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 : $M = B_{pub}\, N$.

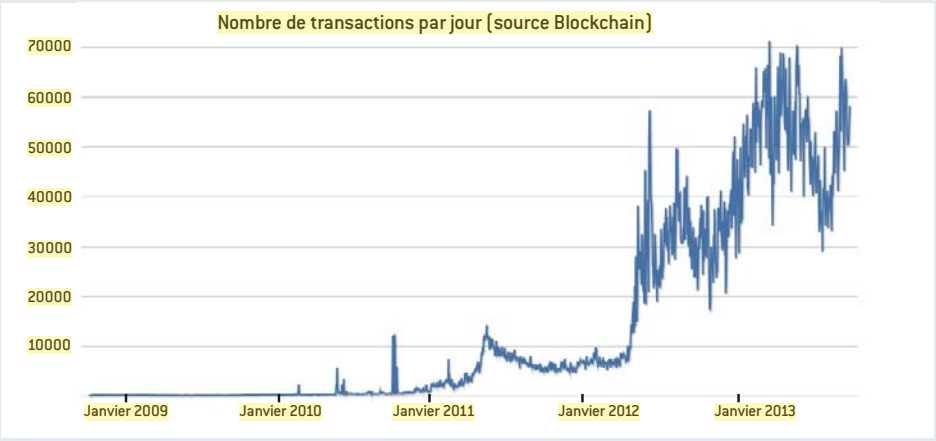
• Alice signe la transaction M avec sa clef privée A_{pri}, c'est-à-dire calcule une suite de symboles $M' = f(A_{pri}, M)$ qui, avec sa clef publique A_{pub}, redonne M : $g(A_{pub}, M') = M$ (tout le monde peut donc contrôler que c'est Alice qui a signé, mais personne ne peut signer à sa place).

• 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