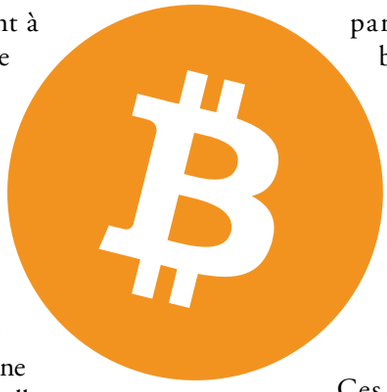
La cryptographie réinvente la monnaie : le *Bitcoin*

Par **Jean-Paul DELAHAYE**
Professeur émérite à l'Université Lille 1
Chercheur au Laboratoire d'Informatique Fondamentale de Lille

En 2008, un événement important s'est produit qui sera un jour inscrit dans les livres d'histoire : une nouvelle façon de concevoir la monnaie a été proposée, qui remet en cause les anciennes idées sur cette institution. Comme pour le courrier électronique ou internet qui ne sont aux mains d'aucune autorité et conduisent donc une meilleure appropriation de l'information par tous, et des pratiques démocratiques nouvelles de communication entre citoyens, il semble que, dans le domaine de la monnaie, tout pourrait fonctionner sans autorité centrale dominante de contrôle.

En effet, fin 2008, l'énigmatique Satoshi Nakamoto – c'est un pseudonyme – publie sur internet un texte décrivant comment il est possible, grâce aux réseaux et à la cryptographie mathématique moderne, de mettre en place une monnaie qui n'a besoin d'aucun contrôle centralisé pour fonctionner, contrairement à toutes les monnaies et à tous les systèmes de paiement en ligne. Le 3 janvier 2009, les programmes nécessaires au lancement de cette crypto-monnaie, le *Bitcoin*, sont prêts et elle est créée. Après des débuts confidentiels où seuls quelques cryptologues avertis s'y intéressent, elle commence à prospérer et son cours, totalement dérisoire en 2009, prend alors son envol, lui donnant une réalité concrète. Début 2013, un *Bitcoin* vaut une dizaine d'euros. L'année 2013 est celle du décollage du *Bitcoin* qui acquiert alors une notoriété mondiale. Il voit son cours multiplié par 50 en un an, pour atteindre 580 euros le 1er janvier 2014. La capitalisation totale des *Bitcoins* atteint alors plus de 6 milliards d'euros. À partir de rien, la cryptologie mathématique vient de créer des devises numériques qui s'échangent contre de l'argent sonnant et trébuchant, permettant par exemple à un étudiant Norvégien – Christoffer Kock – qui avait acquis pour 25 euros de *Bitcoins* en 2009, de les revendre et de s'acheter un appartement au centre d'Oslo.



Quelle est l'idée de cette monnaie ? En quoi est-elle une révolution ? Doit-on la craindre ou se réjouir de sa création ?

Miraculeuses mathématiques

L'idée de cette monnaie est que, grâce à un subtil agencement de protocoles cryptographiques, on peut émettre une monnaie dont le contrôle se fera collectivement sur le réseau internet, sans qu'aucune autorité ne dispose du pouvoir d'agir sur elle. Le protocole de Nakamoto a été rendu possible grâce aux progrès de la cryptographie mathématique qui a inventé, depuis cinquante ans, une multitude de primitives numériques inattendues. Primitives de chiffrages (transformations d'un message en un autre impossible à lire, sauf si on connaît une clef particulière qui peut être différente de la clef utilisée pour le chiffrage) ; primitives d'authentification (méthodes assurant qu'une personne agissant à l'autre bout du réseau est bien celle qui en a le droit, par exemple pour l'utilisation d'une carte bancaire) ; primitives de signatures (créations de traces numériques permettant de certifier qu'un message est bien émis par une personne donnée et interdisant que le message signé soit modifié) ; primitives de « preuve de travail » (défis soumis à un dispositif de calcul ne pouvant pas être exécuté rapidement et servant par exemple à lutter contre le « spam »), etc.

Ces primitives, convenablement assemblées, autorisent la réalisation de dispositifs numériques qu'on pensait impossibles auparavant. La mise en place du protocole *Bitcoin* doit aussi son existence à la puissance informatique dont chacun dispose et qui fait qu'avec son ordinateur personnel il peut participer au contrôle de la monnaie *Bitcoin* au travers d'un réseau décentralisé, dit « P2P ».

Tous ceux qui le souhaitent peuvent télécharger des logiciels (libres et ouverts, dont le code est accessible à tous) et participer à la surveillance de la monnaie *Bitcoin*, c'est-à-dire vérifier que personne ne crée de *Bitcoins* non prévus par le protocole, et que toutes les transactions se déroulent conformément aux règles définies.

Comment avoir des *Bitcoins* ?

Pour posséder des *Bitcoins,* il faut disposer d'un compte, mais il n'est pas besoin de donner son identité pour en créer un : l'anonymat des détenteurs de *Bitcoins* est l'une des caractéristiques de cette monnaie, nous y reviendrons. Chaque compte possède deux numéros. Le numéro secret (qu'il faut absolument garder pour soi, car quiconque en dispose peut dépenser le contenu du compte), et le numéro

public que vous communiquerez et qui vous permet de recevoir des *Bitcoins*.

On obtient des *Bitcoins*, soit en en achetant contre de l'argent usuel sur les plateformes de change : elles prennent vos euros et vous envoient en retour des *Bitcoins* qui s'inscrivent sur votre compte. On peut aussi en acquérir en faisant du commerce : vous vendez un livre à quelqu'un qui vous paie en versant des *Bitcoins* sur votre compte.

Une troisième façon d'obtenir des *Bitcoins* est de participer activement à la surveillance de la monnaie. Les machines qui acceptent de consacrer une part de leur puissance à cette surveillance sont ce qu'on appelle les *mineurs* de *Bitcoins*. En effet, le travail qu'elles fournissent reçoit régulièrement une récompense (en *Bitcoins*) comme des mineurs dans une mine de métal précieux. Cette récompense est de 25 *Bitcoins* toutes les 10 minutes, mais elle n'est attribuée qu'à un seul mineur tiré au sort : il a la chance de trouver l'équivalent d'une pépite d'or. Aujourd'hui, un très grand nombre de mineurs travaillent à la surveillance de la monnaie. C'est très bien, car cela rend la monnaie plus solide, mais cela rend aussi très faible la probabilité que votre machine soit choisie pour recevoir les 25 *Bitcoins* distribués, d'autant plus que cette probabilité de gagner est proportionnelle à la puissance de votre machine et que des concurrents très puissants (utilisant même des puces spécialisées) sont apparus, diminuant encore plus vos chances de gagner avec votre petit ordinateur.

Dureté et persistance des *Bitcoins*

Les *Bitcoins* n'existent pas matériellement, ils n'existent que sur le réseau, et sont le résultat d'un consensus entre utilisateurs qui, grâce aux informations présentes sur le réseau et que chacun peut consulter et contrôler, indiquent quelles sommes d'argent se trouvent sur les comptes. L'ensemble des comptes et leurs soldes sont stockés dans un fichier – la *blockchain* – accessible à tous. Le protocole cryptographique de la monnaie assure que personne ne peut manipuler les comptes, fausser les transactions, ou émettre d'autres *Bitcoins* que ceux qui sont prévus. Il y en a 12 millions aujourd'hui et leur nombre ne dépassera jamais 21 millions (ce maximum est inscrit dans le protocole).

La robustesse du protocole – confirmée par 5 ans de fonctionnement – rend l'existence virtuelle et purement numérique des *Bitcoins* aussi réelle et solide que celle des lingots d'or ou des billets de banque que vous avez en poche. La cryptographie a réussi à créer des objets virtuels infalsifiables, aussi résistants et persistants que s'ils étaient faits de métal, et qu'on peut faire circuler à la vitesse de la lumière (c'est un des avantages des *Bitcoins* sur toutes les autres monnaies) sans coût, d'un endroit à l'autre du monde. Comme toute monnaie, le *Bitcoin* ne tient que par la confiance de ses utilisateurs mais, ici, celle-ci s'établit non pas parce qu'une banque centrale émettrice prétend se porter garante des devises qui circulent (on sait ce qu'il en est en cas de crise !), mais parce que le protocole cryptographique empêche quiconque de truquer les comptes et, en particulier, d'émettre sans retenue des masses de devises qui feraient s'effondrer sa valeur.

La nouveauté principale de cette crypto-monnaie est que cet argent numérique n'est contrôlé par aucune banque centrale et qu'elle est gérée collectivement – démocratiquement disent certains – par tous ceux qui le souhaitent et qui se surveillent mutuellement.

Les caractéristiques des *Bitcoins* ont des *conséquences positives* dont une protection des détenteurs de *Bitcoins* contre l'inflation. Celle-ci provient habituellement de l'émission massive, par les banques centrales, de devises créées à partir de rien : la fameuse planche à billets. Pour le *Bitcoin*, aucune émission en dehors de celle inscrite dans le protocole (et qui est de plus en plus faible, au cours du temps) n'est possible et, donc, *a priori*, il ne peut y avoir dévaluation de la monnaie. Certains prétendent que, par nature, le *Bitcoin* est déflationniste : il ne pourrait que prendre de la valeur.

Incertitudes et risques

Malheureusement, les propriétés de la monnaie *Bitcoin* ont aussi des conséquences négatives. Citons-en quelques-unes :

- Il faut être très attentif lors de la manipulation informatique de son compte, et si un pirate réussit à trouver votre numéro secret de compte en s'introduisant sur votre ordinateur, il pourra en dépenser entièrement le contenu. C'est déjà arrivé ! N'effacez pas non plus votre porte-monnaie numérique par erreur, il serait définitivement perdu. C'est déjà arrivé !,

- L'anonymat (partiel) des comptes intéresse toutes sortes de gens peu recommandables qui utilisent le *Bitcoin* pour échapper au fisc ou mener des trafics en tout genre,

- Le fait qu'aucun contrôle centralisé ne soit opéré par une autorité centrale a pour conséquence que le cours des *Bitcoins*

est soumis à de fortes variations spéculatives. Certains affirment même que le cours du *Bitcoin* est manipulé par ceux qui en détiennent beaucoup. La valeur du *Bitcoin* varie de plusieurs pourcents par jour, et il est arrivé qu'elle varie de plus de 40 % dans une même journée. Cela rend difficile son usage pour le commerce ! ,

- Le fait qu'elle soit concurrente des monnaies des banques centrales a pour conséquence que les États lui sont souvent hostiles et que des réglementations existent, limitant son usage ou même l'interdisant. L'évolution de ces réglementations sera essentielle pour l'avenir du *Bitcoin*,

- Le fait que tous les programmes contribuant au fonctionnement de la monnaie *Bitcoin* sont libres et publics entraîne qu'il est facile de concevoir et de faire fonctionner d'autres monnaies du même type. C'est d'ailleurs ce qui se produit : il existe aujourd'hui plus de 80 monnaies cryptographiques basées sur les mêmes principes que le *Bitcoin* et lui faisant concurrence. Légèrement différentes du *Bitcoin*, elles peuvent posséder des propriétés intéressantes pour certains usages (par exemple, celle d'assurer un anonymat total que n'assure pas le *Bitcoin*) qui feront se détourner du *Bitcoin*.

Ces crypto-monnaies ont chacune une ambition globale et sont conçues prioritairement pour faire circuler le plus facilement possible de la valeur d'un endroit sur terre à un autre. Elles viennent s'ajouter aux « monnaies locales complémentaires » (MLC : le *sol alpin* à Grenoble, la *graine* à Montpellier, le *miel* dans le Libournais, etc.) qui fonctionnent selon des principes totalement différents en général dans le but de favoriser les échanges locaux et le troc (mais qui s'appuient toujours sur un contrôle centralisé). Il est remarquable, et sans doute significatif, de voir qu'aujourd'hui le fonctionnement monétaire imposé par les états, et qui semblait immuable, est contesté à la fois localement et globalement.

Quel avenir ?

On s'interroge sur ce que va devenir le *Bitcoin* né des mathématiques. Comme aucune monnaie de ce type n'a jamais existé auparavant, il est vraiment difficile de faire un pronostic et les avis sont partagés. Certains pensent que son cours élevé aujourd'hui est une bulle qui éclatera et fera perdre toute valeur aux *Bitcoins* : ceux qui en achètent finiront par perdre tout ce qu'ils y mettent. D'autres soutiennent que le *Bitcoin* possède des propriétés telles qu'il gardera toujours un certain intérêt pour mener des transactions rapides, sans coût et anonymes, ou pour conserver de l'argent à l'abri de l'inflation, sous une forme discrète (vous pouvez mémoriser votre numéro de compte secret et tout effacer de votre ordinateur, il vous permettra partout dans le monde de retrouver vos *Bitcoins*) et, donc, que le *Bitcoin* persistera et que son cours ira en s'accroissant au fur et à mesure que les utilisateurs seront plus nombreux. ■

Bibliographie

- Banque de France, *Dangers liés au développement des monnaies virtuelles, l'exemple du Bitcoin*, 2013 : http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf

- Blockchain, *Information et statistiques sur le cahier des comptes* Bitcoin, https://blockchain.info/fr

- Jean-Paul Delahaye, *Bitcoin, la crypto-monnaie*, Pour la science, pages 76-81, décembre 2013 : http://www.lifl.fr/~delahaye/pls/2013/241.pdf

- Jean-Paul Delahaye, *Blog SciLog*, décembre 2013 : http://www.scilogs.fr/complexites/plaidoyer-pour-le-bitcoin/

- Jean-Paul Delahaye, *Le Bitcoin, une monnaie révolutionnaire*, janvier 2014 : http://www.lifl.fr/~delahaye/Bitcoin/Bitcoin.pdf

- Michael Nilsen, *How the Bitcoin protocole actually works*, Data Diven Intelligence, décembre 2013 : http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

- Pierre Noizat, *Bitcoin Book*, 2012 : ISBN-10: 2954310103.

- Wikipedia, *Bitcoin* : http://fr.wikipedia.org/wiki/Bitcoin