Le *bitcoin* : nature et fonctionnement

SYLVAIN MIGNOT
Chercheur associé
CESDIP*

Le *bitcoin* est une monnaie électronique, décentralisée, partiellement anonyme, soutenue par aucun gouvernement ni entité légale. L'intégrité du système repose sur l'existence d'un registre contenant la totalité des transactions, tenu à jour sur l'ensemble des nœuds du réseau. Celle-ci possède divers avantages, comme des frais de transactions extrêmement faibles, mais sa valeur n'étant assurée par aucun État, elle est basée uniquement sur la confiance des utilisateurs à son égard, cela pouvant engendrer un questionnement quant à sa valeur réelle.

Le *bitcoin* est, à l'heure actuelle, la plus connue et la plus utilisée des nombreuses crypto-monnaies en circulation. C'est également la première ayant eu droit à une implémentation complète. Une crypto-monnaie est une monnaie électronique pair à pair et décentralisée. Les échanges se font entre utilisateurs sans recours à une banque qui gérerait les transactions. Cela explique un des gros avantages de ce système, à savoir proposer des frais de transactions extrêmement faibles, bien en dessous de ce que proposent les banques. Afin d'assurer la validation des transactions, et la génération de ce type de monnaie, sont utilisées des méthodes cryptographiques. En particulier, le concept de « preuve de travail », sorte de puzzle informatique devant être résolu par un ordinateur pour valider une tâche. Le *bitcoin* repose sur ces protocoles cryptographiques pour, d'une part, résoudre le problème du double paiement et, d'autre part, garantir l'identité des participants.

Ces monnaies sont considérées comme « alternatives », et bien sûr, aucune nation n'en a adopté comme monnaie fiduciaire.

Il faut faire bien attention de distinguer le *bitcoin*, qui est une unité de cette devise monétaire, du *bitcoin* qui est le système de transactions de cette devise. Il existe à l'heure actuelle plus de dix millions de *bitcoins* en circulation, d'une valeur estimée à plus de 5 milliards d'euros. Mais du fait de la forte volatilité des cours, cette valeur est susceptible de changer très rapidement.

Les crypto-monnaies en général, et donc le *bitcoin*, sont, sur un certain nombre de points, différentes de manière notable des systèmes monétaires « classiques ».

Tout d'abord n'étant pas garantie ou imposée par un organisme centralisateur quel qu'il soit (un État, une banque centrale, etc.), la valeur d'un *bitcoin* sera uniquement déterminée par le marché des changes, sur son usage. Elle ne repose pas sur des biens matériels mais sur la valeur que les individus lui accordent en tant que système de paiement. Ensuite l'émission monétaire n'est pas la prérogative d'une banque ou d'un état, mais est prédéterminée dans le code informatique. Celui-ci est consultable par tous (*open-source*) et l'évolution du nombre de *bitcoins* dans le temps est facilement prévisible. Enfin, de par son implémentation, le *bitcoin* ne nécessite pas d'infrastructure centralisée pour assurer et vérifier les transactions. Ces vérifications sont effectuées par des utilisateurs du réseau *bitcoin*, sélectionnés de manière aléatoire à intervalles réguliers.

Dans cet article, nous commençons par donner un bref rappel historique concernant la création et l'émergence du *bitcoin* (1.), puis nous décrivons le fonctionnement technique de cette crypto-monnaie (2.). Enfin nous présentons différents risques ou faiblesses inhérents au système dans la partie 3, avant de conclure.

1. HISTOIRE

Avant l'apparition du *bitcoin*, de nombreuses monnaies précurseurs ont existé. Par exemple, les technologies développées par David Chaum et Stefan Brands (ecash), Adam Back (hashcash), Wei Dai (b-money), Nick Szabo (bit-gold)... De nombreux mécanismes et concepts uti-

* Centre de recherche sociologique sur le droit des institutions pénales.

lisés ou proposés par ces monnaies ont été repris pour créer le *bitcoin*.

La création du *bitcoin* proprement dite est entourée de mystères. En 2008, un certain Satoshi Nakamoto publia un article de recherche dans une *mailing list* concernant la cryptographie, dont le titre était : *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008). Il est intéressant de noter est que ce Satoshi Nakamoto n'était connu d'aucun des utilisateurs de cette liste de diffusion. De fait, il a rapidement été établi qu'il n'existe pas en tant que personne, ce nom n'étant rien d'autre qu'un pseudonyme.

Dans cet article, l'(les ?) énigmatique(s) auteur(s) présente(nt) le principe de fonctionnement d'une nouvelle crypto-monnaie qu'il(s) appelle(nt) *bitcoin*. À l'heure actuelle, l'identité de son créateur reste inconnue, nul ne sachant même s'il s'agit d'une personne unique ou d'un groupe de personnes. L'entité répondant au nom de Satoshi Nakamoto a cessé de communiquer en 2010. Depuis, elle n'a plus donné signe de vie.

Quoi qu'il en soit, le *bitcoin* fut la première implémentation complète d'une crypto-monnaie et reste à ce jour la plus importante en termes de valeur.

2. PRINCIPES TECHNIQUES

Nous allons ici présenter de manière simple les principes de fonctionnement du *bitcoin*.

Tout d'abord, il est important de noter que le système *bitcoin* ne chiffre aucune des données qu'il utilise, et il est tout à fait possible à tout un chacun de consulter le registre des transactions ayant eu lieu. La cryptographie est uniquement utilisée pour créer des signatures non falsifiables et implémenter des fonctions à sens unique.

Seul le portefeuille de clés privées (là ou l'utilisateur conservera les informations secrètes qui prouveront son droit à dépenser ses *bitcoins*) est susceptible d'être chiffré par l'utilisateur. Mais ceci est facultatif, et du ressort de l'utilisateur et pas du système *bitcoin*. Ce chiffrement peut être à la charge du système d'exploitation ou d'un logiciel adapté, comme pour n'importe quel autre fichier.

Une adresse *bitcoin* est la seule information que vous ayez besoin de posséder pour recevoir des *bitcoins*, et il n'est pas nécessaire d'exécuter le logiciel *bitcoin* pour les recevoir. C'est en effet le payeur qui enverra la transaction au reste du réseau, dans laquelle sera incluse l'adresse du bénéficiaire.

Une idée faussement répandue est que le *bitcoin* est anonyme. Il est possible, bien que complexe, de retrouver l'identité des utilisateurs du réseau. Une étude à ce sujet peut être trouvée dans Reid & Harrigan (2012).

Chaque *bitcoin* est divisible jusqu'à la 8e décimale. Afin de représenter des fractions inférieures au *bitcoin*, il est possible d'utiliser les préfixes du système international d'unités. Les utilisateurs utilisent souvent l'appellation de « Satoshi » pour désigner la plus petite subdivision du *bitcoin* (le cent millionième) en hommage au créateur du système.

L'idée générale du déroulement d'une transaction est la suivante : les utilisateurs de *bitcoin* forment un réseau pair à pair, et communiquent entre eux en utilisant Internet. Pour tout ordinateur cherchant à se connecter au réseau *bitcoin*, la première chose à faire est de trouver les listes des ordinateurs préalablement connectés. Afin d'y parvenir, une liste d'adresse IP statiques (des numéros d'identification correspondant à certains ordinateurs présents de manière permanente sur le réseau *bitcoin*) a été intégrée dans le code source du logiciel. Autrement dit, l'adresse de la porte d'entrée au système est connue de tous les utilisateurs.

La deuxième étape consiste à télécharger la blockchain, la base de données (de taille non négligeable) contenant la liste de toutes les transactions ayant eu lieu depuis le premier jour de fonctionnement du système *bitcoin*. Une fois ce téléchargement effectué, le logiciel est prêt à être utilisé et l'utilisateur peut, s'il le souhaite, s'en servir pour effectuer des transactions. Son ordinateur communiquera en permanence avec les autres membres du réseau, procédant à divers échanges d'informations concernant les nouvelles transactions ayant lieu ainsi que les différentes adresses IP des utilisateurs. Une transaction a toujours lieu entre deux utilisateurs du réseau, et se définit comme le transfert d'un certain montant, exprimé en *bitcoins*, du compte d'un utilisateur (identifié par une adresse unique) à un autre. Chaque transaction doit être signée numériquement afin d'être validée, et prend en entrée la (ou les) référence(s) de la transaction précédente montrant que l'utilisateur dispose bien des fonds à transférer. Elle produit en sortie une liste d'une ou plusieurs adresses de destinataires, associées aux montants transférés à chacune. La somme des entrées doit être égale à la somme des sorties dans tous les cas.

2.1. Validation d'une transaction

Un des problèmes sur lequel ont longtemps buté les crypto-monnaies est celui de la validation des transactions en se passant de l'existence d'une entité centralisatrice. Pour résoudre ce problème, le *bitcoin* utilise une *blockchain*, sorte d'historique de la totalité des transactions ayant eu lieu, une « mémoire parfaite » de l'histoire de *bitcoin*. Comme son nom l'indique elle est composée d'une chaîne de « blocs » de transactions.

Concrètement le fonctionnement est le suivant.

Lorsqu'une transaction a lieu, le payeur diffuse cette information à l'ensemble du réseau. Puis, lorsqu'un utilisateur du système disposant d'un logiciel spécifique (appelé un « mineur » dans le jargon *bitcoin*) reçoit cette nouvelle transaction, il opère une validation de celle-ci, vérifiant qu'elle est bien cohérente avec l'histoire de *bitcoin* (en contrôlant que le payeur dispose bien de la somme, et qu'elle n'a pas déjà été dépensée au cours d'un échange précédent), puis la stocke dans un ensemble d'autres transactions (appelé un « bloc ») qu'il a validé de la même manière. De plus, il y ajoute certaines informations comme la date et l'heure, et rend le bloc infalsifiable grâce à un procédé cryptographique qui lui fournit un identifiant unique, sorte d'empreinte des transactions contenues dans celui-ci. Il est donc impossible de rajouter des transactions supplémentaires dans un bloc déjà validé, car l'empreinte ne correspondrait plus. Cette étape est ren-

due volontairement très coûteuse en temps de calcul par l'utilisation d'une preuve de travail (puzzle informatique à résoudre par l'ordinateur), afin d'assurer une cadence régulière (une dizaine de minutes) dans la production des blocs (la difficulté de ces puzzles s'adapte automatiquement afin que l'intervalle reste globalement constant, et donc qu'il ne soit pas fonction de la puissance de calcul des ordinateurs présents sur le réseau *bitcoin*).

Quand un mineur est arrivé à construire un bloc valide, il le diffuse sur le réseau *bitcoin*.

La dernière étape de validation consiste à l'insertion de ce nouveau bloc de transactions au sein de la *blockchain*. Tous les utilisateurs du réseau ayant reçu ce nouveau bloc tentent de l'intégrer au sein de la copie de la *blockchain* contenue sur leur ordinateur. S'ils y parviennent (les transactions sont bien nouvelles et sont cohérentes vis-à-vis des transactions précédentes), alors ils ajoutent ce bloc à la fin de la *blockchain* qui s'allonge ainsi d'un nouveau bloc de transactions.

2.2. Incitations

Maintenant que nous avons vu comment des transactions peuvent être effectuées dans le réseau *bitcoin*, intéressons-nous à la question des incitations. Nous avons vu qu'ajouter un bloc de transactions était coûteux en termes de temps de calcul pour les utilisateurs. Comment faire pour les inciter à résoudre ces puzzles, afin qu'ils ne se contentent pas tous d'effectuer des transactions ? Si personne ne prend la peine de les valider, le système ne fonctionnera plus. Il y a deux réponses à cette question : la création de nouveaux *bitcoins* à chaque validation de bloc qui va rémunérer les mineurs, et la possibilité pour ces mêmes mineurs d'exiger des frais de transactions. Actuellement, seul le premier mécanisme est utilisé pour rémunérer les mineurs. Le second ne sera utilisé que lorsque le nombre maximum de *bitcoins* sera atteint, comme nous le verrons par la suite. Concernant le montant des frais de transactions, celui est laissé à l'appréciation des utilisateurs. Lorsqu'un utilisateur fait une transaction (le payeur), il a la possibilité de proposer un certain nombre de *bitcoins* à celui qui validera sa transaction. Chaque mineur, quant à lui, peut choisir un seuil minimal de frais de transactions sous lequel il ne la validera pas. Il pourrait donc être potentiellement utile d'offrir des frais de transactions relativement élevés afin d'être sûr de voir sa transaction validée rapidement.

2.3. Création monétaire

La création de nouveaux *bitcoins* n'a rien à voir avec celle des monnaies classiques. La masse monétaire ne s'adapte pas à la richesse échangée par son biais. Elle se rapprocherait plutôt des métaux précieux comme l'or, ce qui a poussé certain à définir les *bitcoins* comme de l'or numérique. Les *bitcoins* sont émis de manière régulière à chaque validation d'un nouveau bloc de transactions. Le nombre de *bitcoins* crée à chaque validation diminue dans le temps. À l'origine du système, 50 *bitcoins* étaient créés à chaque validation d'un bloc. Donc environ 50 *bitcoins* toutes les dix minutes. Mais le *bitcoin* est programmé afin que ce nombre soit divisé par deux tous les quatre ans. Et ce jusqu'à finir par être nul d'ici quelques années (en 2140). À cette date, le nombre de *bitcoins* en circulation sera de 21 millions, et plus aucun *bitcoin* ne sera plus, et ne pourra plus, jamais être créé de quelque manière que ce soit. La création monétaire n'étant fonction d'aucun organisme pouvant procéder à des émissions monétaires massives (comme on peut en observer ces dernières années avec les assouplissements quantitatifs observés aux États-Unis par exemple), le *bitcoin* est en théorie peu enclin à subir une inflation. Au contraire, d'un point de vue purement théorique et à très long terme, on peut imaginer que le nombre de *bitcoins* retombera à 0 (bien sûr, dans la pratique, cela n'arrivera jamais). En effet, le nombre total qui sera créé est connu : 21 millions. Mais il est inévitable que des utilisateurs perdront leurs *bitcoins*, en oubliant leur mot de passe, ou suite à un décès si le mot de passe n'est communiqué à aucun héritier, entre autres exemples. Le nombre de *bitcoins* sera donc forcément décroissant à l'horizon 2140. Nous pouvons donc supposer que celui-ci sera une monnaie à tendance déflationniste.

3. RISQUES ET LIMITATIONS TECHNIQUES

Lorsque l'on parle du risque concernant le *bitcoin*, on parle rarement des risques techniques inhérents à la nature même du *bitcoin*, mais plus des risques de bulles spéculatives concernant la valeur du *bitcoin*, ou de sa réputation (usurpée) d'être une monnaie anonyme servant principalement à payer de la drogue ou à embaucher des tueurs à gages. Choses auxquelles nous ne nous intéressons pas ici.

Nous parlerons uniquement des problèmes techniques et des faiblesses du système. Le premier et le plus évident est le risque d'existence de bugs informatiques présents dans le code du *bitcoin*. Mais celui-ci étant open source avec une communauté très active, le risque de problème majeur qui ne serait pas corrigé rapidement semble très faible.

Un autre problème assez évident à comprendre est celui de la taille de la *blockchain*. Celle-ci devant regrouper la totalité des transactions ayant eu lieu de tout temps sur le réseau *bitcoin*, sa taille sera donc forcément strictement croissante. Le risque étant que, devenant trop importante, elle ne puisse plus être stockée sur l'ordinateur personnel d'un utilisateur lambda, réduisant ainsi le nombre de mineurs potentiels. Mais les performances des ordinateurs ayant tendance à augmenter avec le temps, on peut supposer que ce problème ne se posera pas à court terme, d'autant plus que des méthodes informatiques permettant de diminuer la taille de cette chaîne peuvent potentiellement être implémentées en cas de besoin.

Un autre problème bien connu est la possibilité d'une collusion entre une majorité de mineurs du réseau *bitcoin*. En effet, si une entité contrôle la majorité des mineurs, alors cette entité est à même de choisir quelles transactions seront ou ne seront pas acceptées dans la *blockchain*. De fait, cette entité contrôlera le système *bitcoin* aussi longtemps qu'elle sera majoritaire. Ce risque est bien réel : le 13 juin 2014, une communauté de mineurs

appelée guash.io a regroupé plus de 50 % des ressources informatiques utilisées pour miner les *bitcoins*, et aurait théoriquement pu prendre le contrôle du *bitcoin*, mais heureusement n'en avait pas la volonté.

Une des limitations du système est le délai nécessaire à la validation d'une transaction. En effet, une transaction n'est validée qu'une fois intégrée à la *blockchain*, ce qui peut prendre jusqu'à dix minutes. Ce fait, couplé à une absence totale d'assurance des transactions effectuées en *bitcoins* (aucun recours possible), empêche toute transaction rapide (à moins d'être prêt à courir le risque, c'est-à-dire en faisant confiance à la personne avec laquelle vous faites échange).

CONCLUSION

D'un point de vue technique, le fonctionnement du *bitcoin* en lui-même est intéressant, le protocole ayant prouvé sa robustesse et son efficacité. Mais il est très difficile de faire des pronostics quant à son évolution, sur son avenir en tant que monnaie, et cela dépend très peu de l'aspect technique. Même fonctionnant à la perfection, certains problèmes persisteraient malgré tout. Tout d'abord, une infinité d'autres crypto-monnaies peuvent être créées, pouvant être de simples clones rigoureusement identiques ou posséder des caractéristiques différentes. De nombreuses (des centaines) alternatives existent déjà. Nous pouvons citer, entre autres, Ripple, Litecoin, Peercoin, Darkcoin (première crypto-monnaie cherchant à être réellement anonyme), et bien d'autres. *Bitcoin* sera, et est d'ores et déjà, concurrencé par d'autres crypto-monnaies. Il est à craindre que leur multiplication dilue la valeur des *bitcoins* aux yeux des utilisateurs. Ensuite, la forte volatilité des cours qui peut être observée interdit aux *bitcoins* d'être considérés comme autre chose qu'un bien hautement spéculatif, rendant difficile pour les entreprises leur utilisation comme moyen de paiement privilégié. Enfin, l'absence de cadre réglementaire fixé pèse sur le développement des crypto-monnaies. Rien ne nous dit que les transactions en *bitcoins* ne seront pas interdites par certains Etats ; l'exemple de la Chine interdisant aux établissements financiers toutes transactions en *bitcoins* montre que la menace est réelle. ■

Références

- Nakamoto S. (2008), *Bitcoin: A Peer-to-peer Electronic Cash System*.
- Reid F. & M. Harrigan (2012), *An Analysis of Anonymity in the Bitcoin System*, Arxiv : 1107.4524.

Sources

- De nombreuses informations concernant le *bitcoin* peuvent être trouvées (entre autres) sur :
- le site personnel de Stéphane Frénot : http://www.jumplyn.com:8005/ ;
- les sites web bitcoin.fr et bitcoin.com.