LOGIQUE & CALCUL

Bitcoin, la cryptomonnaie

La cryptographie et la puissance des réseaux ont rendu possible l'existence de monnaies purement numériques et dépourvues d'une autorité centrale de contrôle.

Jean-Paul DELAHAYE

Une nouvelle monnaie purement électronique intéresse de plus en plus. Ne s'appuyant sur rien de tangible, le total des devises sorties d'un protocole cryptographique vaut aujourd'hui l'équivalent de un milliard d'euros.

Le *bitcoin* a été proposé en 2008 et mis en œuvre le 3 janvier 2009 par un chercheur, ou peut-être plusieurs, caché sous le pseudonyme de Satoshi Nakamoto. La logique de cette monnaie numérique et la confiance qu'elle inspire seront le but de notre analyse. Le sujet est passionnant du fait de l'originalité, du mystère et du succès de cette construction informatique ; il est important, car on a affaire à un nouveau type de monnaie susceptible de jouer un rôle central en économie ; et il est délicat, car personne ne sait ce que ce montage numérique va devenir.

D'une certaine façon, toutes les monnaies sont électroniques : depuis longtemps, presque toutes les opérations bancaires se réduisent à des jeux d'écritures opérés dans les mémoires des ordinateurs. Cela signifie que l'on sait faire des systèmes informatiques robustes manipulant l'argent, même quand il s'agit de dizaines de milliards d'euros. Certes, les pannes, les « bugs », les virus, les pirates informatiques existent, mais on réussit assez bien à s'en protéger : l'informatisation du stockage et du transfert massif d'argent n'a pas entraîné de catastrophes. Les crises financières comme celle de 2009 n'ont pas pour origine le dysfonctionnement ou la fraude informatique, mais des erreurs d'analyse économique et financière commises par des humains, qui sont par ailleurs parfois trop voraces, voire malhonnêtes.

Pas d'autorité centrale

Aujourd'hui, toute monnaie repose sur une autorité centrale : une banque, adossée à un État ou à une association d'États. C'est aussi le cas de tous les systèmes de pseudo-monnaies électroniques privées, les monnaies « complémentaires » ou « alternatives ». Elles permettent des paiements par Internet *(Paypal)*, le commerce au sein d'un jeu sur le réseau (le dollar *Linden* de *Second Life*) ou la fidélisation des clients (les *miles* des compagnies aériennes, les points que votre superette inscrit sur votre compte à chaque passage aux caisses).

Les *bitcoins* sont conçus pour s'autoréguler. Le bon fonctionnement des échanges est garanti par une organisation générale que tout le monde peut examiner, car tout y est public : les protocoles de base, les algorithmes cryptographiques utilisés, les programmes les rendant opérationnels et les données des comptes.

À tout instant, chacun peut savoir combien il y a de *bitcoins* sur chaque compte existant et participer à la vérification des nouvelles transactions. Cette transparence totale n'empêche pas l'anonymat, les propriétaires des comptes n'étant pas tenus de se déclarer. C'est presque un paradoxe : tout mouvement de *bitcoins* est public et, pourtant, l'anonymat des détenteurs est protégé.

La possession des *bitcoins* est matérialisée par une suite de chiffres et de lettres qui constituent un porte-monnaie virtuel (ou compte). Une personne peut détenir plusieurs porte-monnaie. Le porte-monnaie comporte le montant en *bitcoins* de l'argent qu'il contient, une clef publique qu'on peut laisser circuler et une clef privée qui doit rester secrète, car son détenteur peut dépenser l'argent du porte-monnaie.

Tout support convient pour conserver la suite de symboles constituant votre porte-monnaie : papier, clef USB, la mémoire, etc. Grâce à des logiciels adéquats, vous pouvez gérer votre porte-monnaie sur votre ordinateur ou votre téléphone. Nombre de ces logiciels sont développés dans le cadre d'un projet *open source* : les programmes ne sont pas secrets et ceux qui le veulent peuvent contrôler ce qu'ils font et même contribuer à leur amélioration *(voir https://multibit.org/)*.

Pour avoir des *bitcoins* sur un compte, il faut soit qu'un détenteur de *bitcoins* vous en ait donné, par exemple en échange d'un bien, soit passer par une plate-forme informatique qui convertit des devises classiques en *bitcoins*, soit les avoir gagnés en participant aux opérations de contrôle

1. La signature et l'identification d'un document

Un protocole de signature à double clef est la donnée de deux fonctions f et g permettant de signer les messages et d'interpréter les signatures. Ces fonctions sont connues de tous. Nous ne nous préoccupons pas ici de la teneur du message, mais seulement de son identification.

À Alice sont associées deux clefs, A_{pri} (clef privée) et A_{pub} (clef publique). Ce sont des suites de chiffres. A_{pub} est accessible à tous, mais la clef A_{pri} n'est connue que d'Alice. Il est impossible en pratique de déduire A_{pri} de la connaissance de A_{pub}.

Les deux fonctions f et g servent à signer un message et à lire la signature.

Soit M un message à signer. Alice applique f aux données A_{pri} et M : $f(A_{pri}, M) = M'$. Ce sera le message signé par Alice. Toute personne ayant en main M' et connaissant la clef publique d'Alice vérifiera que c'est bien Alice qui a signé le message : pour cela, elle appliquera la fonction de lecture g aux données A_{pub} et M', ce qui donne M, car $g(A_{pub}, M') = M$. Le fait qu'il soit nécessaire d'appliquer la clef publique d'Alice à M' pour prendre connaissance du message empêche toute falsification du message M signé.

Il est parfois commode pour Alice de transmettre à la fois M et M', M' servant seulement à contrôler pour ceux qui le veulent qu'Alice a bien signé M avec sa clef privée.

Il existe de nombreuses façons de construire les fonctions f et g, mais la monnaie *bitcoin* est fondée sur la cryptographie à courbes elliptiques. La courbe employée est celle notée secp256k1. On aurait pu utiliser l'algorithme RSA, plus connu, mais il nécessite des clefs plus longues. La sécurité du système *Bitcoin* repose sur l'inviolabilité de la signature.

Les signatures de Napoléon Bonaparte.

collectif de la monnaie (nous verrons plus loin comment).

La gestion d'un porte-monnaie doit être très soigneuse. Si vous le perdez en l'effaçant par mégarde ou si vous oubliez le code secret qui permet d'y accéder, alors son contenu est perdu, comme quand vous lancez par-dessus bord un porte-monnaie réel au milieu de l'océan. De nombreux *bitcoins* ont ainsi été perdus par des utilisateurs imprudents ou négligents. Il n'est pas impossible non plus qu'on vous vole votre porte-monnaie virtuel, par exemple à l'occasion d'une intrusion dans votre ordinateur par un hacker. Pour éviter cela, certains porte-monnaie contenant d'importantes sommes en *bitcoins* sont gardés sur des ordinateurs non connectés au réseau ou éteints.

La cohérence des comptes, et donc la solidité de la monnaie *bitcoin*, se fonde sur un principe général de la théorie *Money is memory* de l'économiste américain Narayana Kocherlakota. Ce principe s'exprime ici sous la forme suivante :

– toutes les transactions faites depuis le début des *bitcoins,* le 3 janvier 2009, sont publiques et, à chaque instant, la somme totale des *bitcoins* émis est connue de tous, ainsi que le contenu de chaque porte-monnaie (mais pas le détenteur de ce porte-monnaie) ;

– seul celui qui connaît la clef secrète d'un porte-monnaie peut dépenser son contenu en envoyant tout ou partie de ce dernier à un autre porte-monnaie, cela à la vue de tous, ce qui permet à tous de connaître à chaque instant le contenu de chaque porte-monnaie ;

– tous ceux qui le souhaitent peuvent participer au calcul général de la répartition des *bitcoins* entre les porte-monnaie, cela à l'aide de logiciels (libres et gratuits) dont la correction est contrôlable par tous.

On n'utilise pas ici la cryptographie à clef publique pour cacher de l'information, mais pour signer les transactions. Toute transaction est irréversible, sauf accord explicite des deux contractants pour réaliser une transaction inverse. Quand vous avez dépensé l'argent d'un porte-monnaie, personne n'a autorité pour demander à celui qui a reçu l'argent de le rendre. C'est là une grande différence avec les monnaies numériques à autorité de contrôle centralisée où, assez fréquemment, des transactions sont annulées, parfois plusieurs jours après leur réalisation, ce qui donne lieu à toutes sortes d'escroqueries. L'absence d'autorité centrale et l'anonymat des comptes font qu'il sera très difficile d'agir sur celui qui détient le porte-monnaie ayant reçu vos *bitcoins*... même s'il ne vous livre pas l'achat que vous pensiez régler.

Ce système simplifié des *bitcoins* a une faille qui a contraint son inventeur à ajouter une série de dispositifs cryptographiques au mécanisme de base. La faille est que le propriétaire d'un porte-monnaie pourrait tenter de dépenser deux fois l'argent qu'il contient. Ces doubles dépenses seraient impossibles si les échanges étaient instantanés sur le réseau et si tout propriétaire d'un porte-monnaie participait au calcul continu du contenu de tous les porte-monnaie : sous cette hypothèse de connectivité totale et parfaite, celui qui recevrait l'argent d'un porte-monnaie déjà vidé (ou insuffisamment pourvu) refuserait la transaction, qui serait simultanément considérée invalide par tous.

Des améliorations

Malheureusement, les échanges électroniques ne sont pas instantanés, et certaines parties d'un réseau sont parfois temporairement déconnectées du reste. De plus, tous les utilisateurs de *bitcoins* ne souhaitent pas participer à la vérification continue de toutes les transactions et au recalcul permanent du solde de la totalité des comptes, car cela demande une grande puissance informatique et beaucoup de mémoire. Il faut donc améliorer le modèle.

Les améliorations se fondent sur une série de protocoles qui rendent la monnaie *bitcoin* résistante aux pannes du réseau ou de certaines machines et aux tentatives de manipulation de la monnaie ou de tricheries (dont les doubles dépenses). Ces perfectionnements rendent aussi facultative la participation au contrôle global des porte-monnaie ; pour éviter que trop peu de nœuds du réseau participent

au contrôle, un système de rémunération est prévu. Ce délicat agencement a étonné les spécialistes et prouve que l'inventeur des *bitcoins* est un cryptologue averti ou un groupe incluant d'excellents cryptologues.

Cette monnaie ne tient que par la cohérence et l'accord unanime de ceux qui y participent et s'entendent sur le contenu de chaque compte, que rien ne matérialise et qu'aucune autorité ne garantit. La construction logicielle et cryptographique doit donc assurer par elle-même que personne ne puisse augmenter le total des *bitcoins* détenus, ni modifier des comptes, sans que tout le monde s'en aperçoive rapidement. Il n'y a pas de police ; la conception même de la monnaie doit donc empêcher la fraude et les dysfonctionnements. Celle de Satoshi Nakamoto y parvient.

Le scepticisme sur la robustesse de la nouvelle monnaie s'atténue. La meilleure preuve est que la monnaie a tenu quatre ans, malgré toutes les attaques qu'elle a subies. C'est pourquoi la valeur actuelle d'un *bitcoin* dépasse 100 euros (mais le *bitcoin* fluctue beaucoup… il vaudra peut-être moins quand vous lirez l'article !).

Une page toutes les dix minutes

L'amélioration du modèle simplifié consiste à créer un cahier de comptes (dont le nom technique est *Blockchain*) qui est complété progressivement par ajout de nouvelles pages de transaction (nommées *blocs*) toutes les dix minutes environ, chaque ajout d'une page étant validé par ceux qui participent à la gestion et à la surveillance décentralisée des comptes. Pour récompenser cette vérification, un tirage au sort désigne toutes les dix minutes environ celui des participants qui ajoute la nouvelle page au cahier de comptes, et qui est rémunéré pour cela par 25 *bitcoins* créés *ex nihilo*. Lorsque la nouvelle page est ajoutée au cahier de comptes, les transactions qui y apparaissent sont validées. Cette création de *bitcoins* est la seule possible, et tous les *bitcoins* existants sont apparus de cette façon.

Lors d'une transaction en ma faveur, mon ordinateur connecté au réseau consulte le cahier de comptes et vérifie que le porte-monnaie qui m'envoie des *bitcoins* ne les a pas déjà dépensés. Cependant, à cause de la possibilité d'une double dépense simultanée, une transaction n'est considérée comme valide que si elle apparaît dans le cahier de comptes. Par conséquent, pour être assuré de l'irréversibilité (par exemple avant d'envoyer le livre qu'on vient de vous acheter en vous faisant parvenir

2. Le protocole d'une transaction

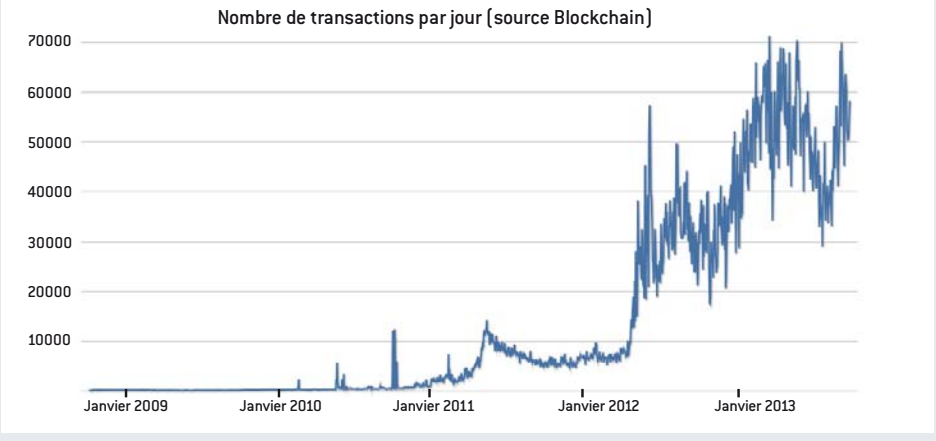
Lorsqu'Alice veut faire un paiement en *bitcoins* à Bernard (par exemple en échange d'un livre), leurs ordinateurs vont opérer une série d'échanges. Ces échanges sont gérés automatiquement par les logiciels installés sur leurs ordinateurs. Les communications sur le réseau *Bitcoin* se font directement entre les deux correspondants, qui y ont des rôles équivalents. On parle de réseaux pair-à-pair (ou P2P, *peer-to-peer*). L'existence de tels réseaux est essentielle pour la monnaie *bitcoins*, qui n'est gérée par aucun nœud central de réseau qui contrôlerait l'ensemble des communications. La transaction qui résulte des échanges entre Alice et Bernard sera publique (tous les ordinateurs présents sur le réseau y auront accès) et permettra la mise à jour par tous du cahier de comptes, qui indique combien de *bitcoins* sont déposés dans chaque porte-monnaie existant.

- Alice souhaite envoyer N *bitcoins* à Bernard.
- Bernard communique sa clef publique B_{pub} à Alice.
- Alice forge un message M de transaction contenant la clef publique B_{pub} de Bernard et la somme N à transférer : $M = B_{pub}\, N$.
- Alice signe la transaction M avec sa clef privée A_{pri}, c'est-à-dire calcule une suite de symboles $M' = f(A_{pri}, M)$ qui, avec sa clef publique A_{pub}, redonne M : $g(A_{pub}, M') = M$ (tout le monde peut donc contrôler que c'est Alice qui a signé, mais personne ne peut signer à sa place).
- Alice diffuse la transaction signée sur le réseau afin qu'elle soit vue par tout le monde. Le protocole réel est légèrement plus compliqué (il contrôle qu'Alice dispose bien de la somme N dans son porte-monnaie).

En regardant cette transaction depuis l'extérieur, tout le monde voit que l'individu qui contrôle le compte d'Alice (individu que personne ne connaît) a donné son accord pour transférer N *bitcoins* sur le compte contrôlé par l'individu Bernard (que nul ne connaît).

Ne disposant pas de la clef privée d'Alice, personne d'autre qu'elle ne peut envoyer une telle transaction sur le réseau. Son envoi est donc la preuve qu'Alice était d'accord pour le transfert. Tout le monde considérera alors le transfert comme valide.

Le protocole de signature à doubles clefs utilisé est considéré comme robuste. Bien sûr, s'il venait à être cassé (c'est-à-dire si, par exemple, on réussissait à trouver une méthode rapide pour calculer la clef privée à partir de la clef publique), tout le système de la monnaie *bitcoin* s'effondrerait.



3. La naissance du *bitcoin*, Satoshi Nakamoto et l'anonymat

Le *bitcoin* a été défini en 2008 par un personnage actuellement anonyme au nom d'emprunt de Satoshi Nakamoto, qui dit avoir travaillé deux ans à la conception de sa monnaie. Une grande traque se déroule sur Internet pour identifier le personnage. On analyse la façon dont il s'est exprimé en anglais, on fait des listes de personnes pouvant avoir les compétences requises… et on spécule.

L'anonymat des utilisateurs des *bitcoins* est assuré par le fait que seuls les numéros et les contenus des comptes sont nécessaires au maintien de la cohérence du livre des comptes (la « Blockchain »). La clef privée d'un compte assure son propriétaire que lui seul pourra dépenser l'argent qui s'y trouve. En théorie, donc, l'anonymat des détenteurs de comptes est assuré. Cependant, l'anonymat n'est pas absolu. D'une part, on peut suivre le déplacement des *bitcoins* d'un compte à l'autre et ainsi en déduire des informations sur le propriétaire unique d'une série de comptes visiblement gérés par une seule personne. De plus, au moment de transformer des *bitcoins* en euros ou en une devise classique, l'anonymat n'est plus possible.

Des chercheurs, dont Sergio Lerner, ont étudié le cahier de comptes du *bitcoin* et conclu que S. Nakamoto détient probablement l'équivalent de dix pour cent des *bitcoins* émis à ce jour. Il est en effet à peu près certain qu'au lancement de la monnaie, il fut le seul à « miner » les *bitcoins* pour se constituer un pécule personnel et qu'il a regroupé ce pécule sur quelques comptes en nombre assez limité.

L'invention des *bitcoins* aurait permis à Nakamoto de se constituer une fortune de l'ordre de 100 millions de dollars (au cours d'aujourd'hui). Il lui sera difficile de les remettre sur le marché sans dévoiler son identité, à moins qu'il mette en action des techniques de brouillage faisant perdre sa trace !

un paiement en *bitcoins*), il faut attendre dix minutes et voir sa transaction sur la nouvelle page du cahier.

La non-transmission instantanée des messages a pour conséquence que, parfois, deux ajouts de pages au cahier se feront presque simultanément dans deux parties éloignées du réseau, créant temporairement un dédoublement du cahier de comptes. Les deux versions peuvent alors contenir une dernière page sensiblement différente, ce qui rend alors possible une double dépense. L'événement est rare, mais comme il est possible et inévitable à cause de l'imperfection des communications, un procédé de remise en ordre du système est prévu. Les deux cahiers continueront chacun de leur côté à se voir ajouter des pages toutes les dix minutes environ. Le temps nécessaire à l'ajout est lié au processus de tirage au sort qui désigne le gagnant des 25 *bitcoins*. Les ajouts de pages des deux cahiers malencontreusement créés ne se feront donc pas à la même vitesse exactement. Le cahier le plus long (celui qui a été complété de plusieurs nouvelles pages le plus rapidement) est considéré comme le bon. Cette règle, traduite dans les programmes de vérification des comptes, conduit à l'élimination de l'autre cahier et à la reconstitution d'un état cohérent du système, où ne persiste qu'un seul cahier et où les doubles dépenses sont impossibles.

Ces ennuis temporaires, rares mais inévitables, dans la gestion du cahier de comptes ont pour conséquence que pour être certain qu'une transaction soit définitivement valide (c'est important dans le cas de grosses sommes), il faut attendre non pas dix minutes, mais plusieurs fois ce délai. On considère qu'une heure produit une garantie parfaite.

Ruée vers l'or numérique

La désignation des gagnants des 25 *bitcoins*, toutes les dix minutes, se fait par un processus cryptographique qui en assure la parfaite honnêteté et surtout une totale imprévisibilité et « infalsifiabilité » (il est impossible de manipuler le choix du gagnant). Le tirage au sort vous donne d'autant plus de chances de gagner que vous disposez de plus de puissance de calcul. Plus vous acceptez de consacrer des ressources de calcul à tenter de gagner, plus vous augmentez vos chances de gagner. Le travail fait par vos machines pour tenter de gagner porte le nom de *minage*, par analogie au travail dans une mine qui conduit ceux qui ont de la chance à trouver de l'or.

Aujourd'hui, participer à ces tirages au sort (et donc participer au contrôle général des comptes) est très tentant : 25 *bitcoins* s'échangent contre environ 3 200 euros (au 26 octobre 2013). Du coup, les « mineurs de *bitcoins* », comme ils se nomment, se sont multipliés, ce qui renforce le système de contrôle général des comptes. Les mineurs de *bitcoins* ont progressivement perfectionné leurs outils avec l'espoir d'augmenter leurs chances de gagner. Dans un premier temps, les mineurs ont programmé des cartes graphiques pour effectuer, le plus rapidement possible, les calculs demandés par le minage. En effet, les cartes graphiques disposent d'une puissance importante et on peut la détourner à d'autres choses que le simple traitement des images numériques. Aujourd'hui, les cartes graphiques ne suffisent pas pour avoir de bonnes chances de gagner, car, à mesure que plus de mineurs se sont mis à jouer, il est devenu plus difficile de gagner.

Précisons que le système de S. Nakamoto est conçu pour qu'il y ait un gagnant toutes les dix minutes environ et qu'il s'ajuste automatiquement pour que ce temps moyen ne diminue pas. Des entreprises se sont donc mises à fabriquer des cartes et des machines spécialisées dont le seul objectif est de miner les *bitcoins*. La consommation électrique consacrée au minage s'est considérablement accrue depuis un an. Le phénomène ressemble un peu à une ruée vers l'or, sauf qu'ici tout se déroule dans le monde des réseaux et des ordinateurs en faisant circuler des bits d'information et fonctionner des microprocesseurs dédiés.

En raison de la puissance de calcul nécessaire, il devient impossible, même pour un acteur très puissant, et on sait qu'il en existe, de s'emparer de tous les gains. L'analyse générale du protocole des *bitcoins*, effectuée dès 2008 par S. Nakamoto, montre que si un acteur pouvait disposer de la moitié de la puissance consacrée au « minage », il serait en mesure

4. Forces et faiblesses des *bitcoins*

Nouveauté, forces et qualités des bitcoins

– La monnaie *bitcoin* est fondée sur un réseau pair-à-pair et des logiciels libres et gratuits. Indépendante de toute banque, elle n'est pas soumise à une autorité centralisée et est complétement transparente.

– Les transactions de *bitcoins* sont rapides et irréversibles (après un délai d'une heure ou moins). Personne ne peut agir sur les *bitcoins* de vos comptes sans votre consentement.

– Il n'y a pas de frais de transaction ou de gestion, ou ceux-ci sont minimes (électricité, réseau, commissions volontaires et déterminées par l'utilisateur).

– Le nombre de *bitcoins* ne dépassera jamais 21 millions. Avec les *bitcoins*, vous échappez au risque qu'un acteur dominant (une banque centrale) décide de faire fonctionner la planche à billets et vous prenne de l'argent par l'inflation créée.

– Anonymat : le réseau fonctionne à partir de comptes. Détenir un compte, c'est connaître la clef privée qui lui est associée. L'identité des utilisateurs n'est utile à aucun moment.

– Un *bitcoin* peut être divisé en fractions de *bitcoin* jusqu'au 1/100 000 000e.

– Le *bitcoin* (à cause du nombre maximal de *bitcoins* en circulation) est déflationniste (il prend peu à peu de la valeur) : vos économies ne sont pas rongées par l'inflation, mais s'apprécient !

– Le *bitcoin* est conçu pour que l'intérêt de ceux qui s'en occupent est qu'il fonctionne bien, et plus il prend de la valeur, plus les contrôles auxquels il est soumis sont nombreux.

– Les protocoles et programmes permettant de gérer les transactions peuvent évoluer, mais cela ne peut se faire que par vote, donc dans l'intérêt de tous.

Doutes, fragilités, risques des bitcoins

– L'anonymat de l'inventeur S. Nakamoto et les *bitcoins* qu'il a gagnés facilement aux débuts de la monnaie créent un sentiment désagréable et font craindre une machination.

– Aujourd'hui, les *bitcoins* sont tout petits à côté des autres monnaies : il y a environ un milliard de dollars en *bitcoins*, alors que circulent 1 200 milliards de dollars.

– La monnaie *bitcoin* repose sur des protocoles cryptographiques dont la robustesse n'est pas prouvée mathématiquement.

– Le système de gestion des *bitcoins* repose sur un ensemble de protocoles rendus opérationnels par des programmes. Des erreurs peuvent s'y trouver.

– Le *bitcoin* reste assez compliqué à comprendre et suscite donc la méfiance du plus grand nombre (qui ne saisit pas mieux la façon dont fonctionnent vraiment les monnaies classiques).

– Peu de sites et peu de commerçants acceptent les *bitcoins* aujourd'hui.

– Le *bitcoin* favorise le blanchiment d'argent sale, facilite les trafics en tous genres, et permet la fraude fiscale.

– Le *bitcoin* est déflationniste, ce que certains considèrent comme négatif, car cela constitue un frein à la circulation de l'argent ; surtout, son cours est très volatil du fait des incertitudes qui l'entourent.

– Le *bitcoin* pourrait faire l'objet d'interdictions ou de contrôles stricts imposés par des États voulant protéger leur propre monnaie. Le *bitcoin* pourrait être victime d'attaques menées par des agences, telle la NSA, qui tenteraient de briser toute confiance en lui, pour maintenir les monopoles monétaires actuels.

– L'anonymat y est imparfait.

– Le succès des *bitcoins* a inspiré toutes sortes d'autres Nakamoto et des dizaines de nouvelles cryptomonnaies copiées sur lui ont vu le jour tout récemment. Certaines, un peu différentes et encore mieux conçues, pourraient capter l'intérêt et faire se déplacer l'argent misé aujourd'hui sur les *bitcoins*.

– L'évolution possible des protocoles et programmes, prévue mais au fonctionnement délicat, conduit à la mise en place d'une forme d'administration centralisée constituée par l'ensemble des nœuds les plus puissants du réseau de contrôle. Cela ferait à terme ressembler le *bitcoin* aux monnaies usuelles dont S. <Nakamoto voulait se démarquer *(voir l'article de Joshua Kroll et al. en bibliographie)*.

de perturber gravement le fonctionnement du système *Bitcoin*. Avec l'accroissement des efforts investis dans l'extraction de *bitcoins*, il est de plus en plus difficile de réunir ces 50 pour cent, ce qui renforce indirectement la monnaie *bitcoin*. Le système conçu par S. Nakamoto se consolide au fur et à mesure que des gens s'y intéressent : plus le cours du *bitcoin* monte, plus il devient intéressant de chercher à extraire des *bitcoins* ; or plus ceux qui le font sont nombreux, plus le *bitcoin* devient robuste et donc plus son cours a des chances de monter.

La puissance globale consacrée aujourd'hui (le 26 octobre 2013) au minage de *bitcoins* est de 36 080 pétaflops *(voir http://bitcoinwatch.com/)* (1 pétaflops = 10^{15} opérations en virgule flottante par seconde). C'est plus de 1 000 fois la puissance du plus puissant ordinateur du monde (le *Tianhe-2* détenu par la Chine), qui ne fait que 33 pétaflops, et c'est largement plus que la puissance cumulée des 500 ordinateurs les plus puissants.

C'est considérable ! Ce qu'on peut voir comme un énorme gâchis de temps de calcul empirera si le *bitcoin* s'impose et que son cours (qui, bien sûr, détermine l'argent que les mineurs sont prêts à investir) progresse.

Aujourd'hui, en utilisant seulement son ordinateur pour « miner », on n'a aucune chance de gagner des *bitcoins*. Cette situation a conduit à la création de « guildes de mineurs ». Les mineurs associés décident de partager les gains qu'ils feront, en proportion de la puissance de calcul qu'ils consacrent. Ces regroupements assurent à chacun de gagner un peu, car la guilde (si elle est puissante) remportera assez fréquemment les 25 *bitcoins* qu'elle redistribuera à ses membres. Toutefois, ne vous faites pas d'illusion : en rejoignant une guilde, si vous n'offrez que la puissance de votre ordinateur personnel, la part qui vous reviendra sera minuscule.

Pas plus de 21 millions de *bitcoins*

Les protocoles de S. Nakamoto (qui sont traduits dans les programmes utilisés pour la gestion décentralisée de la monnaie *bitcoin*) prévoient que tous les quatre ans, la somme distribuée aux gagnants du minage est divisée par deux. Au début, elle était de 50 *bitcoins* ; le 22 novembre 2012, elle est passée à 25 *bitcoins*, et elle passera à 12,5 *bitcoins* dans trois ans. Du fait qu'un *bitcoin* ne peut être divisé en unités plus petites que le cent millionième de *bitcoin*, le gain attribué toutes les dix minutes finira par s'annuler. Un petit

L'AUTEUR

J.-P. DELAHAYE est professeur à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

BIBLIOGRAPHIE

P. Noizat, **Bitcoin : derrière la bulle, de vrais débats,** *Les Échos*, 23 août 2013 http://blogs.lesechos.fr/paristech-review/bitcoin-derriere-la-bulle-de-vrais-debats-a13320.html

S. Barber *et al.*, **Bitter to better, How to make Bitcoin a better currency**, *Proceedings of Financial Cryptography*, 2013.

D. Ron et A. Shamir, **Quantitative analysis of the full Bitcoin transaction graph**, *Proceedings of Financial Cryptography*, 2013.

J. Kroll *et al.*, **The Economics of bitcoin mining, or bitcoins in the presence of adversaries,** 12th Workshop on the economics of information security, 2013 : www.weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf

FBI Directorate of Intelligence, **Bitcoin virtual currency : Unique features present distinct challenges for deterring illicit activity**, 2012 : www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Satoshi Nakamoto, **Bitcoin : A peer-to-peer electronic cash system**, 2009 : http://bitcoin.org/bitcoin.pdf

Bitcoin Foundation : https://bitcoinfoundation.org

calcul montre que le processus d'émission de ces nouveaux *bitcoins* de récompense aura cessé en 2140 et qu'il y aura alors un total de 21 millions de *bitcoins*. À partir de cette date, aucun nouveau *bitcoin* ne sera plus jamais créé.

Afin d'éviter que tous les mineurs, essentiels au bon fonctionnement du protocole, désertent et que la construction et la validation continue du cahier de comptes cessent, S. Nakamoto a prévu qu'à chaque transaction, on donne une commission à celui qui ajoutera la page contenant la transaction au cahier. L'intérêt de miner sera donc préservé, même au-delà de 2140. Donner une telle commission n'est pas obligatoire et, aujourd'hui, même si vous ne laissez rien, vos transactions sont quand même validées et passent dans le cahier de comptes. Après 2140, il deviendra sans doute souhaitable de laisser un petit quelque chose à chaque transaction… On a le temps d'y penser.

L'impossible devenu réalité… et valeur

Le système mis en fonctionnement il y a quatre ans tient bien. Au début, le cours du *bitcoin* était dérisoire. Depuis un peu plus d'un an, il a monté pour atteindre 200 euros le 9 avril 2013. Il a ensuite chuté, puis est remonté à 100 euros. Certains ont réalisé d'excellentes affaires soit en achetant des *bitcoins* quand ils ne valaient rien, soit en les « minant » quand c'était facile. L'instabilité du cours fait qu'acheter des *bitcoins* est un pari. Cependant, à mesure que son usage se répandra et que des commerçants accepteront d'être payés en *bitcoins*, on peut espérer que le cours se calmera. Les avis sont partagés sur son devenir, mais l'intérêt qu'il suscite a de quoi rendre optimiste. Quelque chose d'important s'est produit avec la naissance de cette monnaie qu'une valorisation du total des *bitcoins* supérieure à un milliard d'euros a installé pour longtemps dans le monde réel. Une question se pose : pourquoi le *bitcoin* n'est-il pas apparu plus tôt ?

La réponse est simple : avant 2009, il était impossible d'envisager une telle monnaie qui doit son existence aux progrès récents dans plusieurs domaines.

a) Il fallait un réseau mondial fiable ; le *bitcoin* cesserait d'exister immédiatement en cas d'arrêt du réseau (il reprendrait à sa remise en marche).

b) Rien de possible non plus sans d'importantes puissances de calcul et de mémorisation informatique. C'est seulement récemment qu'elles sont devenues suffisantes pour que la tenue et la vérification des comptes, même en considérant toutes les transactions depuis la création de la monnaie, soient possibles quasi simultanément par des milliers d'acteurs indépendants. Ce modèle crée sans doute une confiance bien meilleure dans les comptes immatériels de cette monnaie que celle que l'on a dans ceux d'une banque qui s'occupe de gérer sa monnaie seule en faisant marcher la planche à billets de façon imprévisible et sans demander leur avis aux détenteurs de devises qui s'en trouvent pourtant lésés.

c) Le génie d'un informaticien (ou plusieurs ?) qui, en s'appuyant sur une cryptographie qui a formidablement progressé depuis 30 ans, a produit un protocole subtil et robuste que personne ne pensait possible, et qui a réussi à le faire fonctionner et décoller.

d) Essentielle aussi est la communauté des passionnés, un peu anarchistes, qui s'occupent des programmes et des réseaux pair-à-pair. Ils rendent l'utilisation pratique des *bitcoins* possible gratuitement par tous et évitent qu'un groupe, une banque ou un État ne s'empare de ce qui est au fond une monnaie commune, universelle et démocratique.

Ceux qui, à propos du *bitcoin*, parlent de pyramide de Ponzi ou de construction sur du vide pouvant s'écrouler du jour au lendemain n'ont rien compris à cette nouveauté remarquable, due aux mathématiques, aux avancées techniques et à l'ingéniosité de S. Nakamoto. Ils n'ont rien compris non plus aux monnaies qui reposent toutes sur la confiance (depuis l'abandon général de la convertibilité en or) et qui créent donc, comme le *bitcoin*, de la valeur à partir de rien. Le temps est peut-être venu aujourd'hui d'accorder sa confiance à des protocoles bien conçus, contrôlés par tous, plutôt qu'à des banques qui se moquent du reste du monde et qui, sans régulation collective, manipulent les monnaies aux dépens de (presque) tous. ■