Le *Bitcoin*, première crypto-monnaie

Jean-Paul Delahaye [1]

Conçu grâce aux progrès de la cryptographie et rendu possible par les réseaux pair à pair (P2P), le Bitcoin *fonctionne depuis 2009. Sa capitalisation dépasse aujourd'hui 5 milliards d'euros.*

Les États ont depuis toujours souhaité émettre et contrôler la monnaie. Les monnaies locales, privées et complémentaires sont peu utilisées et surveillées ; de plus elles dépendent toujours d'une autorité centrale. La cryptographie moderne qui propose des protocoles sûrs et réalisant des opérations qu'on pensait impossibles (comme les signatures digitales), et l'installation dans le monde entier des infrastructures permettant le fonctionnement quasiment sans failles d'un système de réseaux mondiaux, changent la donne. Une nouvelle forme de monnaie (le terme est discuté mais nous l'accepterons) semble possible : purement numérique, gérée collectivement sans intervention d'aucune autorité centrale, permettant des transferts sûrs, instantanés et d'un coût minime d'un point du globe à un autre, ce sont les *monnaies cryptographiques* ou *crypto-monnaies*. Après quelques essais inaboutis, la première version robuste de ce nouveau type de monnaie, le *Bitcoin* (dont la capitalisation représente aujourd'hui 92% de la capitalisation de toutes les monnaies cryptographiques) est né en 2009. Il suscite la passion, aussi bien de ses détracteurs que de ceux qui veulent y croire et qui ont entrepris de construire un secteur économique lié à son existence. Cela pourrait à terme changer profondément l'économie et même nos sociétés.

1. Université de Lille 1, Sciences et Technologies, Laboratoire d'Informatique Fondamentale de Lille, UMR 8022 CNRS, Bât M3-ext, 59655 Villeneuve d'Ascq Cedex. E-mail : delahaye@lifl.fr.

N'est-il pas remarquable que le total des devises sorties d'un protocole cryptographique réussisse l'exploit de valoir aujourd'hui l'équivalent de plusieurs milliards d'euros (plus de 5 milliards d'euros le 27 août 2014, voir `http://coinmarketcap.com/`).

Le *Bitcoin* est le résultat d'un subtil assemblage de protocoles cryptographiques élaborés fin 2008 et mis en œuvre le 3 janvier 2009 par un chercheur — ou peut-être plusieurs ? — caché sous le nom de Satoshi Nakamoto. Comprendre la logique de cette monnaie numérique et tenter de savoir si on peut s'y fier sera notre but. On va voir que le sujet est à la fois passionnant — du fait de l'originalité, du mystère et du succès et de cette construction mathématique et informatique — important — car il s'agit incontestablement d'un nouveau type de monnaie pouvant jouer un rôle central — et particulièrement délicat — personne aujourd'hui ne sait vraiment ce que ce montage numérique va devenir. Les avis les plus extrêmes s'expriment à son sujet [2].

Les monnaies électroniques ne sont pas une nouveauté et, d'une certaine façon, toutes les monnaies sont déjà électroniques. Il y a longtemps en effet que la totalité des opérations bancaires ne sont plus que des jeux d'écritures opérés dans les mémoires des ordinateurs. C'est important de le noter car 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 « bug », 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'est pas la porte ouverte à de colossales catastrophes financières. Si on s'en donne les moyens — ce qui est le cas car quand il s'agit d'argent, c'est sérieux –, on y arrive très bien. Les crises financières comme celle de 2009 n'ont pas pour origine le dysfonctionnement ou la fraude informatique, mais des erreurs commises par des humains qui se trompent dans leurs analyses économiques et financières ou sont trop voraces, voire malhonnêtes.

Autorité centrale

Aujourd'hui toute monnaie repose sur une autorité centrale : une banque avec, derrière, un État ou un ensemble d'États associés. C'est le cas aussi de tous les systèmes de pseudo-monnaies électroniques privées, dénommées monnaies complémentaires ou alternatives. Elles permettent des paiements par internet, 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 supérette inscrit sur votre compte à chaque passage aux caisses).

La caractéristique principale des *Bitcoins* est qu'à l'inverse, ils ont été conçus comme devant s'autoréguler sans autorité centrale. Le bon fonctionnement des échanges est garanti par une organisation générale que tout le monde peut examiner

2. voir le *Complément 7* à la fin de l'article.

car tout y est public : les protocoles de bases, les algorithmes cryptographiques utilisés, les programmes les rendant opérationnels et — c'est plus étonnant — 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 publicité totale des outils et du contenu des comptes n'empêche pas l'anonymat puisque les propriétaires des comptes ne sont pas tenus de se déclarer. C'est presque un paradoxe : tout mouvement de *Bitcoins* est public et pourtant le système produit un certain anonymat des détenteurs (dont il faut préciser qu'il est parfois imparfait).

Porte-monnaie virtuel

Posséder des *Bitcoins*, c'est connaître une suite de chiffres et de lettres qui constituent un compte. Une personne peut bien sûr posséder plusieurs comptes. Chaque compte comporte le montant en *Bitcoins* de l'argent qu'il contient, une clef publique qu'on peut laisser circuler (c'est le numéro de compte), et une clef privée qui doit absolument rester secrète car quiconque en dispose peut dépenser l'argent du compte.

Voici des numéros de compte :

1FxkfJQLJTXpW6QmxGT6oF43ZH959ns8Cq
13cia2KGVASavNmRs4niK5RSRfwkB1uLAu
1A6dpTWvoLWmTgwezLmyQti8oDUcLtjTKX

Voici aussi un exemple de clef secrète [3] :

E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6
1F 20 BD 67 FC 23 3A A3 32 62

Tout support est bon pour conserver la suite de symboles définissant votre compte, y compris un papier, une clef USB ou votre mémoire si vous le souhaitez et êtes capable de retenir les séries de chiffres et de lettres des numéros. Vous pouvez gérer vos comptes à l'aide d'un logiciel appelé « wallet » ou « porte-monnaie ». Vous pouvez aussi confier la gestion de vos comptes à un site internet de confiance, mais alors vous renoncerez à l'anonymat puisque le site en question aura besoin de savoir qui vous êtes. De plus — et c'est arrivé — les gestionnaires du site peuvent s'emparer de votre argent et disparaître avec ou se le faire voler. Le plus prudent sera donc peut-être de gérer soi-même ses comptes sur son ordinateur ou son smartphone. Les logiciels permettant cela, et plus généralement permettant le contrôle des *Bitcoins*, sont souvent développés dans le cadre de projets « open source » (licence MIT) : les programmes ne sont pas secrets et ceux qui le veulent contrôlent ce qu'ils font ou contribuent à leur amélioration. Aujourd'hui les logiciels permettant de gérer sur sa machine des comptes *Bitcoins* sont disponibles gratuitement (le

3. Le *Complément 1* explique ce que sont les *clefs privées* et *clefs publiques*, introduites en cryptographie il y a une quarantaine d'années.

plus souvent) pour tous les types de machines. Pour une liste de porte-monnaie, voir https://bitcoin.org/fr/choisir-votre-porte-monnaie.

Pour avoir des *Bitcoins* sur un compte, il faut qu'un détenteur de *Bitcoins* vous en ait donnés — par exemple en échange d'un bien. Autre possibilité : passer par une plateforme de change qui accepte de convertir des devises classiques (euros, dollars, etc.) en *Bitcoins* (il faut donner son identité).

Il existe aussi des machines distributeurs de *Bitcoins* (ATM-Bitcoin : Automated Teller Machine Bitcoin, voir http://en.wikipedia.org/wiki/Bitcoin_ATM). Vous entrez un ou plusieurs billets (en euros par exemple) dans la machine ; la machine envoie la somme convertie en *Bitcoins* (moins quelques frais) sur le compte *Bitcoin* que vous lui avez indiqué (par exemple en présentant le QRcode du numéro de compte à un lecteur optique). Quelques minutes plus tard vous pouvez vérifier que la somme a été ajoutée au compte en question. Une telle machine (que j'ai testée) se trouve à la *Maison du Bitcoin*, 35 rue du Caire à Paris.

Dernière possibilité pour avoir des *Bitcoins* : vous les gagnez en participant aux opérations de contrôle collectif de la monnaie appelé « minage ». On verra plus loin comment.

La gestion d'un compte doit être menée très soigneusement. Si vous effacez les clefs par mégarde, alors son contenu sera définitivement perdu, exactement comme quand vous lancez par-dessus bord une pièce de monnaie au milieu de l'océan. De nombreux *Bitcoins* ont ainsi déjà été perdus par des utilisateurs imprudents ou négligents. Il n'est pas impossible non plus qu'on vous vole vos *Bitcoins* en allant fouiller votre ordinateur et en y dénichant la clef secrète d'un de vos comptes : celui qui la connait peut dépenser le contenu du compte. Cela peut se produire à l'occasion de l'intrusion d'un hacker accédant aux données de votre machine par l'intermédiaire du réseau. Pour éviter cela, certains porte-monnaie contenant d'importantes sommes en *Bitcoins* sont gardés « au froid », c'est-à-dire sur des ordinateurs non connectés au réseau, ou même que l'on éteint. Sur ces questions consulter https://bitcoin.org/fr/securiser-porte-monnaie.

L'argent, c'est la mémoire

La cohérence des comptes — et donc la solidité de la monnaie *Bitcoin* — se fonde sur un principe général qui est l'application moderne de la théorie « Money is memory » de Narayana Kocherlakota (voir http://www.minneapolisfed.org/research/sr/sr218.pdf).

Ce principe général s'exprime ici sous la forme suivante :

— toutes les transactions faites depuis le début des *Bitcoins* le 3 janvier 2009 sont publiques, et donc, à chaque instant, la somme totale des *Bitcoins* émis est connue de tous, ainsi que le contenu de chaque compte qui en détient ;

— seul celui qui connaît la clef secrète d'un compte peut dépenser son contenu en envoyant tout ou une partie de celui-ci à un autre compte, cela publiquement sur le réseau à la vue de tous, ce qui permet à tous de connaître à chaque instant le contenu de chaque compte ;

— tous ceux qui le souhaitent participent au calcul général de la répartition des *Bitcoins* créés, cela à l'aide de logiciels — open-source et gratuits —, dont la correction et le comportement sont contrôlables par tous.

La cryptographie mathématique à clef publique n'est pas utilisée ici pour cacher de l'information, mais seulement pour signer les transactions, autrement dit, pour que personne ne puisse dépenser à votre place les *Bitcoins* qu'il y a sur vos comptes [4].

Une transaction est irréversible (sauf en cas d'accord explicite des deux contractants pour faire une transaction inverse). En effet, une fois que vous avez dépensé l'argent d'un compte, personne n'a l'autorité pour demander à celui qui a reçu l'argent de le rendre. Lui seul connaît la clef privée de son compte qui est nécessaire pour faire une dépense de l'argent du compte. 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 qu'elles ont été opérées, ce qui donne lieu à toutes sortes d'escroqueries. L'absence d'autorité centrale et l'anonymat des comptes ont cette conséquence dont il faut être conscient : l'échange est rapide et sans frais, mais une fois effectué, il sera impossible d'agir sur celui qui possède le compte ayant reçu vos *Bitcoins*... même s'il ne vous livre pas l'achat que vous pensiez régler.

Un système simplifié pour comprendre

Pour bien saisir l'idée des *Bitcoins* nous allons décrire un système simplifié des *Bitcoins*. Nous énumérerons ses défauts avant de voir comment il a été perfectionné par Satoshi Nakamoto pour aboutir au véritable protocole.

Le *système simplifié des Bitcoins* consiste en un *fichier de comptes* que tous les utilisateurs — dont la liste est fixée à l'avance et ne peut pas évoluer — calculent chacun de leur côté et mettent à jour en permanance, sur une feuille de papier, ou à l'aide de leur ordinateur. Ce *fichier de comptes* tenu à jour par tous les utilisateurs contient toutes les opérations de transfert (transactions) d'un compte vers un autre et permet donc de savoir quelles sommes sont présentes sur les comptes. Ce *fichier de comptes* pourrait ne conserver à chaque instant que l'information du solde de chaque compte, mais s'il contient l'historique des toutes les transactions, c'est plus précis et cela permet aussi le calcul du solde de chaque compte.

Les seules transactions possibles sont du type « le compte A verse la somme S au compte B ». Seul le détenteur du compte A peut enclencher une telle transaction. À chacune d'elles, tous les utilisateurs sont consultés, et donnent leur accord, après

4. Dans le *Complément 2* on explique le protocole d'une transaction.

avoir contrôlé en utilisant leur *fichier de comptes* que celui qui dépense l'argent, A, le possède bien. Une fois l'accord unanime obtenu, la transaction a lieu, ce qui signifie que chacun met son *fichier de comptes* à jour : le solde du compte A est diminué de la somme S, le solde du compte B est augmenté d'autant.

Ce système simplifié fonctionnerait très bien pour gérer une caisse entre une dizaine d'amis qui décideraient par exemple aussi que l'unité de compte de leur système vaut un euro. S'ils sont honnêtes et attentifs, ces amis seront toujours unanimes pour dire à chaque instant quelle somme se trouve sur chaque compte. Ils seront donc toujours d'accord pour valider les demandes honnêtes de dépense d'un compte vers un autre.

L'argent des comptes dans ce système simplifié serait purement virtuel : ce serait la mémoire que le *fichier de comptes* commun en a. Cette caisse permettrait par exemple aux dix amis de vivre ensemble dans un appartement en contribuant inégalement aux dépenses communes (faites avec de vrais euros), que le *fichier de comptes* rééquilibrerait. Quand Jean dépense 100 euros (véritables) pour les courses de l'appartement, ses 9 amis lui versent chacun 10 unités sur son compte. Au démarage des comptes, il n'y aurait pas besoin de faire le moindre versement, chacun se voyant attribuer par exemple 500 unités. Si les dix amis souhaitent mettre fin au système, ils rééquilibrent les comptes en faisant de vrais échanges entre eux. Une fois l'équilibre atteint, ils oublient la caisse et le *fichier de comptes*.

Transposer cela sur le réseau et à une échelle plus grande est difficile. Les échanges électroniques ne sont ni parfaits ni instantanés. Certaines parties d'un réseau sont parfois temporairement déconnectées du reste du réseau. De plus, tous les utilisateurs de *Bitcoins* ne souhaitent pas participer à la vérification continue des transactions et au re-calcul permanant du solde des comptes, car cela demande une puissance informatique non négligeable et beaucoup de mémoire. Faire l'hypothèse que personne ne voudra jamais tricher (par exemple en se retirant après avoir vidé son compte) est un peu naïf. Il est aussi très ennuyeux que la liste des utilisateurs du modèle simplifié soit fixée au départ et ne puisse pas évoluer. Il faut donc perfectionner le modèle simplifié pour l'adapter et lui donner plus de souplesse et de robustesse.

Insistons sur le fait que le *système simplifié des Bitcoins* réalise le plus simplement possible l'idée que « l'argent c'est la mémoire ». Admettre qu'il fonctionne parfaitement pour gérer une caisse entre une dizaine d'amis est le premier pas pour saisir précisément la nature du *Bitcoin*, et pourquoi cela fonctionne et ne constitue en rien une escroquerie. Les insuffisances du système simplifié ont contraint Satoshi Nakamoto à proposer un système plus compliqué, organisé autour d'une série de dispositifs cryptographiques, mais l'idée économique est celle de la caisse des dix amis, gérée par un *fichier de comptes* que chacun suit, opération après opération, en déplaçant des unités monétaires virtuelles.

Pannes, tricheurs, nouveaux arrivants

Bien des avantages résultent des perfectionnements de Nakamoto. En effet le système des *Bitcoins* mis en place en janvier 2009 possède les propriétés suivantes.

— Des nouveaux utilisateurs (comptes) peuvent s'introduire à chaque instant ou se retirer.

— Les utilisateurs ne sont pas tous contraints de suivre une à une les opérations faites d'un compte à un autre.

— Les opérations peuvent être plus complexes que le seul versement d'une somme S du compte A vers le compte B.

— Un change flottant de l'unité de compte (le *Bitcoin*) permet à sa valeur d'évoluer : aucune valeur n'est attribuée au départ au *Bitcoin* ; celle-ci s'établit progressivement, puis une fois adoptée, évolue en fonction de l'offre et de la demande.

— Les pannes de certaines machines du réseau, la coupure et même l'isolement de certaines parties du réseau, de longs délais de transmission entre nœuds du réseau, le désaccord de certains nœuds, les tentatives de tricheries — par exemple les doubles dépenses — n'auront pas d'effet sur le fonctionnement général du système.

Personne ne peut tricher, à la seule condition qu'un nombre minimum de participants acceptent de suivre le *fichier de comptes*.

Les améliorations faisant passer du *modèle simplifié* au *modèle réel du Bitcoin* se fondent sur une série de protocoles particuliers qui font la nouveauté du système des *Bitcoins* et qui aboutissent à un montage subtil et complexe — sinon il aurait été inventé bien avant ! — mais qui rend la monnaie *Bitcoin* résistante à toutes sortes de dysfonctionnements en même temps qu'à toutes sortes de tentatives de manipulation de la monnaie. La participation au contrôle ne sera menée que par les nœuds du réseau qui le souhaitent. Pour éviter que trop peu de nœuds du réseau participent au travail de contrôle un système de rémunération est prévu. Ce délicat agencement a étonné les spécialistes et prouve que l'auteur anonyme qui a conçu les *Bitcoins* est, très probablement, un cryptologue averti ou un groupe incluant au moins un cryptologue averti.

Il ne faut jamais oublier que cette monnaie ne tient que par *la cohérence et l'accord général et 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*. Il faut donc que la construction logicielle et cryptographique assure par elle-même que personne ne peut augmenter le total des *Bitcoins* détenus, ni modifier des comptes sans que tout le monde le découvre dans un délai très court. Il n'y a pas de police, la conception même de la monnaie doit empêcher seule la fraude et les dysfonctionnements.

Cela semble impossible et c'est pourquoi la construction conçue par Satoshi Nakamoto est parfois qualifiée de géniale. Personne avant lui n'avait imaginé un système robuste réalisant cette gestion infalsifiable d'un *fichier de comptes*. Le scepticisme sur la robustesse de la nouvelle monnaie, assez fort au départ, tend à s'atténuer. Le fait que la monnaie ait résisté plus de cinq ans malgré les attaques qu'elle a eu à subir est une preuve par l'expérience que le protocole tient. C'est l'une des explications de la valeur actuelle du *Bitcoin*.

Une page toutes les 10 minutes

L'idée pour l'amélioration du modèle simplifié consiste à gérer dans le cadre d'un réseau pair à pair (P2P) un *fichier de comptes* numérique (dont le nom technique est *Blockchain*) qui est complété progressivement par ajout de nouvelles *pages de transactions* (nommées *block*) toutes les 10 minutes environ. Cette *Blockchain* est le *fichier de comptes* du modèle simplifié. Il ne sera pas modifié à chaque opération, mais seulement toutes les 10 minutes.

Chaque ajout d'une page est validé par ceux qui participent à la gestion et à la surveillance décentralisée des comptes et qui détiennent chacun une copie de la *Blockchain*. Pour inciter à participer à la vérification, un concours se déroule en permanence. Une sorte de tirage au sort désigne toutes les dix minutes environ celui des participants qui ajoute la nouvelle page à la *Blockchain*, et qui est rémunéré pour cela par 25 *Bitcoins* créés ex nihilo. Lorsque la nouvelle page est ajoutée à la *Blockchain*, cela valide les transactions qui y apparaissent. La création de *Bitcoins* pour rémunérer le gagnant déterminé toutes les dix minutes est la seule création de *Bitcoins* possible. Tous les *Bitcoins* existants sont apparus de cette façon.

Lors d'une transaction en ma faveur, mon ordinateur connecté au réseau consulte la *Blockchain* qui est un fichier commun partagé par tous les nœuds vérificateurs du réseau P2P du *Bitcoin*. En consultant la *Blockchain*, mon ordinateur contrôle que le compte 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 la *Blockchain*, et donc pour être assuré de l'irréversibilité (par exemple avant d'envoyer le livre qu'on vient de vous acheter en vous faisant parvenir un paiement en *Bitcoins*), il faut attendre dix minutes et voir la transaction sur la nouvelle page du cahier. Les problèmes sont assez rares, et pour de petites transactions, on n'attend donc même pas les 10 minutes. La *Blockchain* peut être explorée à partir de `http://blockchain.info/fr`.

Dédoublement de la *Blockchain*

La possibilité d'ennuis sur le réseau et les délais de transmission des messages ont pour conséquence que parfois deux ajouts de pages à la *Blockchain* se feront

quasi-simultanément dans deux parties éloignées du réseau, créant temporairement un dédoublement de la *Blockchain*. 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 *Blockchains* continueront chacune de leur côté à se voir ajouter des pages toutes les 10 minutes environ. Le temps nécessaire à l'ajout est lié au processus de tirage au sort qui désigne le gagnant des 25 *Bitcoins* et donc les ajouts de pages aux deux *Blockchains* malencontreusement créées ne se feront pas à la même vitesse exactement. La *Blockchain* la plus longue (donc celle qui a été complétée de plusieurs nouvelles pages le plus rapidement) est considérée comme la bonne. Cette règle traduite dans les programmes conduit à l'élimination de l'autre *Blockchain* et donc à la reconstitution d'un état cohérent du système où ne persiste qu'une seule *Blockchain* et où d'éventuelles doubles dépenses sont impossibles.

Ces ennuis temporaires, rares mais inévitables, dans la gestion de la *Blockchain* ont pour conséquence au final que pour être certain qu'une transaction est définitivement valide — c'est important dans le cas de grosses sommes –, il faut non pas attendre dix minutes, mais plusieurs fois 10 minutes. On considère qu'une heure produit une garantie parfaite.

Une 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 que personne absolument ne peut connaître à l'avance). Ce tirage au sort se fait selon un procédé qui 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 [5]. 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 assez tentant puisque 25 *Bitcoins* s'échangent contre plus de 9000 euros (27 août 2014). 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 faire, le plus rapidement possible, les calculs demandés par le minage (les cartes graphiques disposent d'une puissance de calcul importante

5. Voir le *Complément 4* sur les *preuves de travail* qui explique la méthode cryptographique qui réalise cela.

qu'on peut détourner). Les cartes graphiques sont maintenant insuffisantes pour avoir de bonnes chances de gagner car au fur et à mesure que plus de mineurs se sont mis à jouer, il est devenu plus difficile de gagner. Le système de Nakamoto est conçu pour qu'il y ait un gagnant toutes les dix minutes environ et il s'ajuste automatiquement pour que ce temps moyen ne diminue pas. Des entreprises de hardware se sont donc mis à fabriquer des cartes et des machines spécialisées dont le seul but est de miner les *Bitcoins*. La puissance — et donc 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 rougir des microprocesseurs dédiés.

La puissance de calcul nécessaire pour gagner fait qu'il devient impossible même pour un acteur très puissant — et on sait qu'il y en a ! — de s'emparer de tous les gains. L'analyse générale du protocole des *Bitcoins*, effectuée dès 2008 par Nakamoto, montre précisément que si un acteur pouvait disposer de la moitié de la puissance consacrée au minage, alors il serait en mesure de perturber gravement le fonctionnement de la monnaie *Bitcoin*. L'accroissement des efforts faits pour miner des *Bitcoins* rend de plus en plus difficile de réunir ces 50%, et indirectement renforce donc la monnaie *Bitcoin*. Le système conçu par 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 miner des *Bitcoins*, plus nombreux sont ceux qui minent, plus le *Bitcoin* devient robuste y compris aux attaques d'acteurs très puissants, et donc, plus son cours a des chances de monter.

Vingt mille fois le plus puissant des ordinateurs

La puissance globale consacrée aujourd'hui au minage de *Bitcoins* est de 2 250 000 pétaflops (le 27 août 2014, voir `http://bitcoinwatch.com/` ; 1 pétaflops = 10^{15} opérations en virgule flottante). C'est plus de 20 000 fois la puissance du plus puissant ordinateur du monde (le « Tianhe-2 » détenu par la Chine qui espère atteindre en 2015 une puissance de 100 pétaflops) et c'est largement plus de cent fois la puissance cumulée des 500 ordinateurs les plus puissants.

C'est considérable ! Ce qu'on peut voir comme un énorme gâchis empirera si le *Bitcoin* s'impose et que son cours (qui bien sûr détermine l'argent que les mineurs sont prêts à investir) progresse. Les défenseurs du *Bitcoin* argumentent en disant qu'une monnaie basée sur l'or est aussi absurde que le *Bitcoin*. En effet on n'utilise pas l'or qui reste dans des coffres, qu'il faut surveiller. Même pour les monnaies usuelles comme l'euro ou le dollar, une quantité très importante de ressources est consacrée à leur création (conception et impression des billets) à leur transport, à leur surveillance (dans des coffres aussi), à la recherche des faussaires, etc.

Même si le minage des *Bitcoins* est utile à la consolidation de la monnaie *Bitcoin*, la chose apparaît parfois absurde car ces calculs menés pour augmenter les chances de gagner 25 *Bitcoins* n'ont aucune utilité directe. C'est sans doute pourquoi l'informaticien Sunny King a conçu un procédé pouvant se substituer à celui aujourd'hui utilisé pour miner les *Bitcoins*. Avec sa méthode, les calculs faits par les candidats produisent un tirage au sort équitable et infalsifiable, mais, en même temps, ils font découvrir des chaînes de nombres premiers intéressant les mathématiciens. King a mis en œuvre son idée en créant en juillet 2013 une nouvelle crypto-monnaie *Primecoin* concurrente des *Bitcoins* et qui a déjà conduit à découvrir des chaînes de nombres premiers record. La capitalisation de tous les *Primecoins* est, aujourd'hui (27 août 2014), d'environ un million d'euros. Le *Primecoin* arrive en position 26 par importance dans le classement (par capitalisation décroissante) des crypto-monnaies. Peut-être qu'on finira par imaginer encore mieux, et concevoir un protocole de minage qui — par exemple — aide aux calculs nécessaires pour déterminer le repliement des protéines, ce qui serait cette fois utile à la recherche médicale.

Aujourd'hui, en utilisant seul son ordinateur pour miner des *Bitcoins*, on n'a aucune chance de gagner des *Bitcoins*. Cette situation a conduit à la création de « coopératives de mineurs » (« *mining pool* »). Les mineurs associés décident de partager les gains qu'ils feront en proportion de la puissance de calcul qu'ils consacrent à miner. Ces regroupements assurent donc de gagner régulièrement, car la coopérative (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 coopérative, si vous n'offrez que la puissance de votre ordinateur personnel, la part qui vous reviendra sera minuscule et ne paiera sans doute même pas l'électricité que vous dépenserez pour faire tourner votre machine. Vous trouverez une liste de coopératives de minage en `http://www.bitcoin.fr/pages/Mining-pools`.

Vingt-et-un millions de *Bitcoins* en tout

Les protocoles de Nakamoto (qui sont fixés quasi définitivement et 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 départ, elle était de 50 *Bitcoins*, le 22 novembre 2012, elle est passée à 25 *Bitcoins*, et elle passera à 12,5 *Bitcoins* dans 2 ans. Du fait qu'un *Bitcoin* ne peut pas être divisé en unités plus petites que le cent millionième de *Bitcoin*, le gain toutes les dix minutes finira par arriver à 0. Un calcul montre que le processus d'émission de nouveaux *Bitcoins* 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.

De manière à éviter que tous les mineurs — essentiels au bon fonctionnement du protocole — désertent et que la construction et la validation continue de la *Blockchain* cesse, Nakamoto a prévu qu'à chaque transaction, on donne une commission à celui qui ajoutera la page contenant la transaction. 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 la *Blockchain*. Après 2140, il deviendra souhaitable de laisser un petit quelque chose à chaque transaction... on a le temps d'y penser. En fait dans certaines circonstances pour décourager les trop petites transactions qui encombreraient le système (et pourraient même le faire s'écrouler), laisser une commission — très minime — est déjà obligatoire : voir `http://bitcoinfees.com/` ou `https://en.bitcoin.it/wiki/Transaction_fees`.

L'impossible devenu réalité... et valeur

Le système mis en fonctionnement il y a bientôt cinq ans tient solidement. Dans un premier temps, le cours du *Bitcoin* était dérisoire. Il valait environ 10 euros en janvier 2013. Il a atteint 200 euros le 9 avril 2013. Il a ensuite chuté, puis en décembre 2013 le *Bitcoin* est monté jusqu'à près de 900 euros (voir `http://www.bitcoin.fr/pages/Cours-du-bitcoin`). Depuis il est revenu à 390 euros (le 27 août 2014). Certains ont fait d'excellentes affaires, soit en en achetant quand le *Bitcoin* ne valait rien, soit en minant les *Bitcoins* quand c'était facile. L'instabilité du cours fait qu'acheter des *Bitcoins* est un pari.

La page `http://www.bitcoin.fr/pages/Cours-du-bitcoin` indique clairement : « Bitcoin *est une expérience inédite. N'y investissez que ce que vous pouvez vous permettre de perdre.* »

Au fur et à mesure que son usage se répandra et que des commerçants accepteront d'être payé en *Bitcoins*, on peut espérer que le cours se calmera. Tout a été dit sur le *Bitcoin* et les avis sont partagés sur son devenir à long terme [6]. Il semble bien cependant que quelque chose d'important se soit produit avec la naissance de cette monnaie que quelques années d'existence et une valorisation du total des *Bitcoins* qui se compte en milliards d'euros ont installé pour longtemps dans le monde réel. Une question cependant doit être posée : pourquoi est-ce que cela ne s'est pas produit plus tôt ?

La réponse est assez simple : avant 2009, il était impossible d'envisager une telle monnaie qui doit son existence aux progrès récents dans plusieurs domaines et à leur association dans la construction de Nakamoto :

> (1) Il fallait un réseau mondial fiable ; sans lui rien ne serait possible ; le *Bitcoin* cesserait d'exister immédiatement en cas d'arrêt du réseau (il reprendrait à sa remise en marche).

6. Voir le *Complément 7*.

(2) Rien de possible non plus sans d'importantes puissances de calcul et de mémorisation informatique : la *Blockchain* fait 21 giga-octets (le 27 août 2014). Ce n'est que récemment — grâce à la loi de Moore — 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 simultanément par des milliers d'acteurs différents et indépendants se contrôlant donc les uns les autres.

(3) Le génie d'un (ou plusieurs ?) informaticien qui, en s'appuyant sur une discipline ayant formidablement progressé depuis trente ans — la cryptographie mathématique et informatique — a produit un protocole étonnamment subtil et robuste que personne n'imaginait possible, et qui a réussi à le faire fonctionner.

(4) Essentielle aussi est la communauté des passionnés qui s'occupe des programmes libres et des réseaux P2P rendant l'utilisation pratique des *Bitcoins* possible gratuitement par tous et évitant qu'un groupe, une banque ou un État ne s'empare de ce qui est parfois présenté comme une monnaie commune, universelle et démocratique.

Ceux qui, à propos du *Bitcoin*, parlent de pyramide de Ponzi ou de construction sur du vide susceptible de s'écrouler du jour au lendemain n'ont probablement rien compris à cette nouveauté remarquable, produit des mathématiques, des avancées techniques et de l'ingéniosité de Nakamoto. Ils n'ont peut-être rien compris non plus aux monnaies actuelles qui reposent toutes sur la confiance (depuis l'abandon général de la convertibilité en or) et donc sont — autant que le *Bitcoin* — de la création de valeur à partir de rien.

Plutôt que de continuer à faire reposer l'indispensable monnaie sur des institutions centralisées qui se sont cent fois révélées défaillantes, il serait peut-être plus rationnel de s'appuyer sur une organisation et un fonctionnement général de la monnaie fondés sur des protocoles cryptographiques reconnus, sur des logiciels que tout le monde peut examiner, et sur une transparence des comptes les rendant infalsifiables. Cela mérite au moins d'être discuté. Le *Bitcoin* pose une multitude de problèmes techniques, réglementaires, législatifs, fiscaux, policiers, et politiques. L'avenir du *Bitcoin* dépend de la façon dont ils seront traités et résolus. Sous la forme qu'il a aujourd'hui ou sous une autre forme (une autre crypto-monnaie), il est très probable qu'il continuera d'exister, et que ceux qu'il gêne et qui voudraient s'en débarrasser échoueront : on ne désinventera pas le *Bitcoin*.

Pour en savoir plus...

[1] James Angel and Douglas M. McCabe. *The Ethics of Payments : Paper, Plastic, or Bitcoin ?*, 2014.
http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2379233

[2] Jan Bergstra and Peter Weijland. *Bitcoin : a money-like informational commodity*. arXiv preprint arXiv :1402.4778, 2014.
http://arxiv.org/pdf/1402.4778.pdf

[3] Félix Brezo, Pablo G. Bringas. *Issues and Risks Associated with Cryptocurrencies such as Bitcoin*. SOTICS 2012 : The Second International Conference on Social Eco-Informatics.
http://www.thinkmind.org/index.php?view=article&articleid=sotics_2012_1_40_30101

[4] Nicolas Courtois, Marek Grajek, Rahul Naik. *The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining*, 2013.
http://arxiv.org/pdf/1310.7935v2.pdf

[5] Jean-Paul Delahaye. *Le* Bitcoin*, la cryptogmonnaie*. Pour la science, décembre 2013, pp. 86-91.
http://www.lifl.fr/~delahaye/pls/2013/241.pdf

[6] Jean-Paul Delahaye. *Les preuves de travail*. Pour la science, avril 2014, pp. 86-91.
http://www.lifl.fr/~delahaye/pls/2014/245.pdf

[7] Danielle Drainville. *An Analysis of the Bitcoin Electronic Cash System*. University of Waterloo 12-2012.
https://math.uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/Drainville,%20Danielle.pdf

[8] Ittay Eyal, Emin Gün Sirer. *Majority is not Enough.* arXiv preprint arXiv :1311.0243, 2013.
http://arxiv.org/pdf/1311.0243v5.pdf

[9] FBI Directorate of Intelligence Cyber Intelligence. *Bitcoin Virtual Currency : Unique Features Present Distinct Challenges for Deterring Illicit Activity*, 2012.
http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

[10] Stephen Goldfeder et al. *Securing Bitcoin wallets via threshold signatures*, 2014.
http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf

[11] Philippe Herlin. *La révolution du Bitcoin et des monnaies complémentaires*. Editions Eyrolles, 2013.

[12] Joshua Kroll, Ian Davey, Edward Felten. *The Economics of Bitcoin Mining, or Bitcoins in the Presence of Adversaries*. The Twelfth Workshop on the Economics of Information Security, 2013.
http://www.weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf

[13] William Luther. *Bitcoin is Memory*. Social Science Network, 2013.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730

[14] Satoshi Nakamoto. *Bitcoin : A Peer-to-Peer Electronic Cash System*, 2009.
http://bitcoin.org/bitcoin.pdf

[15] Michael Nielsen. *How the bitcoin protocol actually works*, 2013.
http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

[16] Mark Pinklinton. *Bitcoin and Complexity Theory : Some Methodological Implications*. Social Science Network, 2013.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2340007

[17] Fergal Reid, Martin Harrigan. *An analysis of Anonymity in the Bitcoin System*. Security and Privacy in Social Networks, 2013, pp 197-223.
http://arxiv.org/pdf/1107.4524.pdf

[18] Tetsuya Saito. *Bitcoin a Search Theoretic Approach*. Research Institute of Economic Science College of Economics, Nihon University, 2013.
http://www.eco.nihon-u.ac.jp/center/economic/publication/pdf/13-01.pdf

[19] Bitcoin Foundation (consulté en août 2014).
https://bitcoinfoundation.org

[20] Sites des développeurs principaux du Bitcoin (consulté en août 2014).
https://bitcoin.org/en/ouhttps://bitcoin.org/fr/

[21] Wikipedia, Bitcoin (consulté en août 2014).
http://en.wikipedia.org/wiki/Bitcoin ou http://fr.wikipedia.org/wiki/Bitcoin

[22] Bitcoin wiki (consulté en août 2014).
https://en.bitcoin.it/wiki/Main_Page

[23] La Blockchain (consulté en août 2014).
http://blockchain.info/

Complément 1

La signature par cryptographie à double clef

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.

Supposons par exemple qu'Alice dispose de deux clefs A_{pri} (clef privée) et A_{pub} (clef publique). Ce sont des suites de symboles ou, ce qui revient au même, des nombres entiers.

La clef A_{pub} est transmise à tout le monde, mais la clef A_{pri} n'est connue que par Alice. Si le protocole de signature à double clef est bon, il est impossible en pratique de déduire A_{pri} à partir de A_{pub}.

Les deux fonctions f et g servent à signer un message et à lire la signature.
Exemple. 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 sans peine 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 produira M :

$$g(A_{pub}, M') = M.$$

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 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 que Alice a bien signé M avec sa clef privée.

Il existe de nombreuses façons de choisir les fonctions f et g. Celle qui sert pour la monnaie *Bitcoin* est basée sur la cryptographie à courbes elliptiques, dite ECDSA (*Elliptic Curve Digital Signature Algorithm*). La courbe employée est **secp256k1**. Une autre solution aurait pu être le RSA (Rivest-Shamir-Adleman), plus connu mais demandant des clefs plus longues.

Et si le protocole de signature du Bitcoin *était cassé ?*

Si le protocole de signature venait à être cassé et que quelqu'un disposant d'une clef publique A_{pub} sache calculer facilement la clef privée associée A_{pri}, alors cette personne serait en mesure de dépenser le contenu de tous les comptes. À condition de le faire progressivement pour ne pas se faire repérer, cette personne serait donc très riche ! Les détenteurs des comptes ne s'en apercevraient que lorsque, consultant la somme liée à leur compte (et donc allant lire la *Blockchain*), ils découvriraient que leur compte est vide.

Notons bien que ce vidage des comptes (par quelqu'un sachant calculer A_{pri} à partir de A_{pub}) peut s'opérer même si le porte-monnaie est sur un disque dur déconnecté du réseau et éteint, ou même si la clef privée du porte-monnaie n'est écrite que sur une feuille de papier, ou même si elle est perdue.

On considère cependant que personne ne disposera jamais du moyen pratique de calculer A_{pri} à partir de A_{pub}, ou que si cela se produit, la faiblesse du protocole de signature aura été repérée avant qu'elle soit devenue réellement utilisable, et donc, que la communauté des développeurs *Bitcoin* aura opéré à temps le changement de cette partie du protocole *Bitcoin*. La possibilité d'adapter et donc de corriger des faiblesses qu'on repèrerait dans le protocole *Bitcoin* est prévue dans le protocole *Bitcoin*. Mais cette éventuelle réparation d'une défaillance du protocole de signature n'est envisageable que si on s'en aperçoit...

On peut même imaginer que si des vidages de comptes étaient opérés en trop grand nombre, la communauté *Bitcoin* arrêterait toutes les transactions et tenterait de réparer le protocole et de rétablir les comptes dans un état antérieur à la détection de la fraude. De telles situations obligeant à une intervention des équipes de développement du *Bitcoin* se sont déjà produites deux fois. Une première fois, en août 2010, à la suite de la découverte d'un bug qui avait permis la création de 184 millions de *Bitcoins* frauduleux qui furent immédiatement annulés. Une seconde fois en mars 2013, à la suite d'une duplication de la *Blockchain* (voir `http://en.wikipedia.org/wiki/History_of_Bitcoin`). Au total, même dans les cas extrêmes de mise en cause du protocole *Bitcoin*, il est donc possible d'en limiter les conséquences et donc d'éviter l'écroulement total du système. Notons que lors de ces rares événements, le principe de décentralisation du *Bitcoin* cesse temporairement d'être respecté, et qu'une équipe restreinte de développeurs reprend la main et

opère des choix qui ne sont pas inscrits d'avance dans le protocole. Ces choix sont faits publiquement et à la suite d'accords entre les développeurs, mais — temporairement et pour sauver le *Bitcoin* de catastrophes graves — il s'agit quand même d'écarts inquiétants à la doctrine de base.

Complément 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'opérations. Ces opérations sont gérées automatiquement par le logiciel qu'ils ont installé sur leur ordinateur. Les communications sur le réseau *Bitcoin* se font directement. Ce *réseau* pair à pair ou P2P (peer-to-peer) est le cœur du système. L'existence de tels réseaux est essentielle pour la monnaie *Bitcoin* qui n'est gérée par aucun nœud central qui contrôlerait l'ensemble des communications. La transaction qui résulte des échanges entre Alice et Bernard est publique (tous les ordinateurs présents sur le réseau y auront accès) et permet la mise à jour par tous de la *Blockchain* qui indique combien de *Bitcoins* sont déposés dans chaque compte existant.

(1) Alice souhaite envoyer N *Bitcoins* à Bernard.

(2) Bernard communique sa clef publique B_{pub} (c'est-à-dire son numéro de compte) à Alice.

(3) Alice constitue un message M de transaction contenant la clé publique de Bernard B_{pub} et la somme N à transférer : $M = B_{pub}N$.

(4) Alice signe la transaction M avec sa clé privée, c'est-à-dire calcule une suite de symboles $M' = f(A_{pri}, M)$ qui, avec sa clef publique, redonne M :

$$g(A_{pub}, f(A_{pri}, M)) = g(A_{pub}, M') = M.$$

Tout le monde peut donc contrôler que c'est Alice qui a signé, mais personne ne peut signer à sa place.

(5) 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 qu'Alice a donné son accord pour transférer N *Bitcoins* à Bernard.

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 donc le transfert comme valide.

Complément 3

LE HACHAGE ET LES PREUVES DE TRAVAIL

Une fonction de hachage est une fonction h qui à toute suite de symboles S (par exemple des chiffres) associe une autre suite de symboles (plus courte) $h(S) = R$ et surtout qui est telle qu'il est impossible en pratique pour une valeur possible R de la fonction h de trouver un S tel que $h(S) = R$. Si h est une bonne fonction de hachage les valeurs $h(S)$ produites par quelqu'un qui essaie diverses valeurs pour S, sont aussi imprévisibles que si elles étaient tirées au hasard avec une roue de loterie.

Disposant d'une telle fonction h on peut définir un *travail* qu'il sera impossible de faire rapidement :

Travail de niveau k : Trouver S tel que $h(S)$ commence par k fois le symbole '0'.

Plus k est grand, plus il faut essayer de nombreux S avant de trouver un S convenable. En moyenne, ceux qui prétendent avoir trouvé un tel S ont fourni un travail de calcul qui est d'autant plus important que k est grand.

C'est un peu comme si on demandait à quelqu'un de lancer deux dés jusqu'à obtenir un double 6 (il faudrait en moyenne qu'il les lance 36 fois pour réussir).

On vérifiera facilement que les S prétendument trouvés sont bons, en en demandant la communication, et en calculant $h(S)$ qui doit être un résultat avec k '0' en tête.

L'idée de ces « preuves de travail » a été proposée en cryptographie dans le but par exemple de lutter contre le courrier électronique indésirable (spam) : si chaque ordinateur qui veut accéder à ma boîte de messages doit prouver qu'il a effectué un certain travail dépendant de ma boîte (par exemple trouver un S tel que $h(S)$ commence par 10 fois '0' pour une fonction h qui m'est propre), il devient impossible à celui qui le voudrait d'envoyer de milliers de spam, car la preuve de travail nécessaire à chaque envoi devient trop lourde au total. Cette barrière à l'entrée d'une boîte à lettres électronique n'est pas ennuyeuse pour celui qui ne veut envoyer que quelques messages, car la preuve de travail à fournir est raisonnable si le nombre d'envois est petit. À ma connaissance, cette méthode n'est pas encore utilisée pour lutter contre le spam.

La technique de la *preuve de travail* est au cœur du système des *Bitcoins*. C'est elle qui est utilisée pour le tirage au sort de celui qui ajoute une page à la *Blockchain* et remporte, toutes les dix minutes, 25 nouveaux *Bitcoins*. Tous ceux qui participent se lancent dans la recherche du S, le premier qui en trouve un est le gagnant. Un paramètre contextuel dans la définition de h, connu seulement au moment où un nouveau tirage est lancé, empêche les participants de commencer à chercher le S en avance.

Ajustables en faisant varier l'entier k, les *preuves de travail* exigées pour emporter les 25 *Bitcoins* créés toutes les 10 minutes sont devenues de plus en plus difficiles au cours des mois. Depuis que des puces spécialisées ont été conçues pour calculer très vite les $h(S)$ la difficulté du travail demandé a été augmentée, cela de façon à ce que le temps moyen entre deux gains reste toujours de 10 minutes environ. Cette augmentation de la difficulté des *preuves de travail* est conforme au protocole fixé par Nakamoto, le concepteur des *Bitcoins*.

Pour un article général sur les preuves de travail, voir Jean-Paul Delahaye, *Les preuves de travail*, Pour la science, avril 2014, pp. 86-91, `http://www.lifl.fr/~delahaye/pls/2014/245.pdf`.

Complément 4

Les cours, la capitalisation, les « bulles »

La première page de la *Blockchain Bitcoin* a été publiée le 3 janvier 2009.

Les *Bitcoins* sont émis à un rythme régulier :

— 50 *Bitcoins* nouveaux ont été créés toutes les 10 minutes, jusqu'au 22 novembre 2012.

— Depuis, 25 nouveaux *Bitcoins* sont créés toutes les 10 minutes.

— Le nombre de *Bitcoins* émis sera divisé par 2 tous les quatre ans.

— Le total des *Bitcoins* émis ne dépassera jamais 21 millions.

Aujourd'hui (26 août 2014, 9h20) le nombre de *Bitcoins* émis est 13 188 050. Ils valent exactement 5 002 201 euros (pour une mise à jour, aller en `http://bitcoinwatch.com/`).

Le 9 février 2011 : Le *Bitcoin* a atteint la parité avec le dollar.

Le 11 avril 2013 : Effondrement de la valeur du *Bitcoin* qui passe de 266 $ à 105 $ et descend même brièvement à 60 $.

En décembre 2013, il atteint 1147 $ (900 euros). Depuis, il est redescendu et vaut 504 $ (27 août 2014).

La taille de la *Blockchain* est 21 gigaoctets (27 août 2014).

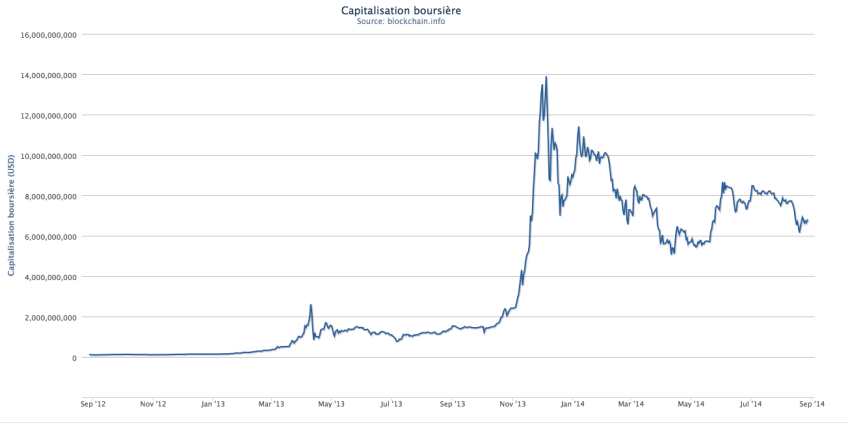

FIGURE 1. Capitalisation boursière jusqu'au 27 août 2014

D'autres informations et graphiques sur la monnaie *Bitcoin* sont mis à jour en continu en :

`https://blockchain.info/fr/charts` (voir Figure 1)
`http://bitcoinwatch.com/`
`http://www.quandl.com/markets/bitcoin`
`http://www.bitcoin.fr/pages/Cours-du-bitcoin`
`http://www.coindesk.com/price/`
`http://coinmarketcap.com/` (Capitalisation de toutes les crypto-monnaies)

Les cinq « bulles » du Bitcoin.

Les montées brusques du cours du *Bitcoin*, suivies de baisses, elles-aussi violentes, ne sont pas un phénomène nouveau comme le croient certains observateurs des récentes variations. En examinant ce cours depuis 2010 (voir Figure 2), on observe que c'est en réalité la cinquième « bulle » qui gonfle et éclate (partiellement).

Ces « bulles » doivent-elles vraiment être appelées des « bulles » puisqu'à chaque fois le cours finit par se stabiliser au-dessus de sa valeur d'avant la « bulle » ?

En 2010, on passe de moins d'un dixième de dollars à plus d'un dollar.
En 2011, on passe d'un dollar à 5 dollars.
En 2012, on passe de 5 dollars à 10 dollars.
Au premier semestre 2013 on passe de 10 dollars à 100 dollars.
Au second semestre 2013, on passe de 100 dollars à plus de 400 dollars.

Parler de « bulles qui éclatent » est étrange : si vous êtes pris dans le gonflement et détenez des *Bitcoins* alors, en vendant après l'éclatement, vous réalisez une excellente affaire. Personne ne regrettera d'avoir acheté à 10 si, quelques mois après, il

FIGURE 2. Les cinq « bulles » du *Bitcoin*

dispose de 100, et cela même s'il a manqué de vendre à 200 ! Il semblerait plus sage de parler de « bouffées de volatilité », car à part des pics temporaires (sans doute excessifs) qui font à l'arrivée quand même monter le cours, il n'y a jamais eu à proprement parler d'éclatement de bulle ! Bien sûr, cela peut venir, et le cours du *Bitcoin* pourrait retomber à moins d'un dollar comme l'annoncent certains.

Complément 5

LA NAISSANCE DU *Bitcoin*

Le *Bitcoin* a été défini en 2008 par un personnage qui se présente sous le nom de Satoshi Nakamoto et qui a écrit avoir travaillé deux ans à la conception de sa monnaie. Nakamoto garde l'anonymat. Il se peut qu'il s'agisse en fait d'un groupe de plusieurs personnes, mais vue la façon dont le protocole qui gère la nouvelle monnaie numérique a été fixé, il est certain que Nakamoto possède des connaissances de très bon niveau en cryptographie. Une sorte de grande traque se déroule sur internet pour identifier qui est le génial inventeur. 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.

Récemment des arguments assez forts semblent désigner Nick Szabo de l'Université George Washington à Washington D.C. aux États-Unis. Voir :

http://techcrunch.com/2013/12/05/who-is-the-real-satoshi-nakamoto-one-researcher-may-have-found-the-answer/

https://likeinamirror.wordpress.com/2013/12/01/satoshi-nakamoto-is-probably-nick-szabo/

http://www.coindesk.com/linguistic-researchers-name-nick-szabo-author-bitcoin-whitepaper/

L'anonymat des utilisateurs des *Bitcoins* est assuré par le fait que seuls les numéros de compte et les contenus des comptes sont nécessaires au maintien de la cohérence de la *Blockchain*. La clef privée d'un compte assure son propriétaire que lui seul pourra dépenser l'argent qui s'y trouve et donc, en théorie, l'anonymat des détenteurs de comptes est assuré. La réalité est plus complexe et l'anonymat n'est pas absolu. D'une part, on peut suivre le déplacement des *Bitcoins* d'un compte à l'autre et de cette façon en déduire certaines 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, en étudiant la *Blockchain* concluent que Nakamoto possède probablement l'équivalent de 10% 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 limités qu'on réussit plus ou moins à suivre. L'invention des *Bitcoins* aurait donc permis à Nakamoto de se constituer une belle fortune de l'ordre de 500 millions d'Euros (somme à réévaluer en fonction du cours). Il lui sera sans doute difficile de les remettre sur le marché sans dévoiler son identité (et sans faire baisser les cours)... à moins qu'il procède lentement et qu'il imagine et mette en œuvre des techniques de brouillage faisant perdre sa trace, comme il s'en développe. Voir par exemple :

http://app.bitlaundry.com/

http://bittumble.com/

https://en.bitcoin.it/wiki/Category:Mixing_Services

https://en.bitcoin.it/wiki/Mixing_service

Complément 6

LE PLUS ET LE MOINS DU *Bitcoin*

***Nouveautés, forces et qualités des* Bitcoins**

— La monnaie *Bitcoins* est basée sur un réseau pair à pair et des logiciels libres et gratuits. Elle est indépendante de toute banque, n'est soumise à aucune autorité centralisée et offre une transparence sans équivalent dans toute l'histoire des monnaies.

— Les transactions de *Bitcoins* sont rapides et irréversibles. Personne ne peut agir sur les *Bitcoins* de vos comptes sans votre consentement (sauf s'il en connaît la clef privée).

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

— Le nombre de *Bitcoins* est rigoureusement fixé et 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 par ce moyen indirect capte une part de votre argent par l'inflation créée.

— Anonymat : le réseau fonctionne à partir de comptes. Posséder un compte, c'est connaître la clef privée qui lui est associée. L'identité des utilisateurs n'est utile à aucun moment. (L'anonymat n'est cependant pas total : voir le Complément précédent.)

— Un *Bitcoin* peut être divisé en fractions de *Bitcoin* jusqu'au 1/100 000 000.

— Le *Bitcoin* (à cause du nombre maximum de *Bitcoins* en circulation) est sans doute intrinsèquement déflationniste : il est amené à prendre petit à petit de la valeur. Non seulement vos économies ne sont pas rongées par l'inflation, mais elles s'apprécient.... à moins que vous ne perdiez tout parce que le protocole *Bitcoin* s'effondre !

— Le *Bitcoin* a été conçu d'une manière telle que l'intérêt de ceux qui s'en occupent est qu'il fonctionne bien. Du fait de sa conception, plus il prend de la valeur plus les contrôles auxquels il est soumis sont nombreux.

— Les protocoles et programmes permettant la gestion des transactions peuvent évoluer, mais cela ne peut se faire que lentement, par une sorte de vote de la communauté, et donc en respectant l'intérêt commun.

Doutes, fragilités et risques des **Bitcoins**

— L'anonymat de Nakamoto « l'inventeur » des *Bitcoins* et l'argent qu'il a gagné facilement au départ de la monnaie créent un sentiment désagréable et font craindre une combine. Certains ont même imaginé que le *Bitcoin* est une création de la NSA.
— Aujourd'hui le *Bitcoin* est économiquement très petit à côté des autres monnaies internationales auxquelles il ne peut donc pas prétendre se substituer : il y a quelques milliards de dollars en *Bitcoins*, alors que la devise américaine par exemple a été émise à hauteur de 1 200 milliards (uniquement en billets).
— La monnaie *Bitcoin* repose sur des protocoles cryptographiques dont la robustesse n'est pas prouvée mathématiquement. Il faut faire confiance à la science cryptographique d'aujourd'hui et à son état de l'art.
— Le système de gestion des *Bitcoins* repose sur un ensemble de protocoles qui ont été 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 peut-être pas mieux la façon dont fonctionne les monnaies classiques !).
— Relativement peu de sites et peu de commerçants acceptent les *Bitcoins* aujourd'hui.
— Le *Bitcoin* (comme l'argent liquide) favorise le blanchiment d'argent sale, facilite les trafics en tout genre, et permet la fraude fiscale.
— Le *Bitcoin* semble intrinsèquement déflationniste ce que certains considèrent comme négatif car cela constitue un frein à la circulation de l'argent, et surtout, les cours du *Bitcoin* sont très volatils du fait des incertitudes qui l'entourent.
— Le *Bitcoin* pourrait être l'objet d'interdictions ou de contrôles stricts imposés par des États voulant protéger leurs propres monnaies. Il n'est pas impossible que le *Bitcoin* soit victime d'attaques menées par des agences comme la NSA qui tenteraient de briser toute confiance en lui, pour maintenir les monopoles monétaires actuels.
— L'anonymat y est imparfait (du fait que toutes les transactions sont publiques).
— Le succès des *Bitcoins* a inspiré toutes sortes de Nakamoto et des dizaines de nouvelles crypto-monnaies directement copiées sur lui ont vu le jour. Bien qu'aujourd'hui le total des autres crypto-monnaies représente moins de 10% du *Bitcoin*, certaines crypto-monnaies un peu différentes et 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 collectif de contrôle. Cela pourrait conduire à terme à faire ressembler le *Bitcoin* aux monnaies usuelles dont Nakamoto voulait se démarquer [7].

Complément 7

QUELQUES AVIS TRANCHÉS

Contre

`http://www.gaullistelibre.com/2013/05/bitcoin-ou-la-folie-de-la-monnaie.html`

• 14 mai 2013, Laurent Pinsole (Blogueur, militant dans le mouvement « Debout la République ») :

Bien sûr, les plus libéraux des libéraux s'enthousiasmeront de cette expérimentation du marché, sans la contrainte étatique. Mais sur le fond, ces monnaies virtuelles posent des problèmes qui justifient largement leur interdiction. Tout d'abord, leur conception, garantissant parfois un anonymat complet, peut permettre le recyclage d'argent sale. Ensuite, il s'agit d'un flux monétaire sur lequel l'État a moins de maîtrise, ce qui peut faciliter la désertion fiscale des entreprises qui les utilisent.

Mais surtout, la monnaie est un pilier des sociétés modernes, à la fois unité nécessaire à l'échange, mais aussi unité de compte qui permet l'épargne ou le prêt. En cela, il est difficile de ne pas comprendre qu'il s'agit d'un service public, qui relève éminemment de l'État pour garantir la valeur de cette monnaie. Confier cela au marché aboutit précisément aux errements constatés avec Bitcoin, à savoir une variation totalement erratique de sa valeur, qui peut faire du mal aux citoyens.

En outre, l'exemple de Bitcoin amène à se poser la question de qui profite de la création de ces monnaies virtuelles. En effet, les dix millions d'unités créées ne sont pas gagées sur quoi que ce soit. Du coup, il faut reconnaître que quelqu'un profite de la création ex nihilo de ces monnaies et l'absence de régulation en ce domaine pose également problème. Bref, rien ne justifie que de la monnaie soit créée de la sorte par des entreprises privées. C'est l'État qui doit gérer la monnaie.

7. Sur ce point voir : Joshua Kroll, Ian Davey, Edward Felten, *The Economics of Bitcoin Mining*, ou *Bitcoins in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security, 2013.

L'expérience Bitcoin montre à nouveau tous les dangers du « laisser-faire » en matière monétaire. Non seulement, les marchés seuls sont incapables d'assurer la stabilité nécessaire à la monnaie, mais les bénéfices de la création de la monnaie doivent rester dans le giron public.

---

http://www.atlantico.fr/decryptage/et-folle-envolee-bitcoin-annoncait-en-realite-disparition-prochaine-benoist-rousseau-903206.html

• 20 novembre 2013, Benoist Rousseau (Ingénieur, Informaticien et historien économiste) :

Cette monnaie virtuelle est aujourd'hui trop instable, ces phases de hausses extrêmes font aussi place à des krachs réguliers, en avril 2013 le Bitcoin a ainsi perdu 60% de sa valeur en moins de 5 jours. Qui accepterait aujourd'hui d'être payé en Bitcoins avec de telles fluctuations ? Le Bitcoin est actuellement en train de devenir un simple instrument spéculatif qui n'est pas sans rappeler le début d'une formation d'une bulle que l'on retrouve dans de nombreux krachs boursiers.

[...] L'envolée récente des cours au mois de novembre 2013 est une réponse en miroir à l'effondrement du Bitcoin du mois d'octobre 2013. On parlait alors de la fin du Bitcoin... Du fait du faible nombre de Bitcoins en circulation, il est très aisé pour une structure organisée disposant de capitaux importants de faire fluctuer le cours comme elle le souhaite. C'est une monnaie « casino » actuellement.

[...] Du fait de la faiblesse du volume des transactions, le Bitcoin doit « appartenir » en fait à quelques personnes fortement capitalisées qui peuvent « jouer » avec lui. Cette monnaie « libre » est sûrement l'une des plus manipulables et des moins libres paradoxalement... Quelques organisations douteuses peuvent se comporter comme les banques centrales sur cet actif et faire la pluie et le beau temps, le prix à payer pour l'utopie d'une dérégulation totale... Ce ne sont plus les États qui peuvent garantir un jeu basé sur des règles établies et connues de tous afin d'éviter les ententes, les délits d'initiés... mais les plus forts qui agissent comme ils l'entendent sur les cours du Bitcoin, sans limite, sans règle. Faut-il préférer les mafias ou les banques centrales ? Quant à savoir quand cette bulle éclatera, personne ne le sait, c'est le principe des bulles, tout le monde la voit mais personne ne sait quand. L'envolée récente peut être vue comme une tentative de sauvetage du Bitcoin après son effondrement d'octobre. Dans un marché si étroit, les variations sont toujours excessives, à la hausse comme à la baisse.

---

http://finance.blog.lemonde.fr/2013/11/20/le-bitcoin-est-une-monnaie-de-casino-qui-profite-a-des-manipulateurs-incontroles/

• 4 décembre 2013, Georges Ugeux (Banquier d'Affaires) :

Le Bitcoin est une « monnaie » de casino qui profite à des manipulateurs incontrôlés.

Je n'ai aucune opinion sur le souhait de ceux et celles qui s'adonnent au jeu, et utilisent la monnaie des casinos. Après tout, le jeu est aussi vieux que le monde. Mon problème est quand les fondateurs de Bitcoin prétendent que c'est une monnaie légitime. Cette semaine a été une brillante démonstration de l'incompétence des politiciens et de la stupidité moutonnière des marchés. Depuis les tulipes hollandaises, nous savons que les modes sont un phénomène régulier dans les marchés. Le tout, c'est de s'en sortir à temps.

Lorsque le château de cartes s'effondrera, qui seront les victimes ? Ceux et celles qui, inconscients du danger, se retrouveront avec des jetons de 900 dollars et découvriront qu'ils ne valent plus rien. C'est là que se trouve la légitimité d'une intervention sérieuse et musclée du législateur. La « Fondation Bitcoin » comporte plus de 100 membres permanents et le même nombre de membres annuels. Ils standardisent, promeuvent et protègent le Bitcoin. Inutile de dire qu'ils n'assument aucune responsabilité quelconque sur la valeur ou les actifs. La « fondation » fait du marketing, et ses membres n'apportent de crédibilité que par leur nombre.

`http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf`

• 5 décembre 2013, La Banque de France (Focus n°10) :

Les bitcoins : une monnaie non régulée qui n'offre aucune garantie.

[...] Une conception qui alimente la spéculation.

[...] Des plates-formes internet proposent, sans aucune garantie de prix ni de liquidité, l'achat/vente de bitcoins contre des devises ayant cours légal.

[...] Par son caractère anonyme, le bitcoin favorise le contournement des règles relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

[...] Même si le bitcoin ne remplit pas à ce jour les conditions pour devenir un support d'investissement crédible et poser ainsi un risque significatif pour la stabilité financière, il représente un risque financier certain pour les acteurs qui le détiennent.

[...] N'offrant aucune garantie de sécurité, de convertibilité et de valeur, le bitcoin présente peu ou pas d'intérêt pour une utilisation par les acteurs économiques, au-delà des aspects marketing et publicitaire, tout en les exposant à des risques importants.

[...] En limitant la quantité maximale de bitcoins pouvant être créée et en faisant fluctuer le rythme de création au cours du temps, les concepteurs ont « organisé » la pénurie de cette monnaie virtuelle et lui ont ainsi conféré son caractère hautement spéculatif.

---

http://wallstreetpit.com/101867-greenspan-i-guess-bitcoin-is-a-bubble/
http://www.businessinsider.com/alan-greenspan-bitcoin-comment-reaction-2013-12

• 5 décembre 2013, Alan Greenspan (Économiste, ancien président de la Réserve Fédérale, la Banque centrale des États-Unis) :

I guess Bitcoin is a bubble.

You really have to stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. But if you ask me, "Is this a bubble in Bitcoin ?" "Yeah, it's a bubble".

---

http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/this-finance-expert-thinks-bitcoin-will-fall-99-percent-by-june/

• 10 décembre 2013, Timothy B. Lee (Journaliste économique) :

In recent weeks, some Bitcoin critics have been rethinking their initial Bitcoin skepticism. But others are as convinced as ever that the cryptocurrency is doomed. One of the harshest critics is Mark Williams, who teaches finance at the Boston University School of Management. He predicts that in the first half of 2014, bitcoins will lose almost 99 percent of their value, falling below $10.

---

https://al3x.net/2013/12/18/bitcoin.html https://al3x.net/

• 18 décembre 2013, Alex Payne (Informaticien, écrivain) :

Bitcoin, Magical Thinking, and Political Ideology.

[...] Most charitably, Bitcoin is regarded as a flawed but nonetheless worthwhile experiment, one that has unfortunately attracted outsized attention and investment before correcting any number of glaring security issues.

To those less kind, Bitcoin has become synonymous with everything wrong with Silicon Valley : a marriage of dubious technology and questionable economics wrapped up in a crypto-libertarian political agenda that smacks of nerds-do-it-better paternalism. With its influx of finance mercenaries, the Bitcoin community is a grim illustration of greed running roughshod over meaningful progress.

Far from a "breakthrough", Bitcoin is viewed by many technologists as an intellectual sinkhole. A person's sincere interest in Bitcoin is evidence that they are disconnected from the financial problems most people face while lacking a fundamental understanding of the role and function of central banking. The only thing "profound" about Bitcoin is its community's near-total obliviousness to reality.

[...] The push toward Bitcoin comes largely from the libertarian portion of the technology community who believe that regulation stands in the way of both progress

and profit. Unfortunately, this alarmingly magical thinking has little basis in economic reality. The gradual dismantling of much of the US and international financial regulatory safety net is now regarded as a major catalyst for the Great Recession. The "financial or political constraints" many of the underbanked find themselves in are the result of unchecked predatory capitalism, not a symptom of a terminal lack of software.

Silicon Valley has a seemingly endless capacity to mistake social and political problems for technological ones, and Bitcoin is just the latest example of this selective blindness

---

http://www.atlantico.fr/decryptage/que-bitcoin-revele-enfer-terrestre-que-serait-paradis-libertarien-eric-verhaeghe-929581.html?page=0,1

• 19 décembre 2013, Eric Verhaeghe (Écrivain, journaliste, ancien élève de l'ENA) :

Ce que le Bitcoin nous révèle de l'enfer terrestre que serait le paradis libertarien.

Il est bien probable que les péripéties que les bitcoins traversent donnent le signal prématuré d'une mort doctrinale pour le libertarisme, et d'un scepticisme généralisé pour les monnaies privées.

Premier problème : le bitcoin est accusé de couvrir les pires activités mafieuses. Alors que le secret bancaire est de plus en plus fragilisé, et que tout flux financier doit, de façon grandissante, être « blanchi », le caractère totalement privé du bitcoin attire les convoitises. Quel système mieux adapté que la relation « peer to peer », loin des règles contraignantes de la puissance publique, pour recycler de l'argent sale ?

Deuxième problème : le bitcoin est une monnaie extrêmement spéculative qui enrichit quelques détenteurs futés. Selon certaines sources, la moitié de la masse de bitcoin serait détenue par moins de mille particuliers. Un tiers du stock serait détenu par moins de cinquante personnes. Cette extrême concentration souligne le premier intérêt du système : enrichir ses créateurs, et rien de plus.

Car, troisième problème : le bitcoin est extrêmement volatil. En quelques jours, il peut perdre une part importante de sa valeur. C'est le cas en ce moment : ce mercredi, le bitcoin a perdu 50% de sa valeur, après des annonces inquiétantes en Chine.

Cet épisode marquera les esprits. Un monde sans État et sans pouvoir public est toujours possible. Mais c'est un monde opaque, inégalitaire, et fondamentalement instable. Or la stabilité et la confiance sont des conditions nécessaires à la prospérité.

---

http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0

• 28 décembre, Paul Krugman (Économiste, Prix Nobel d'économie 2008) :

Bitcoin is evil. [...] I have had and am continuing to have a dialogue with smart technologists who are very high on BitCoin — but when I try to get them to explain to me why BitCoin is a reliable store of value, they always seem to come back with explanations about how it's a terrific medium of exchange. Even if I buy this (which I don't, entirely), it doesn't solve my problem. And I haven't been able to get my correspondents to recognize that these are different questions.

`http://www.livemint.com/Opinion/fEXo8r2OcAIZHWOMbZmmfO/Investors-beware-of-Bitcoin.html`

• 13 janvier 2014, Avinash Persaud (Directeur d'une société spécialisée dans les produits financiers) :

[...] Bitcoin is a cryptographer's wet dream rather than a useful monetary system.

[...] Bitcoins have been stolen and there are allegations of covert creation of bitcoins and cornering of supply by a few larger computer networks.

[...] Bitcoins will be worthless within a couple years.

[...] Because of its anonymity, bitcoins are attractive in the laundering of illicit activities.

[...] Sooner rather than later, holders will find that there are a diminishing number of greater fools left to buy bitcoins from them, and its price will collapse. Don't be tempted.

Pour

`http://bitcoin.org/bitcoin.pdf`

• 2008, Satoshi Nakamoto (personnage anonyme concepteur du Bitcoin, voir *Complément 6*) :

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll

generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

---

http://www.paristechreview.com/2012/01/20/bitcoin-devise-complementaire-universelle/

• 20 janvier 2012, Pierre Noizat (Cofondateur de Paymium (Bitcoin Central) et spécialiste du Bitcoin) :

Tout comme l'or, les bitcoins peuvent être assimilés à des obligations sans échéance. Mais à la différence de l'or, les bitcoins peuvent être divisés indéfiniment et n'impliquent aucun frais de stockage. D'après les estimations de GFMS, fin 2010, le stock d'or extrait se chiffre à hauteur de 166 600 tonnes, ce qui, au prix moyen de l'année 2010, représente 6500 milliards de dollars dont environ 2400 milliards constituent des réserves privées ou officielles, sous forme de pièces ou de lingots. Le stock total moins les 30 000 tonnes correspondant aux réserves officielles mondiales en août 2011, nous donne une estimation de 1230 milliards de dollars pour le marché de l'or, en tant que réserve de valeur. Si l'on devait calculer un taux de change du bitcoin avec le dollar sur la base de ces chiffres, on obtiendrait un taux de change de 600$ pour 1 BTC, si les bitcoins représentaient 1% du marché privé de l'or comme instrument de couverture.

Dans le même esprit, si l'économie bitcoin devait croître à hauteur de 5% du PIB des États-Unis (c'est-à-dire 725 milliards de dollars) et en supposant une vélocité monétaire du bitcoin égale à 50, équivalente au dollar pour les petits montants, un bitcoin représenterait l'équivalent de 700$. Cela équivaudrait à une valeur projetée de 15 milliards de dollars pour le réseau bitcoin. C'est un ordre de grandeur cohérent avec la capitalisation boursière de Visa, Inc. (55 milliards de dollars) ou de MasterCard (39 milliards de dollars). Acheter des bitcoins aujourd'hui, c'est acheter des actions pour un nouveau réseau mondial de transactions électroniques. À 10$ en août 2011, soit une valorisation du réseau bitcoin établie à 210 millions de dollars, les bitcoins sont clairement sous-évalués même en admettant que d'autres devises universelles pourraient entrer en lice.

[...] Du fait qu'ils sont échangés électroniquement, les bitcoins, contrairement à l'or, sont infiniment divisibles et permettent une grande vélocité monétaire. Ainsi, une forte déflation des prix ne ferait que limiter bitcoin à un rôle de réserve de valeur, plus pratique que l'or. En fait, la déflation des prix n'aurait de conséquences économiques néfastes que si les bitcoins étaient la devise exclusive d'une aire géographique donnée. Cela n'est absolument pas le cas puisqu'en tant que devise complémentaire, les bitcoins coexistent avec la devise locale sponsorisée par l'État, sans chercher à la remplacer. Les prix dans les commerces de proximité continueront à

être exprimés en devises locales. Dans une transaction électronique en ligne, le prix exprimé en devise universelle peut facilement être ajusté en temps réel par rapport à un taux de change variable. C'est uniquement pour les transactions qui ne sont pas en ligne que la stabilité des prix est une exigence pour toute devise universelle. En bref, la déflation des prix augmente l'attractivité des bitcoins en tant que valeur refuge et n'affecte que marginalement son application en tant que moyen d'échange.

Conclusions. Dans une économie mondialisée, la naissance d'une ou de plusieurs devises universelles est inéluctable dès lors qu'elle est technologiquement faisable et économiquement souhaitable.

Bitcoin, en tant que première devise du genre, a largement ouvert la voie à de nouvelles applications. En particulier, bitcoin peut fortement améliorer l'efficacité des transferts d'argent là où il y en a le plus besoin, notamment pour l'aide au développement, longtemps considérée (selon les mots de l'économiste Peter Bauer) comme « une excellente façon de transférer l'argent des pauvres des pays riches aux riches des pays pauvres ». Bitcoin peut profiter de la généralisation des téléphones mobiles dans les pays en voie de développement pour permettre de transférer de l'argent directement, sans passer par des intermédiaires, qu'ils soient bureaucratiques ou bancaires. L'institution ou l'organisme non-gouvernemental responsable du transfert assignera simplement des adresses bitcoin aux destinataires et les marchants locaux pourront alors réaliser des transferts d'argent et des paiements en bitcoins.

Cette technologie permet à la fois un nouveau type de transaction sur le réseau et une nouvelle devise universelle.

Par analogie, il est intéressant de noter que la gouvernance du World Wide Web est régie par une organisation à but non-lucratif — le W3C — composée de 300 membres parmi les plus grandes entreprises du secteur des hautes technologies. Clairement, tout appui de la part d'un gouvernement à l'un des membres du W3C peut être contrebalancé par les autres si cela ne convient pas à l'intérêt général. Si ce principe parvient avec succès à réguler un domaine où la technologie sert de nouvelles méthodes de production et de partage du savoir, il est permis d'espérer qu'une organisation similaire peut également superviser les caractéristiques techniques du protocole bitcoin. Cela permettrait à bitcoin de préserver son intégrité et son potentiel d'innovation face aux aléas des mesures macro-économiques.

Philippe Herlin, *La révolution du Bitcoin et des monnaies complémentaires*, Éditions Eyrolles, 2013.

• Mai 2013, Philippe Herlin (Docteur en économie du CNAM, chercheur en finance) :

Soyons clairs, le bitcoin constitue une remise en cause frontale de leur capacité à tout régenter dans le domaine monétaire et financier. Les États, pour la plupart, creusent leur déficit, alourdissent leur dette, demandent à leur banque centrale de

racheter cette dette (c'est la « planche à billets »), ce qui dévalue la valeur de la monnaie. Et ils s'autorisent désormais à ponctionner directement les comptes bancaires et à instaurer un contrôle des mouvements de capitaux, comme on l'a vu à Chypre. Le bitcoin permet d'échapper à tout cela, d'avoir un compte inviolable, une monnaie solide, et d'effectuer facilement des transactions. Face aux États qui jouent aux apprentis sorciers avec leur monnaie, on peut considérer que les citoyens ont le droit à l'autodéfense.

[...] La révolution monétaire, cela consiste tout simplement à ne plus être prisonnier d'une seule monnaie ni du système bancaire, et à retrouver sa liberté, à choisir les systèmes auxquels on accorde sa confiance. Les monnaies officielles resteront encore longtemps prédominantes, mais elles seront de moins en moins exclusives. Elles seront mises en concurrence, comparées, et il y a peu de chance que ça tourne en leur faveur. De la même façon, suite à l'affaire de Chypre et à la ponction opérée sur les comptes bancaires, la volonté de sortir du circuit bancaire ne va faire que croître.

Les alternatives existent, nous l'avons vu, avec les monnaies complémentaires en fort développement depuis les années 1990, la possible remonétisation de l'or, et surtout le bitcoin, universel, électronique, indépendant de toute puissance étatique ou financière, offrant à chacun un compte inviolable et des transactions parfaitement sécurisées.

Les grands groupes internationaux des télécoms s'intéressent également de près à cette révolution et, déjà, des systèmes bancaires alternatifs complets existent dans plusieurs régions du monde. Les grands acteurs de l'électronique grand public ne restent pas inactifs : Google avoue s'intéresser au bitcoin, Amazon a créé sa propre monnaie avec l'Amazon Coin, et d'autres initiatives ne devraient pas manquer d'intervenir.

Quelle sera l'ampleur et la rapidité de cette révolution ? Difficile à dire, mais plus les dettes publiques et privées augmentent à travers le monde, plus les planches à billets des banques centrales tournent, plus le phénomène sera rapide. Les États feront tout pour garder le contrôle de leur monnaie, y compris en en créant une nouvelle si l'ancienne explose en vol, mais tous ses détenteurs auront été ruinés au passage, au contraire de ceux qui possèdent des bitcoins, de l'or, des monnaies complémentaires indexées sur des matières premières, et des actifs réels en général (immobilier, œuvres d'art, terrains agricoles). À bon entendeur...

Face à des États qui s'endettent toujours plus, qui manipulent leur monnaie et n'hésitent pas — comme à Chypre — à ponctionner les comptes et à restreindre les mouvements de capitaux, les citoyens ont à leur disposition de nouveaux moyens d'autodéfense.

http://www.latribune.fr/journal/edition-du-2008/opinions/780725/le-bitcoin-une-exigence-democratique-.html

• 19 août 2013, La tribune :

Le Bitcoin, une exigence démocratique.

[...] Tout bitcoin ou fraction de bitcoin composant le montant d'une transaction trouve son origine dans une transaction précédente, dite transaction de génération, qui crée 25 bitcoins. Ces transactions interviennent toutes les dix minutes et les bitcoins générés sont distribués par un algorithme complexe aux nœuds du réseau qui vérifient et relaient les transactions. Parce que tout le monde peut participer ainsi librement au réseau bitcoin, cette technologie change notre rapport de négociation avec les banques, jusqu'à présent entièrement dominé par le banquier pour tous nos échanges économiques. De même que, grâce à l'email, nous utilisons les services de la Poste lorsqu'ils nous sont vraiment utiles, nous pourrons désormais décider de passer par la banque seulement quand elle aura une valeur ajoutée réelle.

Le bitcoin, plus pratique et plus sécurisé.

Dans la plupart de nos transactions effectuées dans un contexte connu et pour des montants limités (commerce de proximité, amis, famille, etc), la technologie bitcoin sera préférée pour des raisons pratiques et politiques. Sur un plan pratique en effet, les commissions de transactions sur le réseau bitcoin sont fixées librement par le payeur qui peut les mettre à zéro. Et contrairement à un virement bancaire ou un paiement par carte bancaire, une transaction bitcoin est diffusée en quelques secondes sur le réseau. Au plan politique, le citoyen préférera un système de paiement comme bitcoin qui lui laisse maîtriser la divulgation des données de transaction plutôt que la capture systématique de ces données par des multinationales.

---

http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/05/when-will-the-people-who-called-bitcoin-a-bubble-admit-they-were-wrong/

• 5 novembre 2013, Timothy B. Lee (Journaliste économique) :

When will the people who called Bitcoin a bubble admit they were wrong ?

[...] The word "bubble" comes up a lot in discussion of Bitcoin. Bubble talk last peaked in April of this year, when the value of one Bitcoin soared from less than $100 at the start of the month to an all-time high of $266 on April 10. And in the next few weeks, it appeared that the skeptics had been vindicated. Bitcoin prices tumbled, falling to a low of about $50 before stabilizing back around $100. Bitcoin critics argued that the Bitcoin-buying public had fallen prey to irrational exuberance, and that one unit of the crypto-currency couldn't possibly be worth $266. But then something interesting happened. After a few months of relative stability, Bitcoin prices began rising sharply again. Since the start of October, Bitcoin prices have doubled from 125*to*250*. That's just shy of the all-time high of $266.*

That poses a problem for those who called the high prices of last April a bubble. When people describe a market move as a "bubble", they're generally referring to more than a rapid price increase that's followed by a decline — that's just garden-variety volatility. Rather, the term "bubble" refers to appreciation that is driven by hype rather than a sober consideration of market fundamentals. When bubbles pop, they tend to stay popped, as the market comes to its senses and realizes that the earlier, higher price was irrational. So if a price returns to its earlier highs a few months later, that suggests that the original appreciation might not have been so irrational after all.

`http://www.contrepoints.org/2013/12/09/149249-bitcoin-la-monnaie-qui-derange`

• 9 décembre 2013, Jérémy Berthet (Ingénieur informatique) :

La nature déflationniste et décentralisée du système Bitcoin le rend complètement étranger aux mécanismes d'une pyramide de Ponzi. On ne peut pas en dire autant de nos monnaies d'État, réputées sûres et régulées, mais contrôlées par une entité centrale au sommet très accommodante avec les premiers arrivants que sont les banques et qui ne paient pas le contrecoup de l'inflation, à la différence des citoyens en bas de l'échelle.

Tout comme l'échange « peer to peer » de fichiers devrait amener l'industrie culturelle à revoir son modèle, le Bitcoin, pour autant qu'on le laisse vivre, devrait conduire les acteurs de la finance à s'adapter à un « nouveau » paradigme monétaire plus sûr et plus fiable que l'actuel. Internet est une technologie dont l'évolution permet de réduire drastiquement le nombre d'intermédiaires commerciaux. Si Bitcoin n'y parvient pas pour la monnaie, suite à une réaction de peur des États, vous pouvez être certain que d'autres y arriveront plus tard, ce n'est qu'une question de temps.

`http://www.digitaltrends.com/opinion/everyone-planet-invest-bitcoin/`

• 10 décembre 2013, Andrew Couts (Journaliste spécialisé dans les nouvelles technologies) :

At its heart, Bitcoin is a protocol in the same way the Web (HTTP) and the Internet (TCP/IP) are protocols. Whereas HTTP dictates how Internet-connected computers "talkèè to each other, the Bitcoin protocol allows for the encrypted, anonymous transfer of funds (i.e. a unit of value) across the Internet.

To take the Internet comparison further, just as the Internet allows for the free flow of information, Bitcoin allows for the free flow of "money" in ways impossible before its invention. Use a legacy banking system, PayPal, or anything besides cash in an envelope, and you're looking at fees, delays, and headaches. Bitcoin solves all

of this, offering the possibility for instant fund transfers to anywhere in the world, zero or extremely low transaction fees (even when transferring millions of dollars worth of Bitcoin), and the ability to send someone Bitcoin (or fractions of a Bitcoin) simply by knowing their Bitcoin address — no other account information, names, or routing numbers needed.

On top of all these benefits, the Bitcoin protocol is based upon extremely strong encryption and a public ledger system (called the "blockchain") that uses distributed transaction confirmations to ensure the integrity of every single Bitcoin transaction. (Told you it would get nerdy...)

Bitcoin Believers will tell you that no one really knows Bitcoin's true potential, just as the Vint Cerf and Tim Berners-Lee never envisioned what the Internet and Web would become when they created the respective protocols on which these world-changing technologies are based.

---

http://www.lefigaro.fr/secteur/high-tech/2013/12/11/01007-20131211ARTFIG00469-pourquoi-le-bitcoin-fait-grincer-des-dents.php

• 11 décembre 2013, Pierre Noizat (Cofondateur de Paymium (Bitcoin Central) et spécialiste du Bitcoin) :

Si le monde veut rentrer dans l'économie numérique, il faut s'adapter aux changements technologiques plutôt que de crier au loup. [...] Comme toute nouvelle technologie, le bitcoin reste réservé aux personnes averties, conclut Pierre Noizat. Mais une fois que les banques auront compris qu'il s'agit d'un vrai business, les barrières à l'entrée seront levées et la monnaie plus accessible pour les particuliers.

Dans cinq ans, le bitcoin sera adopté par tous.

---

http://cdixon.org/2013/12/12/coinbase/

• 12 décembre 2013, Chris Dixon (Entrepreneur et investisseur internet américain) :

Bitcoin is the first plausible proposal for an economic protocol for the Internet.

This matters for two reasons :

1) It fixes serious problems with existing payment systems that depend on centralized services to verify the validity of transactions. These services are both expensive (roughly a 2.5% tax on all transactions) and prone to failure (Internet payment fraud is rampant).

2) More importantly, Bitcoin is a platform upon which new technologies can be developed. Developers have created some early applications, and speculated about future applications. Some potential applications include : a) micropayments as a replacement for banner ads or subscription fees, b) machine-to-machine payments to reduce spam and denial-of-service attacks, c) a way to offer low-cost financial

services to people who, because of financial or political constraints, don't have them today.

But to proliferate widely, Bitcoin needs a killer app the same way HTTP had web browsers and SMTP had email clients. That's why today I'm excited to announce that Andreessen Horowitz is leading a $25M financing of Coinbase, a service that provides an accessible interface to the Bitcoin protocol. Consumers can use Coinbase to convert to and from other currencies and to pay for goods and services. Merchants can use Coinbase to accept payments and convert currencies. Developers can build new services using Coinbase's API.

Coinbase has grown extremely fast and is now the most widely used Bitcoin service in the US. The founders of Coinbase, Brian Armstrong and Fred Ehrsam, have worked closely with banks and regulators to ensure that the service is safe and compliant. We think Coinbase can significantly accelerate Bitcoin's proliferation, and as that happens the Internet will enter a new phase of invention and opportunity.

[Une réponse en `https://al3x.net/2013/12/18/bitcoin.html`]

`http://motherboard.vice.com/blog/bitcoin-becomes-a-real-job-and-wall-street-is-hiring`

• 2 janvier 2014, Alec Liu (Écrivain spécialisé dans les nouvelles technologies) :

Bitcoin Becomes a Real Job and Wall Street Is Hiring

[...] Yesterday, Wall Street analysts Wedbush added their endorsement (`http://www.businessinsider.com/winners-and-losers-in-bitcoin-2014-1`), noting that they "believe Bitcoin and its associated technology represent a potential disruption to our covered companies", and adding that "Bitcoin's potential lies beyond the 'coin' as the underlying blockchain protocol can be used to replace traditional intermediaries by acting as an exchange mechanism for a multitude of transactions".

Wall Street was also the location of Bitcoin's New Year's Eve party in New York the other day, when Steve Stockman, a Republican representative from Texas, promised to sponsor a pro-Bitcoin bill. [...]. BOND New York, a real estate brokerage firm just announced that it would start accepting Bitcoin as payment for real estate transactions. The litany of pro-Bitcoin news has helped push the price over $800 again on Mt. Gox. Bitcoin, it appears, is as resilient as ever.

The influx of more established financial players will inevitably help decrease Bitcoin's price volatility, which currently prevents it from being a more useful currency.

`http://www.lemonde.fr/idees/article/2014/01/06/pourquoi-les-economistes-devraient-etre-interesses-par-le-bitcoin_4343607_3232.html`

• 6 janvier 2014, Nicolas Houy (Économiste, chercheur CNRS) :

Pourquoi les économistes devraient être intéressé par le Bitcoin

[...] Les économistes ont vite fait de mettre le bitcoin dans une catégorie dont ils ont l'habitude de traiter et de le trouver au mieux inutile, le plus souvent néfaste, en tout cas, à éviter.

Mais le bitcoin n'est rien de tout cela. C'est un protocole. Comme le sont le HTTP (le protocole derrière l'Internet que vous utilisez tous les jours) ou le SMTP (un des protocoles derrière les e-mails). Ainsi, le bitcoin est un langage, un moyen de communication entre ordinateurs.

Grâce à ce moyen de communication, on peut échanger de l'argent entre deux points du globe sans coût. C'est déjà pas mal. Mais le bitcoin ne doit pas être résumé à cela, au risque de passer à côté du sujet. Comme tout protocole, chacun peut s'emparer de ce langage et en faire ce qu'il veut.

[...] le bitcoin ne doit pas être vu seulement comme une nouvelle version d'un objet économique déjà existant (vous entendrez certainement monnaie ou or 2.0). C'est un langage offrant des horizons infinis à quiconque décide de s'en emparer. Et les économistes, qui passent tant de temps à étudier les situations dans lesquelles les contraintes physiques empêchent la contractualisation, pourraient être bientôt les plus intéressés à en imaginer les usages futurs.

D'autres citations sélectionnées, « Pour » et « Contre », se trouvent en :

`http://www.lifl.fr/~delahaye/Bitcoin/Bitcoin.pdf`.