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