Le bitcoin, une monnaie 100 % numérique

PAR
Rémy Chrétien
Stéphanie Delaune

NIVEAU DE LECTURE
Intermédiaire

PUBLIÉ LE
08/09/2014

Découvrir

À l'heure où l'on se souvient des soucis du franc, où l'on a parfois trop vite tendance à accuser l'euro de tous les maux, nous arrive une monnaie 100 % numérique, le bitcoin. De nombreux articles ont insisté sur des aspects financiers ou sociétaux du bitcoin, qui sont passionnants. Nous avons choisi de vous présenter ici quelque chose de tout aussi passionnant : les algorithmes qui rendent possible cette crypto-monnaie.

Bitcoin est une monnaie virtuelle dont le concept fut publié en 2008 sous le pseudonyme de Satoshi Nakamoto. Le réseau Bitcoin lui-même vit le jour en janvier 2009. La crypto-monnaie a depuis fait largement parler d'elle. Son cours s'est envolé : la première transaction permit indirectement d'acheter deux pizzas pour 10 000 bitcoins, alors que le cours au 26 juin 2014 était d'environ 415 € pour un seul bitcoin. Des entreprises comme Wordpress l'acceptent pour le paiement de leurs services, tandis que certains pays, comme la Thaïlande et la Russie, ont interdit son utilisation sur leur territoire. Mais tout cela évolue constamment. La Russie a ainsi récemment revu sa position.

Dessin : Ray Clid .

Bitcoin est critiquée notamment pour sa grande volatilité ou son risque d'utilisation dans des circuits de blanchiment d'argent. Elle attire les spéculateurs, peut faire gagner ou perdre des sommes importantes. Bitcoin, tout comme ses consœurs plus récentes Litecoin, Darkcoin ou encore Dogecoin, apparaît comme un formidable outil à manier prudemment.

Comment ça marche ?

Bitcoin est une monnaie virtuelle, sans émission d'un support physique comme des pièces ou des billets. Elle est établie sur un réseau pair-à-pair , où toutes les machines participant au réseau, les nœuds du réseau, sont sur un pied d'égalité. À l'inverse des monnaies classiques, elle ne repose pas sur l'existence d'une autorité comme la Banque centrale européenne pour son émission ou sa régulation. Cette nouvelle monnaie a été conçue avec un mécanisme d'autorégulation. Le bon fonctionnement des échanges est garanti par un protocole public et transparent exécuté par un grand nombre d'utilisateurs. Découvrons comment ces bitcoins sont échangés, créés, et parfois même perdus.

Auteurs

Rémy Chrétien
Doctorant dans le projet ANR VIP au LSV de l'ENS Cachan.

Stéphanie Delaune
Chargée de recherche CNRS au LSV de l'ENS Cachan.

→ Voir tous les auteurs

Concrètement, comment se passe une transaction ?

Contrairement à l'idée naïve qu'on pourrait se faire d'une monnaie virtuelle, un utilisateur de bitcoins ne dispose pas d'un porte-monnaie sous forme d'un fichier ou dossier qui contiendrait les bitcoins qu'il possède. À la place, il accède à un registre, un grand livre de comptes public consignant toutes les transactions en bitcoins ayant eu lieu depuis la mise en place du protocole. C'est à partir de ce registre qu'il peut calculer sa fortune personnelle (le solde de son porte-monnaie).

Prenons un exemple concret. Supposons qu'Alice souhaite acheter un livre à Bob en réalisant une transaction en bitcoins. Tout d'abord, il est important de veiller à la sécurité des messages échangés, et on utilise pour cela le mécanisme de signature électronique reposant sur le concept de clé privée et de clé publique . Chaque utilisateur dispose d'un tel couple de clés, qui constitue son compte.

1. Bob communique sa clé publique pub(Bob) à Alice ;
2. Alice construit le message M indiquant qu'elle souhaite transférer N bitcoins à Bob :
   M = « transfert à pub(Bob) d'un montant de N bitcoins » ;
3. Alice donne son accord pour effectuer ce transfert en signant ce message avec sa clé privée priv(Alice), et en diffusant dans tout le réseau la transaction :
   T = signature(M, priv(Alice)) ;
4. À la réception de cette transaction T, tous les nœuds du réseau, la machine de Bob comme celles de tous les autres utilisateurs, peuvent vérifier la signature à l'aide de la clé publique d'Alice, pour s'assurer que le message vient bien d'elle. En consultant leur registre, ils vérifient aussi qu'Alice dispose bien des bitcoins qu'elle se propose de transférer à Bob.

Il est à noter que le protocole n'exige pas de révéler son identité lors d'une transaction. Derrière chaque paire de clés, il y a un propriétaire anonyme. Une personne peut ainsi posséder plusieurs comptes en bitcoins.

Lorsqu'on parle de porte-monnaie ou de compte, c'est par analogie avec les monnaies classiques et les comptes en banque, mais avec les crypto-monnaies, il faut raisonner différemment. En réalité, un compte est une paire de clés, c'est-à-dire deux séries de caractères, l'une publique, l'autre privée, qui lui permettent d'effectuer les opérations et d'accéder au registre. Un porte-monnaie est l'ensemble des bitcoins disponibles d'un compte, et se calcule à partir du registre.

Qui gère les comptes ?

Comme mentionné précédemment, toutes les transactions sont consignées dans un grand livre de comptes public appelé « registre » ou encore « blockchain ». À l'heure actuelle, le réseau traite environ 60 000 transactions par jour. Il est important de noter que le registre de transactions croît à mesure que Bitcoin est utilisé. Sa taille, actuellement de l'ordre d'une vingtaine de mégaoctets, risque d'exploser si Bitcoin connaît un succès beaucoup plus large.

Ce registre permet à chacun de calculer le nombre de bitcoins existant sur chaque compte, c'est-à-dire associé à chaque clé publique. Chacun peut donc a priori valider une transaction, c'est-à-dire vérifier que les bitcoins à dépenser sont disponibles sur le compte de l'acheteur, puis autoriser le transfert de ces bitcoins du compte de l'acheteur vers celui du vendeur. En fait, chacun des nœuds du réseau pair-à-pair a sa propre copie du registre où il consigne les différentes transactions dont il a connaissance, et l'absence d'autorité centrale pose le problème de la cohérence entre tous ces registres. En particulier, il faut éviter une double dépense.

Est-il possible de dépenser un même bitcoin plusieurs fois ?

Considérons un scénario où Alice essaie de dépenser un même bitcoin pour payer un achat effectué auprès de Bob (transaction T_{Bob}), et régler sa dette envers Charlie

(transaction $T_{Charlie}$). En supposant une communication un peu lente entre certains nœuds du réseau, il se pourrait que parallèlement ces deux transactions se trouvent validées. Le réseau est alors divisé en deux, avec deux copies du registre, l'une contenant la transaction T_{Bob}, et l'autre la transaction $T_{Charlie}$. Les deux registres résultants ne sont plus cohérents, mais personne n'est encore au courant de cette situation. Lorsqu'un participant apprendra l'existence des transactions T_{Bob} et $T_{Charlie}$, l'incohérence sera révélée, et il faudra alors décider du registre qui fait foi, et donc de la transaction à garder.

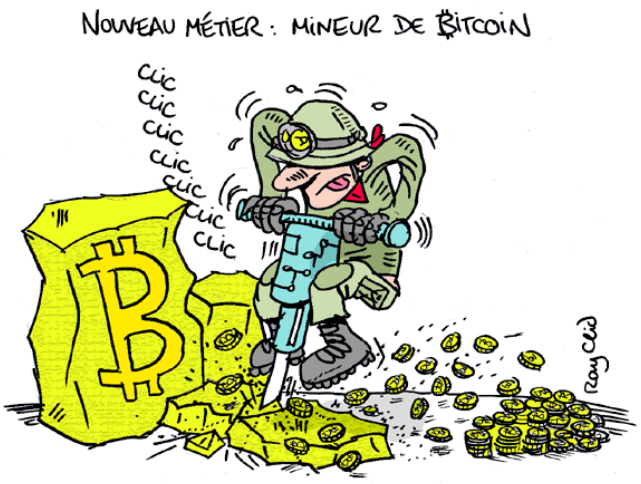
L'idée de base est de travailler sur le registre le plus long dont on ait connaissance. Il se pourrait qu'il y ait localement des divergences, mais, dans un réseau où la communication est suffisamment rapide et où une majorité de nœuds jouent le jeu, il devrait se dégager un registre significativement plus long assez rapidement. Une fois une transaction réalisée, il faudra donc laisser passer ce temps nécessaire à la synchronisation des registres pour garantir que la transaction se retrouve bien dans le registre qui fait foi, et pouvoir la valider définitivement.

Le problème est que la longueur d'un registre serait alors facilement manipulable par quelqu'un de mal intentionné. En ajoutant et validant des transactions fictives, Alice pourrait faire en sorte que les copies du registre contenant respectivement T_{Bob} et $T_{Charlie}$ deviennent à tour de rôle le registre de référence. Elle pourrait ainsi faire croire à Bob qu'il doit lui faire parvenir son livre, alors qu'elle a réglé sa dette envers Charlie. Bob se rendrait compte que le bitcoin est finalement dans les mains de Charlie… mais ce serait trop tard.

Comment empêcher une manipulation du registre des transactions ?

Pour éviter une telle double dépense, l'idée centrale est de rendre coûteuse la validation d'une transaction (ou, en réalité, d'un bloc contenant les transactions effectuées en une dizaine de minutes). Ainsi, Alice ne pourra pas aisément ajouter des transactions au registre et ainsi valider l'opération avec Charlie. Pour expliquer ce mécanisme central de Bitcoin, on a besoin d'introduire une nouvelle notion : celle de fonction de hachage. Le hachage est une opération qui consiste à transformer un texte de longueur arbitraire en un texte de longueur fixe. Dans le cas de Bitcoin, une suite de 256 bits. Mais cette suite (appelée *hash* du texte) doit vérifier une propriété fondamentale : il est virtuellement impossible de créer un second texte avec le même *hash*.

Grâce à ce mécanisme, mettre à jour le registre des transactions sera plus compliqué. Plutôt que de simplement valider la transaction T_{Bob} avant de l'ajouter au registre, il faudra aussi trouver un nombre x tel que le message « T_{Bob} + x » ait un *hash* se terminant par dix zéros (par exemple). Trouver une bonne valeur pour x demande du temps de calcul, mais il est en revanche très facile, étant donné x, de vérifier que la valeur convient bien. Ainsi, pour chaque transaction, ou pour être précis chaque bloc de transactions, des utilisateurs de Bitcoin, appelés « mineurs », vont vérifier que celui-ci est valide et trouver une valeur de x. Le premier mineur ayant réussi à trouver x l'enverra aux autres utilisateurs, qui pourront ajouter ces transactions à leur copie du registre. On appelle cette opération réaliser une preuve de travail ou encore « minage » dans le vocabulaire des crypto-monnaies.



Dessin : Ray Clid .

Qu'est-ce que ça change ?

Avec ce mécanisme, si Alice veut ajouter un nouveau bloc de transactions au registre pour tenter de faire valider $T_{Charlie}$ plutôt que T_{Bob}, elle va devoir effectuer de lourds calculs en un temps très réduit (avant que d'autres mineurs ne minent les blocs correspondants), ce qui lui sera concrètement impossible, à moins qu'Alice ne contrôle l'essentiel de la puissance de calcul de l'ensemble du réseau.

L'utilisation d'une fonction de hachage permet par ailleurs de chaîner les différents blocs de transactions : en ajoutant à tout nouveau bloc le *hash* du bloc précédent, il est impossible pour quiconque d'introduire de nouvelles transactions au milieu du registre commun.

Des transactions risquent-elles d'être effacées ?

Lors de la synchronisation des registres, aucune transaction ne sera perdue. En effet, deux chaînes parallèles correspondent à deux vues différentes du même registre (et sur chacune, la validation permet d'assurer qu'un bitcoin n'est dépensé qu'une seule fois). Si Alice a réalisé une transaction et que tout le réseau en a été informé, il y a toutes les chances que cette transaction existe dans les deux chaînes (dans celle supprimée mais aussi dans celle qui fait foi). De plus, si Alice est honnête et qu'il s'agit bien d'une seule et même transaction, alors il y a un unique destinataire (le même dans les deux chaînes), supprimer l'une des deux n'a donc aucun effet pour cette transaction.

Un tel cas de divergence s'est produit il y a un peu plus d'un an, à cause d'un problème entre deux versions du logiciel Bitcoin. Ceci a conduit une moitié des utilisateurs à refuser un bloc miné alors que l'autre moitié l'a accepté. Ainsi, deux registres différents ont coexisté pendant plusieurs heures. Mais il semble qu'ils ne contenaient que des transactions honnêtes (aucun bitcoin n'avait été dépensé différemment sur ces deux chaînes), il a donc été possible de retourner à une situation cohérente une fois le problème logiciel résolu. Il a fallu choisir une chaîne, mais cela n'a eu aucun impact sur les bénéficiaires des bitcoins.

Création des bitcoins : par qui, quand, et comment ?

Nous avons vu comment s'échanger des bitcoins, mais, en l'absence d'autorité centrale, il demeure une question essentielle pour l'autorégulation du système. Comment les bitcoins sont-ils créés ?

Que gagnent les mineurs à faire tourner leurs machines et consommer de l'énergie ? Des bitcoins fraîchement créés ! Le premier bloc (appelé bloc « genèse ») a été miné en

janvier 2009. Depuis lors, toutes les dix minutes environ, un bloc de transactions est miné. Le mineur concerné, et lui seul, reçoit une récompense de 25 bitcoins, ce qui correspond, au cours du 26 juin 2014, à environ 10 375 euros. C'est en fait la seule et unique façon de créer de nouveaux bitcoins. Il faut savoir que cette récompense diminue, en pratique, elle est divisée par deux tous les quatre ans. L'unité bitcoin n'étant pas divisible à l'infini, cette récompense atteindra aux alentours de l'an 2140, la plus petite sous-unité, appelée « satoshi », et plus aucun bitcoin ne pourra être créé. Ils seront alors au nombre de 21 millions.

Les plus pessimistes verront cette limite comme annonçant la fin des bitcoins... mais, pour continuer à assurer le bon fonctionnement du protocole au-delà de cette date, un mécanisme de commission (similaire à des frais bancaires) a été prévu. Pour l'instant, le montant de cette commission, laissé à l'appréciation des utilisateurs, reste en général très faible. Les mineurs pourront donc toujours prétendre à une rémunération, mais l'utilisateur devra payer !

Acheter et stocker des bitcoins ?

Les plateformes d'échange de bitcoins permettent d'acheter facilement et rapidement des bitcoins. Le principe est simple : vous vous inscrivez sur le site pour y transférer des euros ou des dollars puis vous pouvez acheter des bitcoins en proposant une offre d'achat. Il vous faut alors retirer du site les bitcoins achetés en les transférant sur un compte Bitcoin que vous créez. Plusieurs solutions s'offrent à vous. La plupart des plateformes d'échange vous permettent également de gérer votre compte. Mais ces dernières ne sont pas à l'abri d'incidents, si l'on se réfère à la fermeture brutale en février 2014 de la plateforme d'échange Mt. Gox, qui a occasionné la perte de 744 408 bitcoins (soit l'équivalent de plus de 250 millions d'euros).

Un « portefeuille papier » généré par ordinateur. Image : bitcoin.fr .

Les plus méfiants préféreront un stockage local sur leur ordinateur personnel ou même un « portefeuille papier », une simple feuille de papier sur laquelle figure la paire de clés de l'utilisateur. Il ne vous reste plus qu'à veiller à la sécurité de votre ordinateur, sans oublier de faire les sauvegardes nécessaires, ou à mettre ce papier en lieu sûr, à l'abri du feu et de l'humidité !

Enfin, sachez que...

Si vous avez choisi de vous lancer dans l'aventure, veillez à conserver votre clé privée précieusement. La perte de cette dernière rend inutilisables ses propres bitcoins, et ce sans aucun recours possible.

Si vous souhaitez devenir riche en vous lançant dans le minage de blocs, sachez qu'en pratique la compétition est telle que les ordinateurs de bureau actuels n'ont plus aucune chance de gagner de l'argent via le minage.

Si vous souhaitez utiliser cette monnaie pour effectuer des opérations en toute discrétion, il faut savoir que, même si le détenteur d'un compte peut rester anonyme, les bitcoins sont, eux, parfaitement traçables. On peut à tout moment calculer la fortune détenue par un compte quelconque ou obtenir la liste de toutes les transactions associées. Alice est

donc peut-être anonyme, mais ses bitcoins sont marqués, permettant de les suivre à la trace sur le réseau.

De notre point de vue, Bitcoin est avant tout un protocole cryptographique, utilisant nombre d'éléments traditionnels en sécurité informatique. La conception de tels objets est notoirement difficile et a, par le passé, laissé paraître des failles longtemps après leur diffusion. La résistance du protocole Bitcoin est encourageante et prometteuse. Cependant, on ne peut, à l'heure actuelle, que spéculer sur l'absence de failles dans ce protocole.

« *Bitcoin est une expérience inédite, n'y investissez que le temps et l'argent que vous pouvez vous permettre de perdre.* » (Bitcoin.fr)

Pour aller plus loin .

Une première version de ce document est parue sur le blog Binaire .

TAGS

Cryptographie **Finance** **Réseau**