deux cas de figure cependant : zéro formalité ! Le logiciel (ou le service en ligne) vous attribue alors une première adresse sous forme d'une **clé alphanumérique publique qui ne révèle pas votre identité** mais est l'équivalent d'un RIB temporaire.

Pour acquérir des bitcoins (BTC), deux solutions s'offrent à vous

Soit vous vous faites envoyer vos premiers bitcoins par une personne qui en possède déjà, ceci en lui transmettant votre clé publique. Soit, plus vraisemblablement, vous vous rendez sur la plateforme de change Mt.Gox pour échanger quelques-uns de vos bons vieux euros (attention pas tous !) contre votre premier bitcoin. Pour vous faciliter votre shopping, il existe par ailleurs des listes de marchands qui acceptent les bitcoins. En quelques clics, chaussettes en alpaga, iPad's et kalachnikovs seront alors à vous.

Une question peut-être vous taraude. Mais pourquoi les bitcoins auraient-ils de la valeur ? La réponse est la même que pour tout autre monnaie. Ce qui leurs confère de la valeur c'est la confiance que l'on peut avoir de pouvoir les échanger auprès d'une communauté en expansion. Par ailleurs, comme nous le verrons dans la section suivante, les bitcoins constituent aussi une forme de denrée rare comparable à l'or.

« For geeks only! » - comment fonctionne bitcoin ?

Comprendre les détails du protocole bitcoin requiert des connaissances avancées en cryptographie et en traitements distribués. Par conséquent nous devrons nous contenter ici d'une simple esquisse et nous supposerons par ailleurs connus du lecteur les rudiments de la cryptographie à clé publique (PKI).

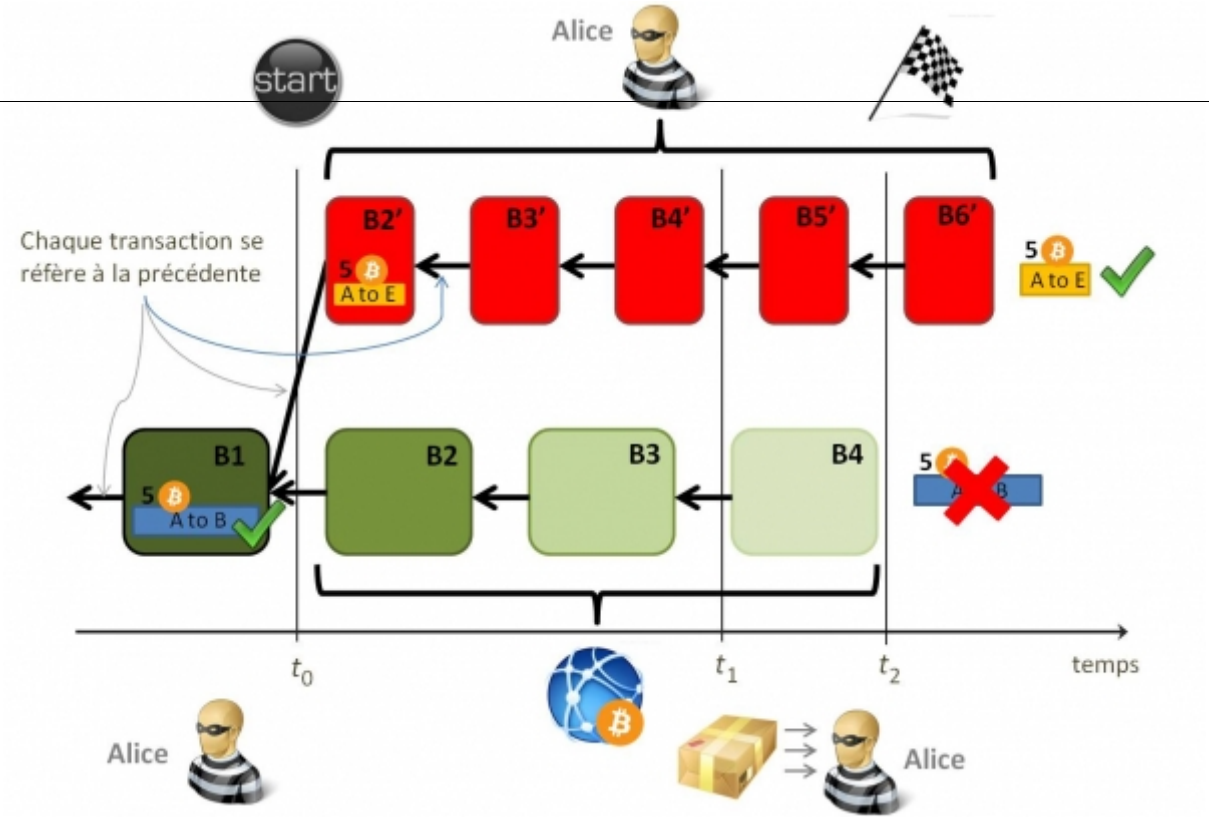
Respectons les traditions et imaginons qu'Alice souhaite envoyer 5 BTC à Bob.

Un petit fichier, appelé transaction, est alors créé par l'application porte-monnaie d'Alice et est publié sur le réseau. Ce fichier, signé par Alice, contient : (1) les clés publiques qui identifient Alice et de Bob, (2) le montant de 5 BTC qu'Alice souhaite transférer et (3) les références aux transactions précédentes qui ont conféré à Alice la possession de ces 5 BTC (dont on comprendra la raison d'être dans un instant). Grâce à la PKI, personne ne pourra se faire passer pour Alice et n'importe quel nœud (=machine) du réseau bitcoin sera à même de vérifier l'authenticité de cette transaction. Comme chaque transaction se réfère aux précédentes (voir (3)), c'est en fait l'intégralité de la chaine de possession des bitcoins qui est vérifiable.

En réalité, Bitcoin ne possède pas livre de compte !

Le solde d'Alice par exemple n'est écrit nulle part mais est calculable à partir de la chaine de toutes les transactions depuis la création du système, dont chaque nœud possède une copie régulièrement mise à jour !

Reste le point le plus épineux : comment éviter qu'Alice ne puisse envoyer frauduleusement ces mêmes 5 BTC à quelqu'un d'autre *après* les avoir déjà envoyés à Bob ? Dans un système bancaire traditionnel une telle vérification est aisée car le système central définit une chronologie qui permet d'établir l'antériorité d'une transaction sur une autre. Dans un réseau P2P comme bitcoin en revanche, la latence du réseau empêche une telle vérification. Rien ne garanti en effet que l'ordre dans lequel les transactions sont émises soit celui dans lequel elles seront reçues par le nœud qui doit les vérifier.



Un exemple de « double spending ». En t_0 La transaction (A to B) contenant l'envoi par Alice de 5 BTC à Bob est validée une première fois par le réseau par inclusion dans le bloc B_1. Une course s'engage alors entre Alice et le réseau honnête. Alice inclut une transaction frauduleuse (A to E) de 5 BTC dans le bloc B'_2 mais, avant de publier sa chaîne de blocs frauduleuse, elle doit attendre que Bob considère que la transaction (A to B) ait été validée un nombre suffisant de fois par le réseau pour qu'il accepte de livrer son produit à Alice. Ce que Bob fait en t_1 En t_2 Alice publie sa chaîne frauduleuse qui est validée par le réseau car elle est plus longue que la chaîne honnête. La transaction (A to B) est alors invalidée et la transaction (A to E) est validée.

La résolution de ce **problème fondamental, connu sous le nom de double-spending** (DS), constitue la percée algorithmique majeure de bitcoin. Les détails sont subtils, même au plan conceptuel, mais **l'idée de base consiste à définir un mécanisme qui exige que**, pour réussir une attaque de type DS, **un fraudeur devrait disposer d'une puissance de calcul équivalente à celle d'une fraction significative du réseau**, disons au moins 10% du CPU total. A cet effet, le système construit une chaîne de blocs de (plusieurs centaines) transactions validées destinée à définir un ordre chronologique au niveau des blocs (à ne pas confondre avec la chaîne des transactions qui établi, elle, l'enchaînement de possession des BTC). Un peu à l'image des CAPTCHA utilisés pour se prémunir des spammer, le protocole bitcoin exige que tout nœud qui prétend inclure un nouveau bloc dans la chaine existante, fournisse au préalable la **solution d'un certain challenge mathématique extrêmement difficile** lié au contenu du bloc à inclure (ce dernier point est essentiel). Toutes les machines du réseau sont mises en compétition pour trouver la solution à ce challenge. Le protocole est ainsi conçu pour qu'une solution soit trouvée, en moyenne, toutes les dix minutes par une seule de ces machines. Lorsqu'une machine trouve la solution à un challenge elle la diffuse sur le réseau (qui peut alors facilement la vérifier).

Dans de rares situations, il se peut que deux blocs différents soient rattachés par des machines différentes à la chaîne existante, créant ainsi un arbre à plusieurs branches au lieu de la chaîne linéaire souhaitée. La règle exigée par le protocole consiste à choisir systématiquement la branche la plus longue. Un examen minutieux de la situation montre alors deux choses.

D'une part, comme il est extrêmement improbable qu'une telle coïncidence survienne plusieurs fois de suite, un consensus émerge rapidement quant à la branche la plus longue, établissant ainsi la chronologie souhaitée.

D'autre part, il est quasiment impossible pour une machine isolée d'insérer assez rapidement une succession de

blocs frauduleux pour créer une branche plus longue que la branche honnête déjà validée par le réseau supposé majoritairement honnête, (voir la figure).

Remporter la course impliquerait en effet d'être capable de résoudre par avance tous les challenges mathématiques associés à une succession de bloc frauduleux. **Ceci n'est pas possible pour une raison subtile :** selon le protocole, chaque nouveau bloc B_n doit incorporer dans son contenu la solution du challenge associé à l'inclusion du bloc précédent B_(n-1). Il est donc extrêmement difficile de tricher en pré-calculant une chaine de faux blocs puisqu'il faut les calculer dans l'ordre et que chaque calcul exige, typiquement, 10 minutes du CPU global. CQFD.

On le voit, **une transaction bitcoin est d'autant plus sûre quelle est validée un grand nombre de fois** et que la puissance de calcul du réseau honnête l'emporte largement sur celle d'un fraudeur. Six validations successives sont suffisantes pour que la probabilité d'un DS réussi tombe à 0.1% avec 10% de CPU malhonnête.

Vous n'avez pas tout compris ? C'est normal ! Pour aller plus loin je suggère de regarder ou lire, dans cet ordre, les trois sources suivantes : (1), (2) et (3).

Toute machine du réseau bitcoin peut participer au processus de validation des blocs, il suffit pour cela d'y installer un logiciel approprié. Une telle machine est alors appelée un « miner ». Comme ce travail de validation est couteux en CPU et en énergie électrique, le protocole bitcoin inclut un mécanisme d'incitation sous forme de rétribution en BTC pour ceux qui y participent. C'est donc ainsi que sont créés, littéralement ex-nihilo, de nouveaux bitcoins dans l'économie : par extraction de solutions à des challenges mathématiques ! D'où le terme de « miner ».

Dans le futur, un autre mécanisme d'incitation prendra progressivement la relève. Il s'agit d'un mécanisme plus traditionnel de commissions (très faibles) que chaque émetteur de transactions peut volontairement inclure pour que les siennes soient traitées en priorité par les miners.

D'un point de vue purement technique bitcoin fait figure de prouesse. Les **idées mises en œuvre sont profondément originales[2]** et vont à l'encontre des intuitions usuelles (le système fonctionne sans livre de comptes et chaque nœud possède une copie intégrale de toutes les transactions !). Voilà une innovation fera date.

Bitcoin a-t-il un avenir ?

L'idée de **décloisonner le marché du paiement** pour faire pièce au monopole des VISA, Paypal et autres MasterCard est assurément dans l'air du temps. Mentionnons à titre d'exemple le projet Compte Nickel qui devrait bientôt permettre à quiconque d'ouvrir un compte chez un buraliste sans conditions de ressources et avec un minimum de formalités. Ou encore la startup française Paymium qui propose d'ores et déjà un service de paiement adossé aux bitcoins.

Contourner le système bancaire est donc à la mode. Mais qui empêchera les banques établies de proposer leurs services et de prendre en charge votre précieux bitcoin-wallet ? Personne probablement. On peut donc s'attendre à voir fleurir prochainement toute une panoplie de services de paiement innovants intégrés aux sites marchands qui auront tout intérêt à offrir un maximum de souplesse quant aux moyens de paiement qu'ils proposent. Par la même occasion, ils profiteront de la manne non négligeable que représente la population qui ne possède pas de compte bancaire (8 % aux USA). Voilà pour l'avenir à moyen terme.

S'agissant de bitcoin, le long terme est moins clair et les critiques ne manquent pas. Une partie d'entre elles émanent de fossoyeurs de l'innovation qui voient-là une menace à leur lucratif monopole mais d'autres apparaissent plus fondées.

Pour y voir clair, faisons un rapide inventaire des avantages et des inconvénients :

« Pour bitcoin » – point de vue l'utilisateur

Aucune condition de ressource n'est requise pour utiliser le système bitcoin.

Aucun organisme ni aucun état ne pourra jamais geler un compte bitcoin.

Les **frais de transactions sont dérisoires** comparés aux frais bancaires usuels.

Comme le liquide, bitcoin permet **des transferts d'argent anonymes**.

Les bitcoins sont utilisables partout, un simple accès à internet suffit.

« Contre bitcoin » – point de vue de l'utilisateur

En cas de fraude vous ne pourrez vous retourner contre personne car **il n'y pas de responsable du système**.

De même si vous perdez vos clés, personne ne pourra vous porter secours. Vos bitcoins seront définitivement perdus, non seulement pour vous même, mais aussi pour l'économie dans son ensemble.

Le marché des BTC est pour l'instant **extrêmement volatile**. Les avoirs en BTC doivent donc être assimilés à un actif à haut risque.

Le **marché des BTC reste à ce jour très illiquide**. Même s'ils ont pris de la valeur face à l'euro, il n'est pas sûr que vous trouviez des acheteurs à court terme.

« Contre bitcoin » – point de vue de la société

Bitcoin facilite la **fraude** fiscale, le blanchiment et les trafics illégaux en tous genres.

Certains économistes prédisent que bitcoin génèrera une **spirale déflationniste**. En effet, le rythme de croissance de la quantité de bitcoins étant spécifié par le protocole[3], une augmentation massive des transactions entrainera mécaniquement une augmentation de la valeur du BTC face aux autres monnaies. Ainsi le BTC deviendrait avant tout une monnaie livrée à la spéculation plutôt qu'une monnaie d'échange au bénéfice de l'économie réelle et de l'emploi.

Bitcoin est un hybride un peu bizarre, entre un système de paiement et une monnaie virtuelle, dont le **statut légal reste encore très flou** dans beaucoup de pays.

Résumons-nous

Bitcoin est né à la confluence de deux rêves. Le premier correspond à une vision technophile un peu naïve qui voudrait croire que les problèmes économiques et sociaux trouveront une solution dans la technologie. À l'instauration d'une relation de confiance envers une institution chargée de définir une politique monétaire, on croit pouvoir substituer la sophistication d'algorithmes cryptographiques.

Le second est une conception libertaire, voire nihiliste, de la société. A ce titre **bitcoin incarne un idéal d'individualisme** d'où sont bannies toute idée de solidarité ou de responsabilité sociale et environnementale. Sachant que toute monnaie favorise certains comportements et véhicule certaines valeurs, comme l'explique fort lucidement le dernier rapport du Club de Rome, il est dès lors légitime de poser la question : « notre monde a-t-il vraiment besoin de plus d'individualisme et de moins de contrôle ? ».

Quel que soit son avenir, bitcoin restera **une expérience fascinante et riche d'enseignements** pour construire, un jour peut-être, d'autres monnaies virtuelles avec d'autres objectifs et basées sur d'autres valeurs. Dans la classe des monnaies virtuelles, sur le livret de l'élève bitcoin, on notera : « peut mieux faire ! ».

---

[1] On parle aussi de réseau P2P pour peer-to-peer.

[2] La création du système bitcoin en 2009 reste d'ailleurs nimbée de mystère, le ou les créateurs se cachent derrière le pseudonyme Satoshi Nakamoto.

[3] Le protocole prévoit explicitement que pas plus de 21 millions de BTC auront été générés d'ici l'an 2140.