Le *Bitcoin*
Une monnaie révolutionnaire ?

27 janvier 2014

Jean-Paul Delahaye

Université de Lille 1

Laboratoire d'Informatique Fondamentale de Lille,

UMR 8022 CNRS, Bât M3-ext 59655 Villeneuve d'Ascq Cedex
email : delahaye@lifl.fr

La cryptographie mathématique et la puissance des réseaux pair à pair ont rendu possible l'existence de monnaies purement numériques sans autorité centrale de contrôle.

Ce nouveau type de monnaies pourrait changer le monde.

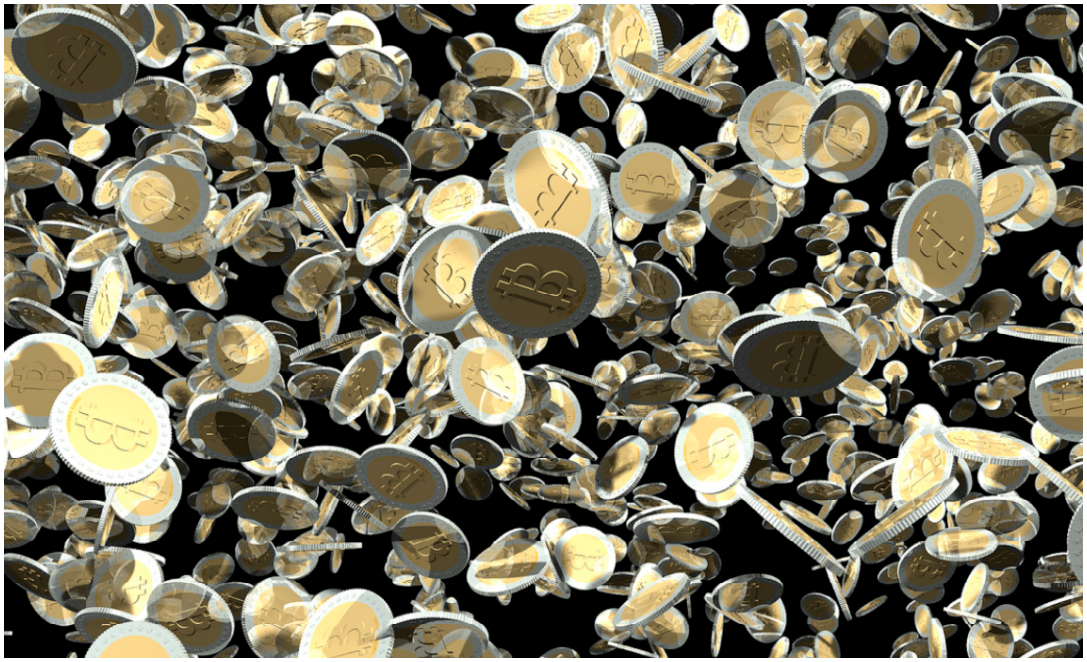


Image de Francesco De Comité (LIFL)

Une étonnante monnaie électronique a récemment été créée. Elle suscite la passion, aussi bien de ses détracteurs que de ceux qui veulent y croire. Ne s'appuyant apparemment sur rien de tangible, le total des devises sorties simplement d'un protocole cryptographique a réussi l'exploit incroyable de valoir aujourd'hui l'équivalent de plusieurs milliards d'euros (plus de 7 milliards d'Euros le 21 janvier 2014, voir http://bitcoinwatch.com/)

Ce *Bitcoin* est basé sur 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 en économie— et particulièrement délicat —personne aujourd'hui ne sait vraiment ce que ce montage numérique va devenir. D'ailleurs, les avis les plus extrêmes s'expriment à son sujet : voir le ***Complément 7*** à la fin de ce document.

Les monnaies électroniques ne sont pas une nouveauté, et d'une certaine façon toutes les monnaies le sont. 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 disfonctionnement 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 superette 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 car tout y est public : les protocoles de bases, les algorithmes cryptographiques utilisés, les programmes les rendant opérationnels et les données des comptes.

À tout instant, chacun peut savoir combien il y a de *Bitcoins* sur chaque compte existant et participer à la vérification des nouvelles transactions. Cette 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 anonymat des détenteurs comme aucun autre système ne le permet.

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 par exemple des numéros de compte :

1FxkfJQLJTXpW6QmxGT6oF43ZH959ns8Cq

13cia2KGVASavNmRs4niK5RSRfwkB1uLAu

1A6dpTWvoLWmTgwezLmyQti8oDUcLtjTKX

Le ***Complément 1*** (à la fin du document) explique ce que sont les *clefs privées* et *clefs publiques* introduites en cryptographie il y a une quarantaine d'années.

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 capables de retenir la longue série de chiffres et de lettres. 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 à qui il a affaire. De plus —et c'est arrivé— les gestionnaires du site peuvent s'emparer de votre argent et disparaître avec. Le plus prudent sera donc peut-être de gérer soi-même ses comptes sur son ordinateur (ou son smartphone). Les logiciels permettant cela (wallet) 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 et même contribuent à leur amélioration. Aujourd'hui les logiciels permettant de gérer sur sa machine des comptes *Bitcoins* sont disponibles gratuitement (le plus souvent) pour tous les types de machines (Voir par exemple https://multibit.org/).

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—, ou alors il faut être passé par une plateforme de change qui accepte de convertir des devises classiques en *Bitcoins*, (la plus importante est Mt Gox : https://www.mtgox.com/). Dernière possibilité : il faut les avoir gagnés en participant aux opérations de contrôle collectif de la monnaie (on verra plus loin comment).

La gestion de ses comptes 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 l'addresse 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 gardées «au froid», c'est-à-dire sur des ordinateurs non connectés au réseau, ou même que l'on éteint.

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 entre les comptes, 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. Dans le ***Complément*** 2 on explique le protocole d'une transaction.

Toute 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 très difficile 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.

Le *système simplifié des Bitcoins* consiste en un *fichier de compte* que tous les utilisateurs —dont la liste est fixée à l'avance et ne peut 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 compte* tenu à jour par tous les utilisateurs contient toutes les opérations de transferts (transactions) d'un compte vers un autre et permet donc de savoir quelles sommes sont présentes sur les comptes. Ce *fichier de compte* peut ne conserver à chaque instant que l'information du solde de chaque compte.

Les seules transactions possibles sont du type «le compte A verse la somme S au compte B» et 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 avoir contrôlé en utilisant leur *fichier de compte* 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 compte* 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 euros. 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 compte* commun en a. Cette *caisse* permettrait par exemple aux dix amis de vivre ensemble dans un appartement en contribuant inégalement aux dépenses communes, faites bien sûr avec de vrais euros, que le fichier de compte rééquilibrerait. Quand par exemple Jean dépense 100 euros (véritables) pour les courses de l'appartement, ses 9 amis lui versent chacun 10 unités sur son compte (chacun a donc dépensé 10 euros). 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 compte*.

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 vider 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 évoluer. Il fallait 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* est intéressant à comprendre car il 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 en profondeur ce qu'est le *Bitcoin*, et pourquoi il marche et ne constitue en rien une escroquerie. Ses insuffisances 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 entre 10 amis, gérée par un *fichier de compte* 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 dans le système des *Bitcoins* mis en place en janvier 2009:

- des nouveaux utilisateurs (comptes) peuvent d'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 des certaines machines du réseau, la coupure et même l'isolation 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 où personne ne peut tricher, à la seule condition qu'un nombre minimum de participants acceptent de suivre le fichier de compte.

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 ou de tricheries. Ces perfectionnements rendent facultative la participation au contrôle qui ne sera mené que par les nœuds du réseau qui le souhaitent, mais pour éviter que trop peu de nœuds du réseau participent au travail de contrôle (ce qui serait catastrophique, bien évidemment) 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 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 s'en aperçoive dans un délai très court. Il n'y a pas de police, la conception même de la monnaie doit donc empêcher seule la fraude et les disfonctionnements.

Cela semble impossible et c'est pourquoi la construction conçue par Satoshi Nakamoto est souvent qualifiée de géniale. Personne avant lui n'avait imaginé un système aussi robuste. Le scepticisme sur la robustesse de la nouvelle monnaie, assez fort au départ, tend à s'atténuer.

Le fait que la monnaie ait tenu plus de cinq ans malgré toutes les attaques qu'elle a eu à subir est la meilleure preuve qu'elle est vraiment sérieuse, et c'est l'une des explications de la valeur actuelle du *Bitcoin* qui dépasse 600 euros (mais fluctue beaucoup... il ne vaudra peut-être plus cela quand vous lirez l'article !).

Une page toutes les 10 minutes

L'idée pour l'amélioration du modèle simplifié consiste à gérer un *cahier de compte* (dont le nom technique est *Blockchain*) qui est complété progressivement par ajout de nouvelles *pages de transactions* (nommées *block*) toutes les 10 minutes environ. Ce *cahier de compte* est le *fichier de compte* du modèle simplifié, sauf qu'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. 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 au *cahier de compte*, et qui est rémunéré pour cela par 25 *Bitcoins* créés ex nihilo. Lorsque la nouvelle page est ajoutée au cahier de compte, cela valide les transactions qui y apparaissent. Cette création de *Bitcoins* est la seule possible, et tous les *Bitcoins* existants sont apparus de cette façon.

Lors d'une transaction en ma faveur, mon ordinateur connecté au réseau consulte le *cahier de compte* (qui est fichier commun partagé par tous les nœuds vérificateur du réseaux P2P) et 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 le cahier de compte, 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 rarissimes, et pour de petites transactions, on n'attend même pas les 10 minutes. Le cahier de compte peut être exploré à partir de http://blockchain.info/fr.

Dédoublement du cahier de compte

La possibilité d'ennuis sur le réseau et les délais de transmission des messages ont pour conséquence que parfois deux ajouts de pages au cahier se feront quasi-simultanément dans deux parties éloignées du réseau, créant temporairement un dédoublement du *cahier de compte*. Les deux versions peuvent alors contenir une dernière page sensiblement différente dans l'un et dans l'autre, ce qui rend alors possible une double dépense. L'événement est rare, mais comme il est possible et inévitable à cause de l'imperfection des communications, un procédé de remise en ordre du système est prévu. Les deux cahiers continueront chacun de leur côté à se voir ajouter des pages toutes les 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 des deux cahiers malencontreusement créés ne se feront pas à la même vitesse exactement. Le cahier le plus long (donc celui qui a été complété de plusieurs nouvelles pages le plus rapidement) est considéré comme le bon. Cette règle traduite dans les programmes de vérification des comptes conduit à l'élimination de l'autre *cahier de compte* et donc à la reconstitution d'un état cohérent du

système où ne persiste qu'un seul *cahier de compte* et où d'éventuelles doubles dépenses sont impossibles.

Ces ennuis temporaires, rares mais inévitables, dans la gestion du *cahier de compte* 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. Voir le ***Complément*** 4 sur les *preuves de travail* qui explique la méthode cryptographique qui réalise cela. Le travail fait par vos machines pour tenter de gagner porte le nom de *minage*, par analogie au travail dans une mine qui conduit ceux qui ont de la chance à trouver de l'or.

Aujourd'hui participer à ces tirages au sort (et donc participer au contrôle général des comptes) est très tentant puisque 25 *Bitcoins* s'échangent contre plus de 16000 euros (21 janvier 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. En effet, on sait que les cartes graphiques disposent d'une puissance importante et qu'on peut la détourner à d'autres choses que le simple traitement des images numériques. Aujourd'hui les cartes graphiques ne sont plus suffisantes 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. Précisons que le système de Nakamoto est conçu pour qu'il y ait un gagnant toutes les dix minutes environ et qu'il s'ajuste automatiquement pour que ce temps moyen ne diminue pas. Des entreprises 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.

Cinq mille fois le plus puissant des ordinateurs

La puissance globale consacrée aujourd'hui au minage de *Bitcoins* est de 191 000 pétaflops (le 21 janvier 2014, voir http://bitcoinwatch.com/ ; 1 pétaflops = 10^{15}

opérations en virgule flottante). C'est plus de 5000 fois la puissance du plus puissant ordinateur du monde (le «Tianhe-2» détenue par la Chine) qui n'a qu'une puissance de 33 pétaflops, et c'est largement plus que vingt fois la puissance cumulée des 500 ordinateurs les plus puissants.

C'est considérable ! Ce qu'on peut voir comme un énorme gâchis s'empirera si le *Bitcoin* s'impose et que son cours (qui bien sûr détermine l'argent que les mineurs sont prêts à investir) progresse. Notons que les défenseurs du *Bitcoin* argumentent en disant qu'une monnaie basée sur l'or est aussi absurde que le *Bitcoin* puisqu'on n'utilise pas l'or qui reste dans des coffres qu'il faut surveiller, et que 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 utilisée 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 intéressants 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. Il n'est pas du tout certain aujourd'hui que *Primescoin* s'imposera.

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 «guildes de mineurs». 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 guilde (si elle est puissante) remportera assez fréquemment les 25 *Bitcoins* qu'elle redistribuera à ses membres. Toutefois ne vous faites pas d'illusion : en rejoignant une guilde, si vous n'offrez que la puissance de votre ordinateur personnel, la part qui vous reviendra sera minuscule.

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 3 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 du cahier de compte cesse, Nakamoto a prévu qu'à chaque transaction, on donne une commission à celui qui ajoutera la page contenant la transaction au cahier. L'intérêt de miner sera donc préservé, même au-delà de 2140. Donner une telle commission n'est pas obligatoire et aujourd'hui même si vous ne laissez rien, vos transactions sont quand même validées et passent dans le *cahier de compte*. Après 2140, il deviendra sans doute souhaitable de laisser un petit quelque chose à chaque transaction... on a le temps d'y penser.

L'impossible devenu réalité... et valeur

Le système mis en fonctionnement il y a bientôt cinq ans tient solidement. Dans un premier temps, le cours du *Bitcoin* était dérisoire. Depuis un peu plus d'un an, il a monté pour atteindre 200 euros le 9 avril 2013. Il a ensuite chuté, puis en décembre 2013 est monté jusqu'à près de 900 euros (voir http://www.bitcoin.fr/pages/Cours-du-bitcoin). 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 :

> *Attention, si par le passé Bitcoin a été un placement très rentable, cela reste un investissement hautement spéculatif. Personne ne pouvant prévoir le destin de l'expérience Bitcoin, tant elle est novatrice et inédite, il est donc fortement recommandé de n'y investir que ce que l'on peut se permettre de perdre.*

Cependant, 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 (voir le ***Complément*** 7), mais l'intérêt qu'il suscite a de quoi rendre optimiste. Il semble bien 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.

-a- 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).

-b- Rien de possible non plus sans d'importantes puissances de calcul et de mémorisation informatique. 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— soit possible simultanément par des milliers d'acteurs différents et indépendants se contrôlant donc les uns les autres. Ce modèle crée sans doute une confiance bien meilleure dans les comptes immatériels de cette monnaie que dans celle qu'on a pour ceux d'une banque qui s'occupe en secret de gérer sa monnaie seule, en faisant marcher la planche à billets d'une manière imprévisible et sans demander leur avis aux détenteurs de devises qui s'en trouvent pourtant lésés.

-c- Le génie d'un (ou plusieurs ?) informaticien qui en s'appuyant sur une discipline ayant formidablement progressé depuis trente ans (la cryptographie) a produit un protocole étonnamment subtil et robuste que personne ne pensait possible, et qui a réussi à le faire fonctionner et décoller —ce n'était pas du tout évident.

-d- Essentielle aussi est la communauté des passionnés —un peu anarchistes— qui s'occupe des programmes libres et des réseaux pair à pair (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 au fond une monnaie commune, universelle et démocratique.

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

d'accorder sa confiance à des protocoles bien conçus, contrôlés par tous, plutôt qu'à des banques qui se moquent du reste du monde et qui, sans régulation collective, manipulent les monnaies aux dépens de (presque) tous.

Plutôt que de continuer à faire reposer l'indispensable monnaie sur des institutions centralisées qui se sont cent fois révélées défaillantes, il est plus rationnel de s'appuyer sur une organisation et un fonctionnement général de la monnaie fondée sur des protocoles cryptographiques reconnus, sur des logiciels que tout le monde peut examiner, et sur une transparence des comptes les rendant infalsifiables.

Bibliographie

• Simon Barber, Xavier Boyen, Elaine Shi, Ersin Uzun, *Bitter to Better, How to Make Bitcoin a Better Currency*, In Proceedings of Financial Cryptography, 2013.

• 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

• Nicolas Courtois, Marek Grajek, Rahul Naik, The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining 2013:

http://arxiv.org/pdf/1310.7935v2.pdf

• 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

• Ittay Eyal, Emin Gün Sirer, Majority is not Enough, arXiv preprint arXiv:1311.0243, 2013 :

http://www.nocash.info.ro/wp-content/uploads/2013/11/Cornell-University-study-about-Bitcoin.pdf

• 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

• Brian Hanley *The False Premises and Promises of Bitcoin*, arxiv 2013 :

http://arxiv.org/pdf/1312.2048.pdf

• Philippe Herlin, *La révolution du Bitcoin et des monnaies complémentaires*, Editions Eyrolles, 2013

• 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

• William Luther, *Bitcoin is Memory*, Social Science Network, 2013 :

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730

• Satoshi Nakamoto,*Bitcoin : A Peer-to-Peer Electronic Cash System*, 2009 :

http://bitcoin.org/bitcoin.pdf

• Michael Nielsen, *How the bitcoin protocol actually works*, 2013 [Explications plus détaillées qu'ici du protocole *Bitcoin*] :

http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

• Pierre Noizat, *Bitcoin : Derrière la bulle, de vrais débats*, Les Echos 23 août 2013 :

http://blogs.lesechos.fr/paristech-review/bitcoin-derriere-la-bulle-de-vrais-debats-a13320.html

• Mark Pinklinton, *Bitcoin and Complexity Theory : Some Methodological Implications,* Social Science Network, 2013 :

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2340007

• 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

• Dorit Ron, Adi Shamir,*Quantitative Analysis of the Full Bitcoin Transaction Graph*, In Proceedings of Financial Cryptography, 2013.

• 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

• Bitcoin Foundation (consulté en décembre 2013) :

https://bitcoinfoundation.org

• Wikipedia, Bitcoin (consulté en décembre 2013) :

http://en.wikipedia.org/wiki/Bitcoin

http://fr.wikipedia.org/wiki/Bitcoin

• Bitcoin wiki (consulté en décembre 2013) :

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

• Le cahier de compte Bitcoin (consulté en décembre 2013) :

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 $\mathbf{A_{pri}}$ (clef privée) et $\mathbf{A_{pub}}$ (clef publique). Ce sont des suites de symboles ou ce qui revient au même des nombres entiers.

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

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 $\mathbf{A_{pri}}$ et **M**

$$f(\mathbf{A_{pri}}, \mathbf{M}) = \mathbf{M'}$$ 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 $\mathbf{A_{pub}}$ et **M'**, ce qui produira **M** :

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

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 était cassé ?

Si le protocole de signature venait à être cassé et que quelqu'un disposant d'une clef publique $\mathbf{A_{pub}}$ sache calculer facilement la clef privée associée $\mathbf{A_{pri}}$, alors cette personne serait en mesure de dépenser le contenu de tous les comptes. À condition de le faire progressivement pour ne pas sa 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 le *cahier de compte*) ils découvriraient que leur compte est vide car quelqu'un a dépensé l'argent qui y était déposé.

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

On considère cependant que personne ne disposera jamais du moyen pratique de calculer $\mathbf{A_{pri}}$ à partir de $\mathbf{A_{pub}}$, ou que si cela se produit, la faiblesse du protocole de signature aura été repérée avant qu'elle soit devenue réellement utilisable, et donc, qu'on 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 celui ou ceux qui s'en aperçoivent le font savoir... ce qui évidemment n'est pas assuré.

On peut imaginer cependant que si des vidages de comptes étaient opérés en trop grand nombre, on arrêterait toutes les transactions et qu'on tenterait de réparer le protocole et de rétablir les comptes dans un état antérieur à la détection de la fraude. Au total, même dans ce cas extrême de mise en cause du protocole *Bitcoin*, il semble qu'on pourrait en limiter les conséquences et éviter l'écroulement total du système.

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

• Alice souhaite envoyer **N** *Bitcoins* à Bernard.

• Bernard communique sa clef publique $\mathbf{B_{pub}}$ à Alice.

• Alice constitue un message **M** de transaction contenant la clé publique de Bernard $\mathbf{B_{pub}}$ la somme **N** à transférer $\mathbf{M = B_{pub}N}$

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

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

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

• Alice diffuse la transaction signée sur le réseau afin qu'elle soit vue par tout le monde.

Le protocole réel est légèrement plus compliqué (il contrôle qu'Alice dispose bien de la somme **N** dans son porte-monnaie).

En regardant cette transaction depuis l'extérieur, tout le monde voit 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 message 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 de compte au *cahier de compte*, 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.

Ajustable 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*.

Complément 4

Les cours, la capitalisation, les «bulles»

La première page du cahier de compte du *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.
- 25 nouveaux *Bitcoins* sont créés aujourd'hui 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 (21 janvier 2014, midi) le total de *Bitcoins* émis est 12 291 625

Ils valent en tout 7 500 00 000 euros environ

Pour une mise à jour aller en http://bitcoinwatch.com/

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

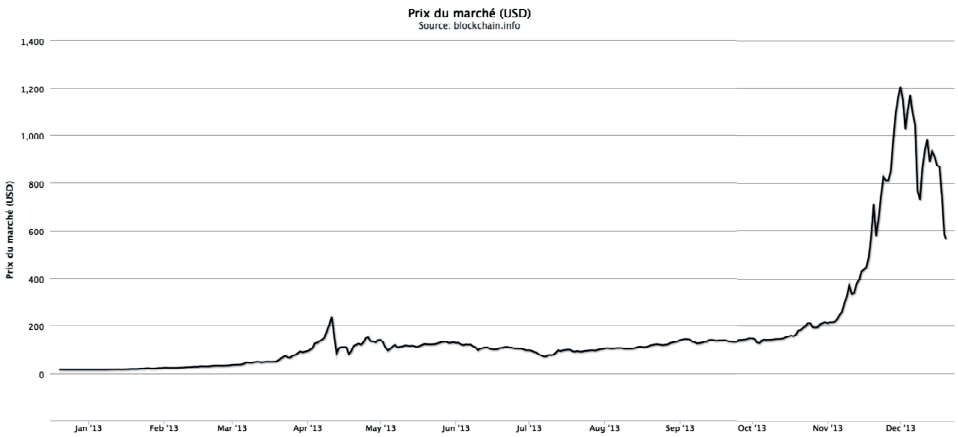
Le 11 avril 2013 : effondrement de la valeur du *Bitcoin* qui passe de 266 $ à 105$ et descend même ensuite à 60 $.

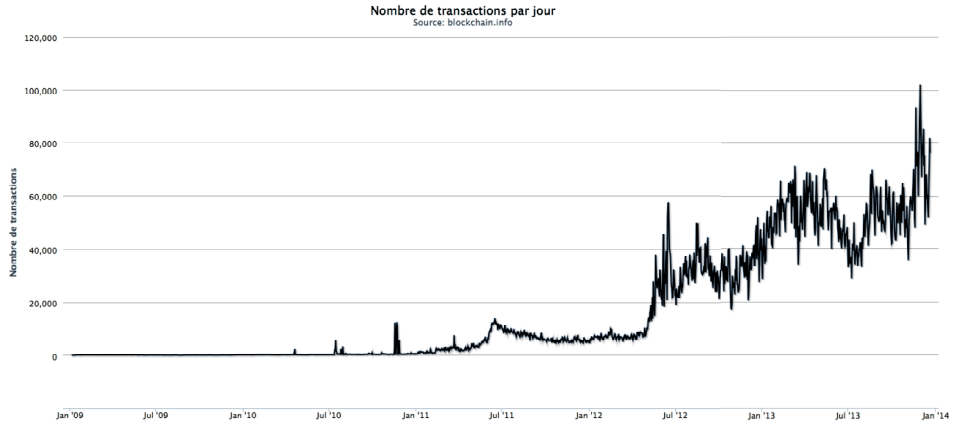
En décembre 2013, il atteint 900 euros avant de redescendre.

Taille de la blockchain 13,2 gigaoctets (21 janvier 2014)

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

https://blockchain.info/fr/charts
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 cryptomonaies)





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 beaucoup d'observateurs des récentes variations. En examinant ce cours depuis 2010, on voit que c'est en réalité la cinquième «bulle» qui gonfle et éclate (partiellement).

Cependant, ces «bulles» doivent-elles vraiment être appelée des «bulles» puisque qu'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.

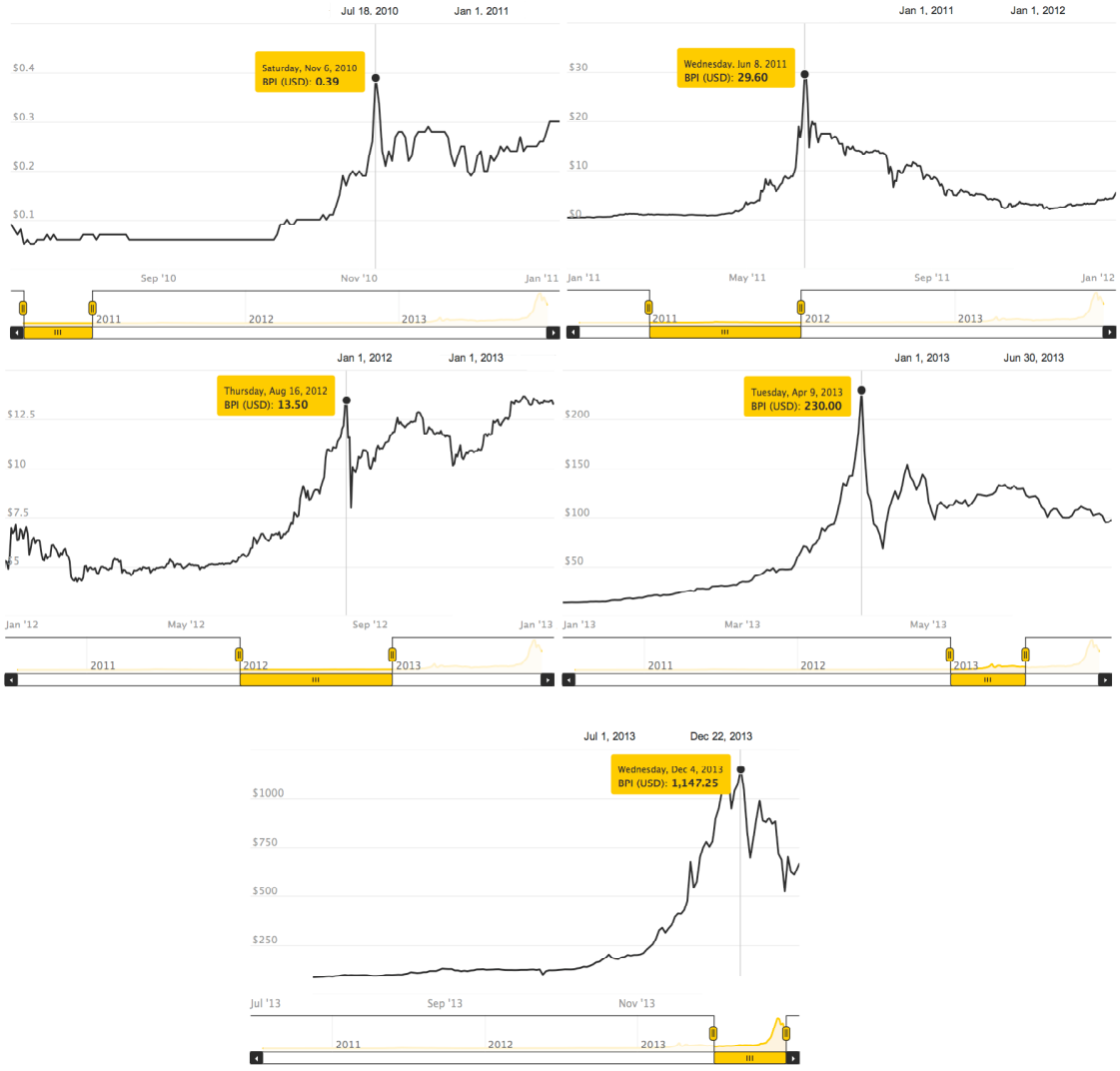
Au premier semestre 2013 on passe de 10 dollars à 100 dollars.

Au second semestre 2013, on passe de 100 dollars à plus de 500 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 dispose de 100, et cela même s'il a manqué de vendre à 200 !

Il semblerait plus sage donc de parler de «bouffée 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. Certains pensent cela inévitable. Est-ce que cette répétition de «fausses bulles» ne devrait pas les faire réfléchir ?



Courbes obtenues grâce à http://www.coindesk.com/price/

Les cinq «bulles» du *Bitcoin*

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 qu'il a dû travailler 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 Etats-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/

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 du l*ivre de compte* (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. L'anonymat pour celui qui y tient n'est donc pas parfait.

Des chercheurs, dont Sergio Lerner, en étudiant le cahier de compte du *Bitcoin* 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 l'ordre d'un milliard 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 brouillages faisant perdre sa trace, comme il s'en développe maintenant. 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

Forces et fragilités des *Bitcoins*

Nouveautés, forces et qualités des *Bitcoins*

- La monnaie *Bitcoins* est basée sur un réseau pair à pair (P2P) et des logiciels libres et gratuits. Elle est donc indépendante de toute banque, n'est soumise à aucune autorité centralisée et offre une transparence complète.

- Les transactions de *Bitcoins* sont rapides et irréversibles (après un délai d'une heure ou moins). Personne ne peut agir sur les *Bitcoins* de vos comptes sans votre consentement, 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 volontaires et 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 vous prenne de l'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 probablement intrinsèquement déflationniste : il prend 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 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, et 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 par vote et donc dans l'intérêt de tous.

Doutes, fragilités et risques des *Bitcoins*

- L'anonymat de Nakamoto l'inventeur et les *Bitcoins* qu'il a gagnés facilement au départ de la monnaie créent un sentiment désagréable et font craindre une combine.

- Aujourd'hui les *Bitcoins* est économiquement tout petit à côté des autres monnaies 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 admis.

- 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 donc suscite la méfiance du plus grand nombre qui ne saisit peut-être pas mieux la façon dont fonctionne vraiment les monnaies classiques dites fiduciaires (voir http://fr.wikipedia.org/wiki/Monnaie_fiduciaire). Le *Bitcoin* est peut-être génial, mais c'est une monnaie de geek !

- Relativement peu de sites et peu de commerçants acceptent les *Bitcoins* aujourd'hui.

- Le *Bitcoin* 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, son cours est très volatil du fait des incertitudes qui l'entourent encore.

- 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.

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

- L'évolution possible des protocoles et programmes —prévue mais au fonctionnement délicat— conduit à la mise en place d'une forme d'administration centralisée constituée par l'ensemble des nœuds les plus puissants du réseau collectif de contrôle. Cela ferait à terme ressembler le *Bitcoins* aux monnaies usuelles dont Nakamoto voulait se démarquer. Sur ce point voir : 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.

Complément 7

Quelques avis tranchés

Contre

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

• 21 octobre 2012, Félix Brezo and Pablo G. Bringas :

Though yet in an underground development phase and, mostly, pretty unknown for the general public, the proliferation of these new payment alternatives brings many uncertainties. What is more, the intrinsic complexity of the protocol and the necessity of having some relatively advanced knowledge on cryptography and computer studies to understand its real behaviour, make these cryptocurrencies the perfect place for speculation and misinformation. For instance, as already stated, there is a widespread belief of the mere fact of using it is sufficient guarantee to perform anonymous transactions, when this is not true by definition.

At the same time, the absence of a regulatory central organism and the chance of not being able to fix the prizes in a explicit way as it happens with the traditional cryptocurrencies, defines a new scenario on an economy strictly ruled by the market movements with all the consequences that this fact leads to in terms of control of massive speculative efforts. At this point, amongst the possible failure scenarios the most urgent for Bitcoin, excepting a dramatical reduction of users which may devaluate the currency once mature, is, precisely, a global governmental campaign against its use.

Just before the end, we can conclude that there is a real risk of a recurrent illegal use of the cryptocurrency. The great number of existing markets and the possibility of exchanging easily bitcoins by euros, pounds or dollars, make this new method the perfect vehicle to perform every kind of transactions related to money laundering or illegal traffic of substances, with all the legal implications associated to the jurisdictional limitation of the criminal acts performed in the cyberspace.

---

http://www.nytimes.com/2013/04/15/opinion/krugman-the-antisocial-network.html?_r=0

• 14 avril 2013, Paul Krugman :

Instead, let's focus on the **two huge misconceptions** — one practical, one philosophical — that underlie both goldbugism and bitbugism.

The practical misconception here — and it’s a big one — is the notion that we live in an era of wildly irresponsible money printing, with runaway inflation just around the corner. It’s true that the Federal Reserve and other central banks have greatly expanded their balance sheets — but they've done that explicitly as a temporary measure in response to economic crisis. I know, government officials are not to be trusted and all that, but the truth is that Ben Bernanke’s promises that his actions wouldn't be inflationary have been vindicated year after year, while goldbugs’ dire warnings of inflation keep not coming

true.

The philosophical misconception, however, seems to me to be even bigger. Goldbugs and bitbugs alike seem to long for a pristine monetary standard, untouched by human frailty. But that's an impossible dream. Money is, as Paul Samuelson once declared, a "social contrivance," not something that stands outside society. Even when people relied on gold and silver coins, what made those coins useful wasn't the precious metals they contained, it was the expectation that other people would accept them as payment. Actually, you'd expect the Winklevosses, of all people, to get this, because in a way money is like a social network, which is useful only to the extent that other people use it. But I guess some people are just bothered by the notion that money is a human thing, and want the benefits of the monetary network without the social part. Sorry, it can't be done.

So do we need a new form of money? I guess you could make that case if the money we actually have were misbehaving. But it isn't. We have huge economic problems, but green pieces of paper are doing fine — and we should let them alone.

---

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

• 14 mai 2013, Laurent Pinsole :

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'Etat 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'Etat 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 quoique 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'Etat qui doit gérer la monnaie.**

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.businessinsider.com.au/if-you-believe-in-bitcoin-you-should-never-buy-anything-in-bitcoin-2013-11

• 11 novembre 2013, Joe Weisenthal :

Remember the pizza that was purchased for $US25 in Bitcoins years back

http://www.businessinsider.com.au/2-million-bitcoin-pizza-2013-4

Had the person not bought that pizza, it would be worth nearly $US 3 million. That purchase was a catastrophic decision, as that was probably the most expensive pizza of all time. Of course this presents a Catch-22. How can Bitcoin become a real currency if it's

not used in transactions? And why would anyone use it in transactions if becoming a real currency offers so much more price appreciation? This contradiction is a core problem, and it's a reason why it's probably doomed to fail (real currencies don't have this issue, since central banks prevent rapid price appreciation, and they mandate that the currency be used). But really, **if you're thinking that Bitcoin is going to be huge, it'd be insane and irresponsible to buy anything with it**.

---

http://www.valuewalk.com/2013/11/bitcoin-news/

• 12 novembre 2013, Elliot Turner :

Bitcoin : the rise and (inevitable) fall.

[...] It is my operating hypothesis that Bitcoin is one such "positive feedback process" which will first lead to a spectacular rise in prices, that will ultimately reverse and crumble into an even more remarkable decline. As it stands today, per my thesis, Bitcoin's "rise" should be in the early stages. This rise has been fueled by a combination of speculation and the promise for the development of actual commerce on Bitcoin. The adoption of broader uses for the currency will be the catalyst for the next stage of ascent. I'm not sure how far Bitcoin can go on the way up, nor am I sure exactly when the inflection point from rise to fall will occur, but one thing I am fairly certain of is that when the fall comes, it will be swift and violent. As they say, "what goes up on an escalator goes down on an elevator" and I would not want to be the one left holding the proverbial bag on the way down.

---

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

• 20 novembre 2013, Benoist Rousseau :

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 Bitcoin 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 délis 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://www.marketoracle.co.uk/Article43356.html

• 30 novembre 2013, Gary North :

Bitcoins are not money.

[...] Here is an economic fact: the number of fools is limited. They are a scarce economic resource. As the price of bitcoins rises, more fools will be lured into the market. But this is a finite market.

In other words, **bitcoins cannot possibly fulfill their supposed purpose: to serve as an unregulated currency unit. Bitcoins are not an alternative currency.** They are something you buy in the midst of a mania, and you will sell at some point in order to get back your money.

You are thinking of buying Bitcoins, not because Bitcoins will serve as a means of exchange, as originally argued, but because you want to get back lots more money than you paid for them. In other words, Bitcoins are not money; dollars are money. There has been no challenge from Bitcoins to the reign of the dollar.

---

http://www.globaltimes.cn/content/829269.shtml#.Up5Mthy9teU

• 2 décembre 2013, Charles Gray :

Bitcoin craze is sure to go bankrupt.

[...] There have been many "virtual currencies," from Dutch tulip bulbs to the collectable cards used in popular games. Without exception, they have all peaked and collapsed, leaving their owners with worthless inventories. The bitcoin craze is unlikely to end any differently, as it is shut down by government intervention, poisoned by criminal involvement, or simply tossed aside for a newer virtual currency. Ultimately, without a stable regulatory foundation and the ability to reliably predict future valuation swings, a virtual currency will simply be an unpredictable investment opportunity rather than a useful circulating currency.

---

http://www.valuewalk.com/2013/12/bitcoin-alternative-payment-system/

• 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 :

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.agoravox.fr/actualites/economie/article/bitcoin-a-vendre-et-surtout-a-144658

• 5 décembre 2013, Laurent Pensolle :

Bitcoin : à vendre, et surtout à interdire !

[...] Le plus incroyable, quand on prend un peu de recul, c'est que les gouvernements laissent faire **ce qui est de facto de la fausse monnaie**, et pire, parfois, l'autorisent, comme en Allemagne.

[...] Du coup, cela ressemble à **un schéma de Ponzi**, où les entrants ne créent aucune valeur. Le système ne tient que parce que les prix montent.

Les Bitcoins posent un triple problème. Ils ne reposent sur rien de concret, à part une puissance de calcul dont le coût est négligeable par rapport à la valeur actuelle. Cette valeur ne repose donc sur rien et n'est que le énième exemple des bulles produites par un marché dérégulé. Ensuite, se pose fondamentalement la question des bénéfices réalisés par cette création. Plus de dix millions de Bitcoins doivent encore être « minés ». Au bénéfice de qui ? Comment se repartira le profit ? Enfin, la monnaie est un service public. Il revient donc à l'Etat d'en avoir la seule responsabilité, dans un cadre démocratique (d'où le scandale des banques centrales dites indépendantes) et d'interdire toute alternative.

Dans quelques années, après quelques bulles et krachs, il est probable que les monnaies virtuelles seront reconnues pour ce qu'elles sont, à savoir de la fausse

monnaie, qui vise aussi à soustraire l'économie du contrôle étatique, et donc démocratique. Alors, les États les interdiront, malheureusement avec retard.

Note (JP Delahaye) : l'auteur commet une erreur en disant que le coût du minage est faible comparé à la valeur des *Bitcoins* gagnés. En fait, le coût du minage s'ajuste à leur valeur par un mécanisme économique qui ne doit étonner personne. Seuls les mineurs utilisant les techniques les plus avancées gagnent parfois de l'argent et cela n'est jamais assuré pour longtemps. En effet, lorsque que c'est le cas, ils sont rejoints par de nouveaux mineurs avec lesquels ils se partagent le *Bitcoins* à gagner, cela jusqu'à ce que le coût du minage rattrape sa valeur sur les marchés.

---

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 :

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**.

---

http://arxiv.org/abs/1312.2048

• 10 décembre 2013, Brian Hanley :

The False Premises and Promises of Bitcoin

Bitcoin makes a number of false claims, including: bitcoin can be a reserve currency for banking; hoarding equals saving; and that we should believe bitcoin can expand by deflation to become a global transactional currency supply. **Bitcoin's developers combine technical implementation proficiency with ignorance of currency and banking fundamentals.**

[...]

Bitcoin's purported capacity for expansion is not credible

But let us forget about that and presume, for the sake of argument, that the USD valuation of each bitcoin rose to approximately $116,600 over the next 5 years as required to match a significant economy in the world. Generating a transactional economic value close to the UK's economy spending virtually all the bitcoins in existence each year would allow us to minimize the required rise in bitcoin valuation. Starting from the valuation of $430 per bitcoin would require bitcoin's valuation to multiply by 271 times over 5 years. That would be a 109% monthly compounded interest rate.

It is impossible to imagine that commercial trade transacted in bitcoins or centi-satoshis would be robust if the valuation were increasing at such rates. No rational player would use bitcoins for spending purposes. Certainly, there are irrational participants in every economy, but it is not in the least credible to believe that virtually every player, from the wealthiest to the poorest would spend large amounts of rapidly appreciating bitcoins every year. Nor is it credible to think that a fraction of players would spend so many bitcoins that their transaction volume would approach the necessary GDP through high velocity of money through the system. Without one or the other, the level of appreciation required to allow bitcoin to support an economy of a mid-size nation would be far higher. A higher rate of appreciation means an even greater incentive to hoard, which further decreases the credibility of bitcoin supporting actual commerce.

Consequently, it is impossible to imagine that the user base for bitcoins used in commerce could enlarge enough to drive such a valuation increase. **The valuation of bitcoin will always be determined by speculation, not by utility for spending**. It is believable

that motivated transactors will continue make use of bitcoin as an alternative for a black and grey-market payment system, although regulators and law enforcement are making that more difficult. However, what will drive speculation is the creation of an enlarged, or simply wealthier, speculator pool.

There may be a useful place for alternative forms of electronic money. However, an improvement requires study of money, financial institutions, finance history, and understanding of how and why our system works as it does today. **At best, bitcoin is an unintentional throwback to pre-medieval finance**

---

http://arxiv.org/abs/1312.2048

• 10 décembre 2013, Brian Hanley, citation :

G. Gardiner, "What bitcoin is," B. Hanley, Ed., ed. email, 2013 :

[Bitcoin is]…a very clever practical joke by someone who is having enormous fun exposing in the most sophisticated way imaginable the naivety of clever mathematicians, economists and/or rich speculators. ... or ... The cleverest con trick ever conceived, and probably one of the most rewarding.

---

http://reflets.info/le-saviez-vous-le-bitcoin-va-disparaitre/

• 10 décembre 2013, Kitetoa :

Le saviez-vous, le Bitcoin va disparaître.

[...] Dans un avenir plus ou moins proche, les banques centrales vont estimer que la masse monétaire représentée par le Bitcoin (aujourd'hui environ 8,5 milliards d'euros) est trop importante et fausse leur mesure de la masse monétaire ou son contrôle. Elles décideront alors de manière concertée que le Bitcoin ne vaut plus rien. Et toutes les institutions financières seront contraintes de ne plus convertir cette devise. Deux inconnues dans cette équation. La date et le volume (le montant) qui fera tiquer les banques centrales. **En d'autres termes, plus le Bitcoin a une valeur élevée, plus le risque est grand qu'il ne vaille plus rien.**

---

http://www.forex.fr/newslist/6814-qui-osera-dire-apres-cela-que-le-bitcoin-nest-pas-un-marche-manipule

• 11 décembre 2013, Claire Boyer :

Qui osera dire après cela que le Bitcoin n'est pas un marché manipulé ?

Les fortes fluctuations sur le Bitcoin des derniers mois ne traduisent pas seulement l'intérêt croissant des investisseurs particuliers pour ce nouveau marché. Elles sont plutôt le signe de l'existence d'**un cartel de prix**, une poignée d'investisseurs détenant l'essentiel des Bitcoins en circulation et imposant leurs prix au reste de la communauté Bitcoin.

C'est la thèse que semble confirmer l'estimation produite par l'entrepreneur finlandais Risto Pietilä, membre actif de Bitcointalk.org. A partir de données publiques disponibles sur Bitcoinrichlist.com, il a estimé qu'**environ 927 personnes détiennent près de la moitié des Bitcoins en circulation**, ce qui représente près de six millions de Bitcoins.

[...] **Tous les traders qui envisagent de spéculer sur le Bitcoin doivent bien prendre conscience que le prix de cette monnaie virtuelle n'est que la manifestation de la volonté d'une poignée de teneurs de marché dont les intérêts sont difficiles à cerner.**

Bulle spéculative, le Bitcoin l'est incontestablement. Monnaie du futur en passe de concurrence le dollar américain ou l'euro, c'est peu probable tant que le Bitcoin fait l'objet

de critiques de toute part. Il aura, au final, seulement permis à un petit cercle de spéculateurs talentueux de s'enrichir encore plus au détriment de la cohorte de particuliers qui a cru, à tort, pouvoir devenir riche avec le Bitcoin.

---

http://www.internetevolution.com/author.asp?section_id=625&doc_id=270367&f_src=internetevolution_gnews

• 12 décembre 2013, Mitch Wagner :

Ambition is usually a virtue. But it's Bitcoin's biggest problem.

When I first started taking Bitcoin seriously a few months ago, I agreed with advocates who thought Bitcoin was revolutionary, as big as the Internet, and likely to replace existing forms of money in huge swathes. But **the more I looked into it, the more I became convinced of the opposite: Bitcoin is a fad. It serves no practical purpose other than as a tool for financial speculation.** Conventional currency is better for all legal transactions. And even crooks are better off using cash. In special circumstances, portable valuable property such as gold, fine art, or jewelry make a fine place to store your value.

France-Culture Emission, L'économie en question : http://www.franceculture.fr/emission-l-economie-en-questions-economie-sociale-solidaire-et-circulairebitcoin-monnaie-virtuelle-2

• 14 décembre 2013, Olivier Pastré :

Vous pouvez rencontrer les commercants dans les cafés, vous leur donnez de l'argent en monnaie sonnante et trébuchante et ils vous donnent des bitcoins. [...]

Le bitcoin, c'est Madoff, ça s'appelle une pyramide de Ponzi, et ça va se casser la gueule [...] C'est amusant, mais c'est uniquement 3 milliards de dollars.

Note (JP Delahaye) : Dans une émission consternante, les intervenants parlent du Bitcoin et montrent avec application qu'ils ne le comprennent pas. Pour ces économistes vedettes des media —Benjamen Coriat, Olivier Pastré, Dominique Pilhon, David Thesmar— professeurs prestigieux et grands donneurs de leçon, la chose est totalement mystérieuse. Olivier Pastré qui (comme le montre la citation ci-dessus) sait bien ce qu'est le Bitcoin fait exception, et nous dit que c'est «très simple». La question que se posent nos experts est : pourquoi ceux qui ne gagnent pas de l'argent en produisant les bitcoins «avec des algorithmes de plus en plus compliqués» acceptent-ils d'entrer dans son jeu dont, de toute évidence, ils sont les perdants ?
Il semble souhaitable d'introduire des cours de cryptologie dans les cursus universitaires français d'économie et de finances : ils seront utiles aux étudiants... et à leurs professeurs.

---

http://www.businessinsider.com/williams-bitcoin-meltdown-10-2013-12

http://www.businessinsider.com/beware-of-bitcoin-2013-12

• 17 décembre 2013, Mark Williams :

Since inception, **Bitcoin has had a flawed DNA**. It was dreamed up in a virtual world -- by computer geeks - but was to be applied in the real world. **Bitcoin is steep in Libertarian and anti-Fed dogma but weak in understanding of how global economics, central banking policies and financial markets function.** The lifeblood of the global capital markets is money – greenbacks -- transactional currency that facilitates commerce. Virtual currency can create value and efficiency but it needs to be linked to fiscal and monetary policy. To assume currency can be computer generated, run in a decentralized manner and outside of the central banking system and controls is farcical and economically dangerous.

[...] Bitcoin lacks the essential attributes that are needed to support a widely recognized transactional currency. If Bitcoin was allowed to proliferate as a currency it would produce greater economic uncertainty, reduced trade and lower individual standard of living.

Bitcoin has not taken off as a transactional currency and is further undermined by the fact that the majority of Bitcoin owners hoard e-coins. The more hoarded the less available to buy goods and services and spur economic growth.

In Bitcoin World it is not uncommon for prices to change by 20 or 30 percent in a given day, making Bitcoin toxic to economic growth. Price swings produce conflicting behavior. Retailers work on tight margins, sometimes as low as 10 percent. Such daily price fluctuations would eliminate all profit and inflict needless losses. Unless retailers want to be in the commodity trading business, they would not be interested in taking Bitcoin risk. At restaurants, Bitcoiners expecting coin values to drop might rush to pay for dinner even before the first entree arrives while restaurateurs would be motivated to delay payment until the drop occurred. If Bitcoin owners believe value would increase, they would hoard more coins and velocity of money would decline, harming economic growth.

In this Bitcoin World of currency uncertainty, guessing and risk, commerce would decline and bartering would increase. Naturally, as Bitcoin price swings increased, the number of businesses willing to accept e-currency risk would decline. This is why in recent weeks, as large price movements have occurred, we have seen more credible retailers saying "No" to Bitcoin.

[...] Bitcoin has seen an end to its hyper price run-up and can no longer support being priced for perfection. **Unlike gold which has tangible value, Bitcoin is backed by hopes/dreams and only worth what people are willing to pay**. As it becomes increasingly evident that Bitcoin will not be the global currency standard, but simply a novel idea that will be improved upon by more nimble competitors such as Litecoin, restrictions and new regulations will be imposed and prices will plummet.

I predict that Bitcoin will trade for under $10 a share by the first half of 2014, single digit pricing reflecting its option value as a pure commodity play. Miners/speculators will be best served to acknowledge the meltdown has begun, act quickly and take fleeting profit off the table.

---

http://www.latribune.fr/bourse/actualite/20131216trib9fabbb847/clap-de-fin-pour-le-bitcoin.html

• 18 décembre 2013, La Tribune (Article partenaire "Forex") :

Clap de fin pour le Bitcoin?

[...] Alors qu'elle n'était cotée qu'autour de 12 dollars l'an dernier à la même époque, la monnaie digitale a depuis franchi le cap des 1 000 dollars avec allégresse, mais connaît des fluctuations totalement anormales, parfois de 20% à 30% en une seule séance, ce qui fait dire à de nombreux experts qu'en l'état actuel, le Bitcoin ne possède pas la stabilité nécessaire pour concurrencer un jour les devises émises par les banques centrales.

La formation d'un cartel des prix a même été évoquée par certains spécialistes, ce qui pourrait expliquer en partie les fluctuations du cours. À défaut de preuve formelle, **tous les analystes sont d'abord au moins sur le fait que le Bitcoin est une gigantesque bulle spéculative**.

La survie du Bitcoin dépendra étroitement de sa capacité à s'imposer massivement et à acquérir la crédibilité nécessaire auprès des utilisateurs comme moyen d'échange et de paiement, à l'instar du dollar ou encore de l'euro. Sans réelle valeur intrinsèque, le Bitcoin demeure un objet financier mal appréhendé et qui devra passer par l'étape de la régulation pour espérer devenir une monnaie virtuelle pérenne.

L'engouement pour le Bitcoin n'est toutefois pas isolé et peut, dans une certaine mesure, être considéré comme une évolution presque normale à l'ère du numérique. Toutes les monnaies virtuelles, dont Litecoins, ont connu de fortes hausses ces derniers mois. Sans commune mesure cependant avec le phénomène Bitcoin. À terme, les autorités nationales

seront certainement contraintes d'adopter aussi une attitude plus compréhensive vis-à-vis des monnaies virtuelles afin de les intégrer aux moyens de paiement traditionnels.

Il reste peu probable que le Bitcoin soit encore là lorsque cela surviendra. **Après les nombreux déboires de la monnaie virtuelle et la défiance croissante des utilisateurs, on est certainement proche du clap de fin pour le Bitcoin.**

---

http://www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html

• 18 décembre 2013, Charlie Stross :

To editorialize briefly, BitCoin looks like it was designed as a weapon intended to damage central banking and money issuing banks, with a Libertarian political agenda in mind—to damage states ability to collect tax and monitor their citizens financial transactions. Which is fine if you're a Libertarian, but I tend to take the stance that Libertarianism is like Leninism: a fascinating, internally consistent political theory with some good underlying points that, regrettably, makes prescriptions about how to run human society that can only work if we replace real messy human beings with frictionless spherical humanoids of uniform density (because it relies on simplifying assumptions about human behaviour which are unfortunately wrong).

---

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

• 18 décembre 2013, Alex Payne :

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 :

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 Etat 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://www.businessinsider.com/two-tragic-facts-about-bitcoin-mining-2013-12

• 22 décembre 2013, Rob Wile :

Thirteen years ago, Stanford researchers created a program that allowed anyone in the world to help solve diseases simply by running their computers. Called Folding@home, the program enables you to perform calculations on your idle computer that are needed to do research into protein folding. This research is important because when proteins mis-fold, cancer, Alzheimer's and Parkinson's can result. So far, 6.3 million CPUs have contributed 18 petaFLOPS of computation, resulting in 109 peer-reviewed articles describing various breakthroughs, big and small, in managing those diseases.

Bitcoin the digital currency, is about four years old. But the amount of computing power that currently goes into mining Bitcoin, which are created by unscrambling complex strings of encrypted numbers, now stands at 110.6 petaFLOPS. So if we apply the amount of computing power now being devoted to Bitcoin mining to Folding@home, we could now be pumping out 666 peer-reviewed papers about chronic diseases.

There's more. Another mass computing program, called Einstein@home, is designed to detect gravitational-wave emissions from spinning neutron stars. The project seems to have gone into partial hibernation. But as of 2010, it had compiled less than a full petaFLOPS' worth of computations to detect 2 new pulsars, which indicate the presence of neutron stars and allow astronomers to study the behavior of matter at nuclear density.

So on our same 110.6 petaFLOPS, we could have found at least 221 new Pulsars.

BI contributor John Aziz has discussed the moral implications of these kinds of calculations, finding them at ambiguous at best. But it seems fair to state that if you're considering devoting resources to Bitcoin mining, you may want to keep these numbers in mind.

---

http://arstechnica.com/business/2013/12/crazy-currency-the-more-i-report-on-bitcoin-the-weirder-it-gets/

• 24 décembre 2014, Cirus Farivar :

"**It's play money in the virtual casino**," James Angel, a business professor at Georgetown University, told me earlier this year. "Everybody else is trying to outguess each other. Bitcoin has turned into a very large multiplayer online game in which everybody is trying to out speculate each other."

Bitcoiners famously like to talk about the fact that like most modern currencies (like the US dollar or the euro), it's a fiat currency. It essentially works on faith. There's nothing inherently valuable about a piece of computer code more than a piece of green paper. We know that $1 is worth $1 because that's what we've decided as a society. I get paid in dollars, and I can buy stuff with dollars. There are shops on the Internet and in real life that will take my physical paper dollars and my digital (debit/credit card) dollars. We have an innate sense of what things are worth because of it. By contrast, precious metals like silver and gold also have inherent worth too, but that's more due to their industrial and aesthetic properties. Bitcoins are physically just bits of code.

"Even if there is a speculative element [with traditional commodities], at the end of the day you expect the price to have a gravitational pull towards the true value," Angel added. "We have models for valuing stocks and bonds, so we can get a sense of what it's worth. But **I really have no way of figuring out what a bitcoin is worth**. Sure, I can go to exchanges and see what the current price is, but how do I know that that price tells me anything? If I look at the price of the euro, I know what I can buy with euros. I know how many euros it takes to get a Big Mac in Paris or a hotel room in Frankfurt. We have this idea called 'purchasing power parity' that says that sooner or later exchange rates should reflect prices across different exchanges. We don't have that with bitcoin."

Plus, he added, traditional commodities like gold, oil, wheat, and others have practical value beyond their monetary value. Gold can be used as jewelry or manipulated industrially to manufacture semiconductors. Oil can be used to power machinery or refined for gasoline. Bitcoins have zero inherent utility.

Now, you can take the opinion that bitcoin is more like a fiat currency like the US dollar—which isn't based on anything either (we went off the gold standard decades ago). **However, the dollar has a massive infrastructure designed to regulate and safeguard its function** as a currency through institutions like the Federal Reserve, the Treasury Department, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and other entities. **Bitcoin has none of these**, which has proven to be both its greatest asset and its greatest liability.

---

http://www.truthdig.com/report/print/bitcoin_and_the_dangerous_fantasy_of_apolitical_money_20131226

• 26 décembre 2013, Yanis Varoufakis :

Bitcoin and the Dangerous Fantasy of 'Apolitical' Money

[...] The reason money is and can only be political is that the only way of steering a course between the Scylla and Charybdis of dangerous ponzi growth and stagnation is to exercise a degree of rational, collective control over the supply of money. And since this control is bound to be political, in the sense that different monetary policies will affect disparate groups of people differently, the only decent manner in which such control can be exercised is through a democratic, collective agency. **In brief, while apolitical money is a dangerous illusion, a Central Bank that is democratically controlled (as opposed to the indefensible notion of an 'independent' Central Bank) remains our best hope for a form of money that is for the people and by the people.** Bitcoin, despite its many interesting features, can never be that.

---

http://equitablegrowth.org/2013/12/28/1466/watching-bitcoin-dogecoin-etc

• 28 décembre 2013, Brad DeLong :

Now suppose that you were on the Internet and it is the early 21st century…

You want to get richer. You can either work doing something useful, or you can set up a botnet to mine BitCoins, or you can fork the code behind BitCoin and set up your own slightly-tweaked virtual cryptographic money network. Setting up a new, alternative network is really cheap. **Thus unless BitCoin going can somehow successfully differentiate itself from the latecomers who are about to emerge, the money supply of BitCoin-like things is infinite because the cost of production of them is infinitesimal.**

How can BitCoin successfully keep itself differentiated from the latecomer copiers?

By asserting, over and over again, simply that it was first. And this might work. But I am skeptical.

By stressing that it has a trustworthy track record of being a safe store of value–and thus appealing to a history that the latecomers do not have. This works until someday, for some reason, demand for BitCoins falls. Then supply and demand drives the value down. BitCoin is then no longer differentiated as a safe store of value. Then the people who were holding BitCoin because they thought it was a safe store of value dump it, its price falls even more, and so it becomes even more questionable as safe store of value. And the downward spiral continues.

[...] In my view, BitCoin's chances would be a lot better if there were some large and durable entity that promised to be a BitCoin sink if necessary. If, say, Google Cayman Islands were to start GoogleCoin, and announce that it would always stand ready to buy back **GoogleCoins at a fixed real value, it could make a (small) fortune and, I think, eliminate BitCoin's business in a month**…

---

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

• 28 décembre, Paul Krugman :

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://nypost.com/2013/12/28/bitcoin-a-modern-day-3-card-monte/

• 28 décembre, Jonathan Trugman :

Each year, new financial scams pop up in which unsuspecting investors get fleeced by crooks and con artists.

Five years ago, it was Bernie Madoff.

This year, it was a barrage of insider trading. And next year, one way or another, the bitcoin flimflam will come to a head (or a tail).

The Tinkertoy "crypto-currency" is nothing more than a modern-day game of three-card monte, with a little Sudoku thrown in, just to add a touch of mystique.

In 2013, thousands of people became convinced they had to get in on bitcoin before it changed the flows of capital around the world. Like most schemes of dubious merit, the sexy intrigue of incalculable calculus combined with no central oversight suckered them in.

---

http://marginalrevolution.com/marginalrevolution/2013/12/how-and-why-bitcoin-will-plummet-in-price.html

• 30 décembre 2013, Tyler Cowen :

Once the market becomes contestable, it seems the price of the dominant cryptocurrency is set at about $50, or the marketing costs faced by its potential competitors. And so are the available rents on the supply-side exhausted.

There is thus a new theorem: the value of [B]itCoin should, in equilibrium, be equal to the marketing costs of its potential competitors.

This theorem will hold even if you are very optimistic about market demand and think that grannies will get in on it. In fact the larger the network of demanders, the lower the marginal marketing cost may be — a bit like cellphones — and that means even lower valuations for the dominant cryptocurrency.

In short, we are still in a situation where supply-side arbitrage has not worked its way through the value of Bitcoin. And that is one reason — among others — why I expect the value of Bitcoin to fall — a lot.

---

http://www.bloomberg.com/news/2013-12-31/bitcoin-is-a-high-tech-dinosaur-soon-to-be-extinct.html

• 31 décembre 2013, Stephen Mihm :

Bitcoin Is a High-Tech Dinosaur Soon to Be Extinct

[...] Anyone who thinks that Bitcoin will triumph has to believe that it will succeed where earlier generations of private currencies failed -- that Bitcoin will, improbably, manage to overthrow more than century's worth of accumulated state power, jealously guarded and ruthlessly enforced.

That's a preposterous fantasy - and a dangerous one, if you're an investor. **Indeed, people who believe that governments of the world will let a stateless cryptocurrency usurp their hard-won monetary prerogatives aren't forecasting the future. They're living in the past.**

---

http://techcrunch.com/2014/01/01/why-i-lost-faith-in-bitcoin-as-a-money-transfer-protocol/

• 1 janvier 2014, Romain Dillet :

Why I Lost Faith in Bitcoin As A Monay Transfer Protocol

[...] As long as Bitcoin remains a young and volatile currency, Bitcoin's mechanisms will remain beautiful on paper. Using it for real world transactions would be crazy, and I think we are still a couple of years away from getting a stable Bitcoin that can be trusted. Until then, using Bitcoin will remain a wild ride — it's definitely fun, but don't take Bitcoin seriously just yet.

---

http://www.bloomberg.com/news/2014-01-02/bitcoin-is-an-expensive-way-to-pay-for-stuff.html

• 2 janvier 2014, Matt Levine :

Bitcoin Is an Expensive Way to Pay for Stuff.

[...] As of today miners took home about 3.5 percent of the value of transactions that they processed. Which is more than credit card companies! Though maybe less than Western Union [...] The claim that Bitcoin could one day provide a low-transaction-cost alternative (or currently provides an anonymous or accessible alternative) to the U.S. dollar payments system is separate from the claim that Bitcoin is currently a cheaper, or free, payments alternative. **Bitcoin, as a transaction mechanism, is actually pretty expensive! It's just that it's clever at hiding its costs.**

---

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

• 13 janvier 2014, Avinash Persaud

[...] Bitcoin is a cryptographer's wet dream rather than a useful monetary system. While bitcoin supporters tap into an understandable reaction against bankers and claim it is a decentralized and democratic system of money, it so happens to give a built-in advantage to those with the biggest code-breaking capacity. It has a deflationary bias with all the adverse repercussions of that that the policy of quantitative easing is trying to avoid. And like everything else **it is not "unhackable".** 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. Last year in the US, FBI shut down "Silk Road", an online black market, and seized $28 million worth of bitcoins. This will be its undoing. After 9/11, the authorities have become far tougher in trying to crack down on the financing of illegal activities through anti-money laundering rules that require banks to know the source of funds being transacted. Bearer bonds or shares, for instance, where the owners are not registered anywhere but merely those who hold them, were once extremely popular, but today can no longer be used in the banking system as a method of payment or collateral or pledges. Bitcoin is just like a bearer bond. **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 :

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.contrepoints.org/2011/07/08/33982-bitcoin-une-monnaie

• 8 juillet 2011, Stéphane Geyres :

Les monnaies traditionnelles, l'or en tête, n'étaient pas sans défaut non plus. Les pièces d'or s'usent, les fondeurs peuvent tricher sur leur poids et les confier à une banque pose le risque de la contrefaçon des certificats de dépôt. L'adoption d'une monnaie reste donc toujours un choix guidé par une prise de risque, entre la confiance accordée en une monnaie pratique et de grande fiabilité et la possibilité marginale mais toujours présente d'inflation par contrefaçon. **BitCoin et les autres monnaies virtuelles ne font pas exception. Elles présentent de très nombreux avantages, à commencer par l'indépendance des banques centrales, ce qui de nos jours est sans doute l'argument majeur.** Mais il faut être lucide et bien se rendre compte que si elles rencontrent le succès, elles rencontreront aussi les assauts des pirates et malfrats de tous poils et risquent donc disparaître en un clin d'œil et sans contrepartie matérielle, ruinant au passage leurs détenteurs. Peut-être faudra-t-il qu'il en existe des milliers de différentes, en concurrence permanente, pour qu'aucune ne devienne dominante au point d'en être fragilisée. **L'avantage d'une monnaie libre sur un marché libre, c'est que c'est le marché qui trouvera tout seul la solution. Vive la monnaie libre.**

---

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

• 20 janvier 2012, Pierre Noizat :

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 Etats-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'Etat, 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 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.

---

http://luc.edu/media/lucedu/law/students/publications/clr/pdfs/kaplanov.pdf

• 29 novembre 2012, Nikolei Kaplanov :

The final reason to resist prohibiting or even inhibiting bitcoin lies in the fundamental concept of the Internet itself. Allowing bitcoin to operate unfettered by substantial regulation allows it to contribute towards job creation, economic growth, and opportunity. By letting the market determine whether or not bitcoin should survive is preferable to federal policy seeking to shut it down.

[...] Complaints against government control of currency have been present in the United States and in other countries throughout history. While alternative currencies have offered some respite for those who want a choice in their medium of exchange, these have still been controlled by some central authority and have generally been limited to a specific region or area. Bitcoin, on the other hand, is the unique confluence of technology and demand allowing it to become a viable, global alternative currency. Functioning much in the same manner as cash, Satoshi Nakamoto's ideas have created over thirty million dollars' worth of bitcoins without the need for a government issuer or a third party transaction network.

This Comment maintains that the traditional bitcoin users buying and selling goods in a cash-like transaction, as well as bitcoin miners, fall outside of the regulatory provisions under federal banking, money transmission, and securities laws. Instead, bitcoin transactions should be treated as a community currency under the law, receiving full contractual enforcement and being treated as a traditional currency in every other way.

Despite genuine concerns relating to bitcoins and criminal activity, this Comment argues against any prohibition by policymakers or judges that encounter bitcoins. Instead, law enforcement should become familiar with the technology, especially since bitcoin provides a public log of every transaction, and use existing tools to investigate and prosecute illegal activity. **Trying to prohibit bitcoin or another bitcoin-like currency would only be problematic. On the other hand, allowing bitcoin to flourish, as the law currently provides, can provide limitless possibilities in commerce around the globe.**

---

http://www.contrepoints.org/2013/04/13/121461-savez-vous-ce-quest-le-bitcoin

• 13 avril 2013, David Graham :

Il y a une c hose particulière à propos de bitcoin : il est basé sur les mathématiques, et aucune organisation ne le contrôle. Même si le gouvernement met des sites publics comme MtGox en faillite, et jette son propriétaire en prison, les transactions en bitcoin transactions continueront. Et vous pouvez même avoir l'effet inverse : plus le gouvernement s'acharne à détruire les monnaies concurrentes, plus un bitcoin deviendra cher, puisque seule monnaie que le gouvernement ne peut pas stopper. Il y aura toujours une très forte demande pour une monnaie souterraine, non gouvernementale qu'aucun gouvernement ne peut écrabouiller avec succès.

Philippe Herlin, La révolution du Bitcoin et des monnaies complémentaire, Editions Eyrolles, 2013

• Mai 2013, Philippe Herlin :

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, oeuvres 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.atlantico.fr/decryptage/entre-flamblee-cours-et-interdiction-quel-avenir-pour-bitcoin-philippe-herlin-836114.html

• 11 septembre 2013, Philippe Herlin :

Aujourd'hui, à un cours de 100 euros, la totalité des bitcoins en circulation (11 millions actuellement) "pèse" environ un milliard d'euros. C'est peu par rapport au futur que l'on peut imaginer pour cette monnaie. Le bitcoin permet en effet des transactions et des virements transfrontaliers à un tarif imbattable, largement inférieur aux cartes bleues, Paypal ou autre Western Union. Les perspectives sont gigantesques et on peut prévoir d'autres bulles suivies d'un krach, mais avec un bitcoin qui vaudra plus cher après qu'avant, dessinant ainsi une croissance en escalier.

[...] Les États et les banques centrales n'aiment pas le bitcoin parce que cette monnaie leur échappe complètement. **Mais nous, citoyens, au nom de quoi devrions-nous être totalement dépendants de l'euro, ou ailleurs du dollar ou du yen, qui sont des "monnaies-papiers" largement manipulées** (taux d'intérêt fixé à zéro, planche à billets ou Quantitative easing), des monnaies qui de ce fait perdent de leur valeur ? Au nom de quoi rester prisonnier d'un système bancaire qui continue de jouer avec le feu ? Le bitcoin (ou l'or si on lui permettait de redevenir une monnaie) permet d'acquérir de nouvelles libertés et une nouvelle indépendance. L'Allemagne, historiquement attachée aux monnaies "saines" l'a compris en légalisant l'usage du bitcoin, espérons que l'Europe suive.

---

http://www.libe.ma/L-alternative-Bitcoin_a42490.html

• 26 septembre 2013, Martin Vlachynsky :

Qu'est-ce qui empêche Bitcoin d'être une monnaie à part entière ? Il exige des compétences plus techniques que les espèces et les opérations bancaires traditionnelles. Il exige encore plus de connaissances lorsqu'il s'agit de maintenir les transactions réellement anonymes. Cela représente un coût pour les utilisateurs potentiels et réduit considérablement leur nombre.

Néanmoins, Bitcoin trouve des utilisateurs même parmi les pauvres et ceux qui ont un faible niveau d'éducation, et il est devenu populaire dans nombre de pays africains. Avec des restrictions croissantes sur les envois de fonds vers les pays blacklistés, comme la Somalie, Bitcoin offre une solution pour ceux qui ont besoin d'envoyer des revenus au pays à des parents désespérés.

Les récentes mesures sévères contre les échanges de Bitcoin de la part d'organismes américains (par exemple, la saisie de plusieurs millions de dollars sur la plus grande plateforme d'échange Bitcoin, MT.Gox, qui a temporairement cessé ses opérations en dollars américains) et les efforts allemands plus subtils pour introduire Bitcoin dans le domaine financier officiel sont les étapes initiales de la prochaine lutte acharnée entre les Etats et les utilisateurs de Bitcoin. Les autorités vont probablement essayer de le contrôler ou de le supprimer en imposant des coûts plus indirects sur les utilisateurs. Certains vont

accepter les coûts et jouer selon les règles. Mais nous pouvons nous attendre à une réaction sous la forme d'innovations qui améliorent l'anonymat et la convivialité.

Il est difficile de prédire si Bitcoin va croître ou disparaître, parce qu'il serait devenu une monnaie virtuelle réglementée et donc ennuyeuse. Mais le projet est déjà un succès. Il s'agit d'une expérience pionnière qui démontre qu'une foule est capable de créer et de maintenir jusqu'ici des canaux d'information privés décentralisés de haute technologie. Bitcoin n'est qu'un exemple de ce nouveau phénomène. On en trouve d'autres : le réseau décentralisé peer-to -peer (P2P), TOR (pour l'anonymat en ligne) et l'impression 3D. Tous offrent des outils modernes pour lutter contre Big Brother, qui est équipé de quelques outils modernes lui-même.

Il est trop tôt pour prédire si ces outils vont garantir la propagation de la liberté à travers le monde. Mais ils vont certainement contribuer à donner un coup de pouce à l'effort dans ce sens.

---

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 Lee :

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://money.cnn.com/2013/12/04/technology/bitcoin-libertarian/

• 4 décembre 2013, Jose Paglieri :

"There will be alternatives to the dollar, and this might be one of them," said former U.S. congressman Ron Paul. If people start using bitcoins en masse, "it'll go down in history as the destroyer of the dollar".

---

http://www.theverge.com/2013/12/5/5178536/bank-of-america-says-bitcoin-could-become-a-major-means-of-payment

• 5 décembre 2013, Adrianne Jeyffries :

Analysts at Bank of America Merrill Lynch issued the bank's first research report

(https://www.documentcloud.org/documents/885843-banks-research-report-on-bitcoin.html)

today on Bitcoin, the virtual currency that approximates cash on the internet, concluding that the currency has the potential to become a "major means of payment for ecommerce" as well as a "serious competitor to traditional money transfer providers." Assuming Bitcoin becomes mainstream, Bank of America currency strategists estimate it is worth $1,300 apiece. But with the value at $1,000 today and increasing rapidly, it is in danger of "running ahead of its fundamentals," they write.

---

http://www.contrepoints.org/2013/12/06/149012-bitcoin-la-banque-de-france-decouvre-un-concurrent-comme-une-poule-un-couteau

• 6 décembre 2013, *h16* :

Panique dans le petit monde des banques centrales : le Bitcoin qui était jusqu'à présent probablement vu par elles comme une expérience un peu bizarre d'adolescents boutonneux commence à prendre une ampleur difficile à ignorer. Si les premiers réflexes furent l'indifférence, la récente publication d'un petit PDF

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

de la Banque de France montre qu'on est maintenant passé à la peur.

Dans ce que certains, n'ayant pas peur du ridicule ou faisant preuve d'un humour corrosif, osent appeler analyse, la vénérable institution bancaire française nous décrit toutes les vilaines tares de la crypto-monnaie. Elle constate ainsi que c'est une monnaie non régulée, c'est-à-dire répondant exclusivement aux besoins du marché et non aux petites lubies politiques. On peut trouver cet argument étrange surtout lorsqu'il est en partie couvert par le bruit ronflant des rotatives de la même Banque de France qui crache des euros en papier signés Draghi que personne ne semble pouvoir arrêter de produire.

Autre grief : cette vilaine monnaie alternative ne garantirait aucun remboursement lors d'un achat, serait utilisée par des mafieux, peut être refusée lors d'un achat par un commerçant suspicieux (si, cela existe !) et surtout, alimenterait la spéculation. Il est vrai que le non remboursement lors d'un achat en euro, cela ne s'est jamais vu, que les billets de 500€ ne sont jamais utilisés par les gangs de trafiquants divers, que ces mêmes billets sont acceptés partout en zone Euro (mais si, c'est l'article 642-3 du Code pénal qui le dit, et d'abord on ne peut pas le refuser nan mais), et qu'il n'y a actuellement aucune spéculation à la hausse ou à la baisse sur l'euro comparé au dollar, au yen ou à la livre anglaise. Vraiment, ce bitcoin est très particulier.

Bien évidemment, le but du papier est d'alimenter des petits sentiments de confusion et de crainte, sentiments qu'on pourrait retrouver de façon semblable dans le dépliant promotionnel d'un vendeur de tapis lorsqu'il évoque un concurrent. En substance, la Banque de France nous rappelle que le seul tapis qui vaille, c'est celui qu'elle vend parce qu'il est garanti par la bonne qualité de la production : la tonte vigoureuse et régulière des moutontribuables permet de produire une laine de si belle qualité qu'elle est impossible à égaler pour tout concurrent. Soyons sérieux. [...]

Encore une fois, ces réactions sont intéressantes par ce qu'elles montrent : un assez consternant manque de curiosité et de culture de la part de ceux qui se permettent d'émettre un avis, sans même parler d'un recul critique qui leur permet de coller sur le dos du Bitcoin des défauts évidents des monnaies étatiques actuelles. Mieux : ces réactions illustrent très bien que certains commencent à comprendre le danger de l'effondrement du monopole monétaire. On est d'ailleurs dans l'exacte symétrie comportementale avec ce que nous avons pu observer de la part des Majors du monde musical à l'apparition du MP3 et des partages musicaux type Napster, dans les années 2000. Pour rappel, les Majors ont, de fait, perdu le monopole de la distribution et chaque année qui passe voit la distribution par internet et la dématérialisation gagner des parts sur les anciens modèles. On doit aussi comprendre que cette perte de statut dans l'industrie musicale ne s'est pas

faite sans violence de la part de ces vieilles entreprises.

On n'aura donc pas de mal à imaginer la violence à laquelle recourront les États lorsqu'ils sentiront, eux aussi, le pouvoir leur échapper. Attendez-vous au pire. Mais quoi qu'il arrive à présent : le chat est sorti du sac. Des millions d'individus savent que les crypto-monnaies peuvent fonctionner et ont cette valeur inestimable d'être libres et indépendantes de l'État.

---

http://www.lesnumeriques.com/bitcoin-rupture-technologique-avant-tout-a1758.html

• 6 décembre 2013, Gonzague GrandVal :

En phase de découverte, ce phénomène de spéculation est assez naturel et on ne peut l'empêcher. Mais plus le bitcoin va gagner en notoriété, plus il sera utilisé chez les marchands et plus les choses vont se stabiliser.

---

http://www.contrepoints.org/2013/12/07/149015-pourquoi-les-banques-entrent-en-guerre-contre-le-bitcoin

• 7 décembre 2013, Mark Maunder :

Dans l'économie Bitcoin, la déflation est au cœur de la devise. Cela signifie que c'est une très mauvaise idée d'emprunter de l'argent en Bitcoin parce que vous devrez de plus en plus au fur et à mesure que le temps passe et que vous ne serez jamais en mesure de le rembourser. En revanche, si vous ne vous endettez jamais et que vous décidez d'épargner, l'argent que vous conservez vaudra un peu plus chaque jour.

C'est un cauchemar pour les banques parce qu'elles veulent que vous empruntiez toujours plus afin que vous payiez des intérêts sur vos emprunts. Elles veulent ainsi maintenir un écart entre les intérêts que vous payez, et ceux qu'elles paient pour emprunter l'argent qu'elles vous ont prêté.

C'est un plus grand cauchemar encore parce que les banques veulent que vous ouvriez un compte d'épargne et y déposiez de l'argent afin que vous puissiez percevoir des intérêts dessus et rester en phase avec l'inflation. Si vous ne déposez pas suffisamment d'argent à la banque dans un contexte inflationniste, votre argent perdra de la valeur. Mais si vous déposez de l'argent dans une banque, elle l'investira à votre place, percevra des intérêts, vous reversera des intérêts à un taux plus bas et conservera la différence. Donc si vous n'alimentez pas un compte d'épargne parce que votre argent prend de la valeur automatiquement par la déflation, les banques perdent.

Pour résumer, vous n'empruntez pas et vous ne déposez pas votre argent dans un compte d'épargne ou un compte d'investissement pour suivre le rythme de l'inflation, par conséquent les banques perdent les revenus des prêts et des dépôts qui leur permettent d'emprunter peu et de prêter beaucoup, qui est un de leurs modèles économiques de base.

Donc, que reste-t-il à faire aux banques ? Eh bien, elles pourraient seulement passer leur temps à faciliter les transactions comme le font Visa, Mastercard, le réseau SWIFT, Western Union Money Transfer et d'autres. Mais on a déjà dit que les transactions Bitcoin sont faites de personne à personne et coûtent très peu. Les banques ne perçoivent même pas ce revenu.

Et c'est pour cela que les banques travaillent très, très dur en coulisse pour essayer de tuer Bitcoin avant qu'il ne les tue.

---

http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/09/heres-why-volatility-isnt-a-big-problem-for-bitcoin/

• 9 décembre 2013, Timothy Lee :

It's true that Bitcoin's volatility is a problem right now, but it's a mistake to treat volatility as an intrinsic characteristic of the currency. Bitcoin is volatile for two basic reasons: it's currently difficult to purchase Bitcoins with dollars, and there's a lot of uncertainty about the Bitcoin network's long-term prospects. These are both issues that should get resolved in the coming years, making the cryptocurrency much less volatile. Liquid markets help to prevent price volatility. When the price of gold or pork bellies or shares of Microsoft stock starts to fall, bargain-hunting buyers jump into the market and push the price back up. That can happen quickly because there are sophisticated institutions like the New York Stock Exchange and the Chicago Mercantile Exchange helping to ensure that buyers who want to get into the market can do so easily.

Regulatory and technical challenges have slowed the development of mature exchanges to perform this function for bitcoins. A thicket of state-based money transmitter laws and the skepticism of conventional U.S. banks has made it challenging to operate a Bitcoin exchange in the United States. As a result, the leading services to trade bitcoins for dollars are all based overseas. They're not well-integrated with the U.S. financial system, so it's slow and expensive for consumers in the United States, Bitcoin's largest market, to buy Bitcoins when they see the price dropping.

Creating liquid markets for Bitcoin is challenging, but there's no reason to think it's impossible. Comments from federal regulators have been surprisingly positive. Complying with state-level regulations is tedious and expensive, but sooner or later some entrepreneur will get the job done. And while conventional banks are currently skeptical of the cryptocurrency, they're likely to warm to it over time as they come to understand it better. So over time, the dollar/bitcoin trade should become a lot more liquid, eliminating one of the major sources of Bitcoin volatility.

---

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

• 9 décembre 2013, Jérémy Berthet :

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 :

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 "talk" 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 :

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 :

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://images.infoworld.com/print/232599

• 13 décembre 2013, Simon Phipps :

The Internet is creating a society where each of us can play the roles previously reserved for corporations and moguls, if we choose -- all without needing an intermediary. We can start businesses, trade goods, conduct relationships, publish, editorialize, and conduct politics, all without needing an intermediary to empower us -- a phenomenon I call "the meshed society." A currency we can use as we engage in those activities is a natural complement and vehicle. As the meshed society matures, our need for digital money is inevitable.

---

http://mashable.com/2013/12/16/cameron-winklevoss-bitcoin/

• 16 décembre 2013, Cameron Winklevoss :

Small bull case scenario for Bitcoin is a 400 billion USD dollar market cap, so 40,000 USD a coin, but I believe it could be much larger. When this will happen, if it happens, I don't know, but if it happens, it will probably happen much faster than anyone imagines.

---

http://www.pcworld.com/article/2081560/bitcoin-the-virtual-currency-built-on-math-hope-and-hype.html

• 18 décembre 2013, Steve Kirsch :

Buy bitcoins now. Take 5 percent of your net worth, and put it into Bitcoin. [...] You won't be sorry. I think for the next few years, any time you buy bitcoins and hold onto them, and then sell it, you'll make substantial amounts of money. You'll be so happy."

---

http://www.policymic.com/articles/77293/even-china-can-t-stop-bitcoin-from-getting-big-here-s-why

• 21 décembre 2013, Jeff Fong :

The real question to ask is if Bitcoin will be adopted as a technology, and that is something different from asking if it will be adopted as a currency.

As a network for clearing payments, Bitcoin is lower cost than anything out there. Transferring Bitcoins between different addresses is far quicker as well as less expensive than using standard credit card processors and a growing number of merchants have taken notice.

Bitcoin's market share is still tiny compared to traditional payment processors, but it has grown considerably from the days when a Bitcoin could only get you Alpaca Socks.

Key to this growth have been businesses that make Bitcoin accessible to consumers and vendors alike. Coinbase — which just raised a cool $25 million in venture capital funding — helps merchants accept Bitcoin as part of their e-commerce platforms. It also offers exchange rate guarantees to give merchants the benefit of Bitcoin as a payments platform without the exchange rate risk of Bitcoin as a currency. Other startups like Bitpay offer similar services.

CoinCove is also trying to leverage Bitcoin as a global payments platform, but for a slightly different market. The company's mission is to lower the cost of sending money to Latin America for immigrant workers abroad. What they came up with was to use Bitcoin as an intermediary to send value from one end of the globe to the other, bypassing more expensive middlemen. A worker in Spain can go to a local broker, exchange Euros for Bitcoin, send the Bitcoin to relatives in Columbia, and have those relatives exchange the

Bitcoin back into Colombian pesos. Coincove plans to flesh out the infrastructure needed to make this possible.

[...] If we want to evaluate Bitcoin's potential, we need think of it as something bigger than just a new form of currency. We need to think about the entrepreneurs leveraging it as a serious problem solving tool and not just the speculators looking to make a quick buck.

---

http://bits.blogs.nytimes.com/2013/12/22/disruptions-betting-on-bitcoin/?_r=0

• 22 décembre 2013, Nick Bilton :

The real question is not what Bitcoin will be worth next week or next month. It is whether digital currencies like this have promise and, if so, how they could change our world. Digital currencies — whether Bitcoin or something else — could make it cheaper and easier to move money around.

"While there are questions about the future of Bitcoin, there is clearly going to be a digital currency that can be used for remittances, micro payments, and across borders," said Susan Athey, a professor of economics at the Stanford Graduate School of Business. "In today's system you see a number of different kinds of commerce not taking place because the fees are too high relative to the transactions."

With small transactions, the cost to send money can be more expensive than the actual money people are spending. People are charged credit card fees, transfer fees and other expenses that all go to a middle man. This is why there are no 10 cent apps on the app store, many companies try to clump small transactions together online.

With virtual currencies, in comparison, there is no middle man. With Bitcoin, for example, anyone running the software on his or her computer also acts as the bank storing the exchange information.

Ms. Athey said that while it was unclear if Bitcoin or a competing math-based currency — and hundreds of other virtual currencies are in the market now — would prevail, it was clear that there was a need for this type of tender online. "Something that has less frictions could enable certain types of commerce to occur that aren't occurring today," she said.

---

http://www.forbes.com/sites/realspin/2013/12/22/libertarians-and-millennials-are-going-crazy-over-bitcoin-what-are-they/

• 22 décembre 2013, Gannon LeBlanc :

With more people taking interest in this fascinating real-world economic experiment, we are going to see Bitcoin enter the everyday consumer's life.

We're also seeing Bitcoin coincide with a generation more mobile than ever. Millennials can use Bitcoins in any country, without having to convert their currency. There is no need to find a currency exchange building, no need to worry about conversion rates, no need to worry about a lot of the problems with government-issued currency. Bitcoin also connects young people in disparate countries with each other so they can pay each other easily for services like software development and intellectual property. Bitcoin has no borders. It connects businesses directly with customers in a more direct way than any "middlemen" like PayPal or a credit card companies. It's economic freedom unlike anything seen before.

Bitcoins can be an investment, a medium of exchange, and much more. It's also a challenge to the status quo and proof that the free market can produce a private currency that works.

[...] Bitcoin is loved and embraced by young bright individuals who see the potential

future that Bitcoin and what it represents and can be.

---

http://www.theaustralian.com.au/technology/bitcoin-use-spreading-despite-vulnerability/story-e6frgakx-1226792056293

• 30 décembre 2013, The Australian :

Internationally, bitcoin is gaining acceptance for various kinds of purchases, such as gift cards and even for Black Friday shopping last month.

Daniel Mery, owner of Planet Linux in Coral Gables, said customers can easily walk up and use their phones to purchase coffee, pastries and sandwiches in the cafe with bitcoin.

"We want to promote bitcoin like we promote new technologies," Mery said. "Bitcoin is a universal currency, it's a currency that no government controls."

Proponents such as Evans see bitcoin as a potential payment solution that facilitates international trade without requiring currency exchange, especially in regions such as the Caribbean and the Americas where cell phone and technology usage is increasing. In Venezuela, for example, there are 30.5 million cell users, a number that tops the country's actual population, according to National Telecommunications Commission data.

Since bitcoin can be transferred via smart phones, Carlos Parra, an economics professor at Florida International University, believes there's a chance to impact impoverished and under-served residents in countries such as Venezuela.

"If it turns out that bitcoins end up having less volatility than the national currency, then people at the bottom of the pyramid in Venezuela, for them it would be easier to use bitcoins," Parra said.

"Bitcoins would be very useful for international transfers. Most of the remittances to the Caribbean come from Miami and they are making a lot of inroads with mobile money."

---

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

• 2 janvier 2014 Alec Liu :

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.coindesk.com/bitcoin-isnt-evil-what-gives-value/

• 4 janvier 2014, Oleg Andreev :

So what gives BTC value?

In the first year of bitcoin, there were almost no transactions, but people were spending their energy on generating bitcoins. The only two reasons that come in my mind are:

1. Value as a collectible, in a similar manner to people collecting rare metals, stones, shells, postal stamps, paintings and baseball cards.

2. Value from betting that other people may find these collectibles valuable and thus would have to buy some of them from earlier collectors, thus making them richer.

Gold is valuable for the exact same reason. Not because it's shiny (many things are), but because it's rare, durable and mobile, and thus can be collected. And once collected, it can only increase in value when more people want it. Once the collectible gets some value, it can become money. Once bitcoins became valuable, you could take advantage of the beautiful transfer network. But it always stays the same network: whether a hundred people use it or millions.

So the network can't be responsible for any single price that people put on bitcoin.

[...] **In the end, bitcoin is valuable as a collectible.** Its reliability as a "store of value" depends on the number of people willing to hold it. The more people believe in the seriousness of bitcoin, the more they will add to this belief in the form of infrastructure around it, increasing people's confidence about it even further.

---

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 :

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 traîter 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.

---

http://www.psmag.com/navigation/business-economics/bitcoin-crash-never-came-72462/

• 8 janvier 2014, Kyle Chayka

The Bitcoin crash that never came

[...] As Bitcoin expands into new markets [...], its value and utility increases, it depends less on speculation for its price, and the threat of a sudden crash becomes less likely. The

rate of its adoption by businesses also seems to be increasing.

[...] Bitcoin's resilience in the face of the Chinese legislation also shows that it's less susceptible to government interference than some expected.

[...] If all users indeed have so much faith in the digital currency, then it doesn't matter much if Bitcoin can be easily traded for yuan or not.

---

http://www.theepochtimes.com/n3/458540-bitcoin-is-poised-to-shake-the-world-are-you-paying-attention/

• 19 janvier, Michael Taylor :

Bitcoin Is Poised to Shake the World: Are You Paying Attention?

[...]The **transaction costs of transfers are as close to zero as you can get**, and (because of Moore's Law) they will keep falling. Essentially, in the Bitcoin universe, there is no difference in the transaction costs between a) buying a loaf of bread at your local store, or b) sending millions of Bitcoins through the ether from one side of the planet to the other. The cost for both is more or less zero.

[..] Convenience is the reason we buy our chewing gum and cigarettes from the local store and not from the out of town cash and carry. Even though we know the local store charges a premium, that's still better than hopping in the car and driving across town for a small purchase. The same logic applies to the world of traditional banking. However unreasonable a transaction cost may be, it'll still be cheaper than hopping on a plane with a sack full of cash. What makes the Bitcoin solution unique here is that it sidesteps this issue by making all financial transactions equally convenient. **From the perspective of both the buyer and the seller that's a very attractive proposition – from the perspective of the (possibly soon defunct) middlemen, it's a nightmare. The emergence of Bitcoin is going to make a lot of very powerful, influential and traditional middlemen-style institutions very nervous.**

[...] One other big paradigm shift in the Bitcoin world is around credit. **In the Bitcoin world, there simply is no fictional money.** This would make fractional banking (the method by which banks lend out more money than they actually have in reserves) almost impossible. In the Bitcoin world, banks would only be able to lend the money they actually have. Perhaps loans would be spread across Bitcoin's distributed network, much like crowdfunding. However it works in practice, the impact of reduced credit on a world currently addicted to the stuff is anybody's guess.

Until recently, SETI (the project who's aim is to Search for Extraterrestrial Intelligence) has been the number one global distributed computing network. However now that Bitcoin is on the rise, it's been bumped down to second place. In fact the surge in Bitcoin's distributed computing power is like nothing we've ever seen before. **As Bill Gates said, "Bitcoin is a technological tour de force".**

[...] The exponential rise of Bitcoin will no doubt start to generate some heat from here on in. It's only a matter of time before we see the traditional gatekeepers start to cry foul. No doubt we'll see a lot of anger and rage in the courtrooms. At least in the west. In Africa and Asia we'll probably see things take off a little quicker. **I predict it will only be a few years from now before we see Bitcoin (or other similar digital currencies) emerge as the exchange of choice for the majority of people otherwise denied access to the established money structures. And when that happens, prepare for the world to shake.**

---

http://finance.fortune.cnn.com/2014/01/21/bitcoin-platform/

• Le 21 janvier 2014, David Z. Morris :

Bitcoin is not just digital currency. It's Napster for finance.

[...] Some still doubt bitcoin's usefulness and durability, but 2014 may leave skeptics even further behind - developers and entrepreneurs are already hard at work building features on top of the Bitcoin protocol that will allow for the **decentralized execution of financial services**, from currency hedging to loans to stock issuance to rental and purchase contracts. These new services rely on the same innovative proof-of-work model of distributed security and record-keeping that has kept the bitcoin currency secure as its value ballooned well past $10 billion. **In the long term, peer-to-peer finance threatens to weaken banks and other financial agents just as peer-to-peer file sharing did the music industry** -- and some of the architects of this financial Napster seem gleeful about the possibility.

[...] Consultant Andreas M. Antonopoulos, echoing a 2012 white paper by software developer J.R. Willett, says that the Bitcoin protocol is to distributed finance what Internet Protocol has been to distributed information.

[...] Efforts to make complex financial functions a part of Bitcoin have been bubbling through 2013, but 2014 will see them come to fruition.

[...] Mastercoin, based on Willett's white paper and programming, is projected to add many functions to the Bitcoin blockchain. These include allowing users to create new asset classes, such as stocks or other ownership certificates, and create a variety of automated "smart contracts."

Independent entrepreneurs are also working to build this infrastructure. One of these is Reggie Middleton, currently building a client called BTC Swap. Middleton, gravelly voiced, dapper, and businesslike, doesn't fit the stereotype of woolly young bitcoin developers. But he slyly describes himself as "not quite an anarchist," and BTC Swap is a shot directly across the bow of the financial industry. Still in early development, BTC Swap is planned to facilitate a variety of what Middleton calls "Zero-Trust Digital Contracts," which recreate financial functions in software code by matching offered and desired transactions between parties without the need for intermediary institutions. Because these contracts are automated, instantaneous, and executed with assets already represented in the Bitcoin blockchain, Middleton says they eliminate counterparty risk while also subtracting conventional banking and brokerage fees.

The most immediate function Middleton envisions for his system is for hedging bitcoin against existing national currencies. With bitcoin's valuation still showing huge volatility, Middleton claims **the availability of distributed hedging will both ensure the value of bitcoin for individuals holding the asset and provide systemic stability**.