

L'AUTEUR



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

BIBLIOGRAPHIE

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

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

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

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

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

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

Bitcoin Foundation : <https://bitcoinfoundation.org>

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

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

L'impossible devenu réalité... et valeur

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

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

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

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

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

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

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

Offre de parrainage

Pour **Noël**, offrez une année de découvertes avec **SCIENCE**



Prix unitaire : 11,95 € - www.hugobouc.fr

Et recevez votre CADEAU

Les amateurs de jeux de chiffres prendront plaisir à résoudre un jeu de chiffres par jour : sudokus, carrés magiques, opérations secrètes, dédalos, hanjes, koudumos, jeux de logique, géométrie...

À partir de janvier 2014, votre filleul recevra au choix pendant un an :

- ou 12 numéros du magazine *Pour la Science*
- 12 numéros du magazine *Pour la Science* + 4 numéros du *Dossier Pour la Science*.



Une personne de votre entourage s'intéresse aux neurosciences et à la psychologie ? Faites-lui plaisir ! Offrez-lui un abonnement d'un an à **Cerveau & Psycho** et recevez votre cadeau !

À partir de janvier 2014, votre filleul recevra au choix pendant un an :

- ou 6 numéros du magazine *Cerveau et Psycho*
- 6 numéros du magazine *Cerveau et Psycho* + 4 numéros de l'*Essentiel Cerveau & Psycho*.



Votre CADEAU

Avec trois niveaux de difficulté, les jeux proposés dans ce livre vous feront exercer votre sens de l'observation et votre logique, et s'ils paraissent simples, ils se révèlent parfois plus complexes qu'il n'y paraît.

Prix unitaire : 10,50 € - www.hugobouc.fr



BULLETIN DE PARRAINAGE **SCIENCE**

À découper ou à photocopier et à retourner accompagné de votre règlement dans une enveloppe non affranchie à : Groupe Pour la Science • Service Abonnements • 8 rue Férou • 75 278 Paris cedex 06

POUR MON/MA FILLEUL(E)

Oui, j'offre 1 an d'abonnement au magazine *Pour la Science* :

- ☐ **formule simple • 12 numéros • 56 €** au lieu de 74,90 €
Tarif valable uniquement en France métropolitaine et d'outre-mer.
Pour l'étranger, participation aux frais de port à ajouter : Europe 12 € - autres pays 25 €.
- ☐ **formule couplée • 12 numéros + 4 Dossiers • 76 €** au lieu de 102,70 €
Tarif valable uniquement en France métropolitaine et d'outre-mer.
Pour l'étranger, participation aux frais de port à ajouter : Europe 16 € - autres pays 35 €.

Oui, j'offre 1 an d'abonnement au magazine *Cerveau & Psycho* :

- Format choisi : ☐ **classique** (21 x 28 cm) ou ☐ **pocket** (16 x 23 cm)
- ☐ **formule simple • 6 numéros • 32 €** au lieu de 41,70 €
Tarif valable uniquement en France métropolitaine et d'outre-mer.
Pour l'étranger, participation aux frais de port à ajouter : Europe 7,50 € - autres pays 15 €.
- ☐ **formule couplée • 10 numéros + 4 Essentiels • 48 €** au lieu de 69,50 €
Tarif valable uniquement en France métropolitaine et d'outre-mer.
Pour l'étranger, participation aux frais de port à ajouter : Europe 11,50 € - autres pays 23 €.

J'indique ci-dessous les coordonnées de la personne qui en bénéficiera :

Nom : _____ Prénom : _____
Adresse : _____
CP : _____ Ville : _____
Pays : _____ Tél. : _____
Email : _____ Pour le suivi client (facultatif)

POUR MOI *

Je reçois en cadeau aux coordonnées suivantes :

- ☐ **Un Jeu de Chiffres par jour - 2014** (983871)
- ☐ **Jeux de Logique** (983870)

Nom : _____ Prénom : _____
Adresse : _____
CP : _____ Ville : _____
Pays : _____ Tél. : _____
Email : _____ Pour le suivi client (facultatif)

Je choisis mon mode de règlement :

- ☐ Par chèque à l'ordre de *Pour la Science*
- ☐ Par carte bancaire
Numéro de carte _____
Date d'expiration _____ Signature obligatoire
Clé _____
(les 3 chiffres au dos de votre CB)

* Vous pouvez profiter de cette offre pour vous réabonner. Dans ce cas, remplissez la partie « Filleul » en indiquant vos coordonnées. Vous recevrez également vos cadeaux.
En application de l'article 27 de la loi du 6 janvier 1978, les informations ci-dessus sont indispensables au traitement de votre commande. Elles peuvent donner lieu à l'exercice du droit d'accès et de rectification auprès du groupe Pour la Science. Par notre intermédiaire, vous ou votre filleul(e) pouvez être amenés à recevoir des propositions d'organismes partenaires. En cas de refus de votre part, merci de cocher la case ci-contre ☐

SCIENCE & FICTION

Matière à fiction

Certains matériaux naturels ont des propriétés que les matériaux artificiels n'atteignent pas. Mais ceux de la science-fiction sont encore plus performants !

Roland LEHOUCQ et Jean-Sébastien STEYER

De la pierre taillée aux nanotubes de carbone, du travail du bois à la métallurgie, l'amélioration des techniques est toujours allée de pair avec la recherche de nouveaux matériaux. Dès l'Antiquité, Platon évoque l'orichalque dans *L'Atlantide* : ce métal, le plus précieux après l'or, aurait été couramment utilisé par les Atlantes. La pierre philosophale, autre matériau de légende, a été recherchée en vain par les alchimistes qui la pensaient capable de transmuter les métaux, notamment le plomb en or. Mais le mythe de la transmutation est devenu réalité avec l'invention des accélérateurs de particules : les collisions de haute énergie qui s'y déroulent transforment les noyaux cibles en d'autres noyaux n'existant pas toujours à l'état naturel. Ainsi la transmutation d'un métal en or fut réussie pour la première fois en 1941, en bombardant du mercure avec des neutrons. Hélas, l'or obtenu est radioactif et son coût de production prohibitif, ce qui rend le procédé totalement inutilisable en pratique !

Les auteurs de science-fiction n'ont bien sûr pas manqué d'inventer quantité de matériaux fabuleux. L'un des premiers exemples est la cavorite, imaginée par H. G. Wells dans son roman *Les Premiers Hommes dans la Lune*, paru en 1901. Cette substance a la propriété singulière de se comporter comme un écran gravitationnel, tout comme une cage de Faraday fait écran aux champs électromagnétiques. La cavorite permet donc de construire un appareil se déplaçant par antigravité ! La physique interdit l'existence

d'un matériau opaque à la gravitation, car il permettrait de fabriquer une machine à mouvement perpétuel : en placer un morceau sous une roue suffirait à la mettre en rotation du seul fait de l'annulation de son poids à l'endroit où le matériau est placé. La cavorite est nommée d'après le héros du roman, le docteur Cavor, qui la réalise en « fondant ensemble quelques métaux et diverses autres choses ».

Un cas plus intéressant encore est celui de Cleve Cartmill. En 1944, il publie dans la revue *Astounding Science Fiction* une nouvelle intitulée *Deadline* où est décrite une bombe utilisant des isotopes radioactifs déjà connus des physiciens nucléaires de l'époque. Les détails qu'il en donna attirèrent l'attention du FBI qui y vit un engin similaire à celui qui était alors en construction dans le cadre du très secret projet *Manhattan*, dont l'objectif était la réalisation d'une bombe nucléaire.

Les auteurs de science-fiction n'anticipent pas toujours l'avenir de façon aussi pertinente. S'ils s'inspirent de matériaux existant réellement, ils en déforment ou en amplifient les propriétés. Ainsi, dans *Les fontaines du paradis*, Arthur Clarke décrit la construction d'un ascenseur spatial, très long câble fixé à la surface de la Terre et permettant d'accéder à l'espace. Il doit être de faible densité et d'une résistance à la traction dépassant largement celle des matériaux ordinairement utilisés dans la construction. Dans son roman, Clarke nomme « monofilament » le matériau utilisé et extrapole probablement les propriétés des fibres de carbone ou des fibres polymères à haute résistance, le kevlar par exemple.



1. DANS LE FILM AVATAR, l'unobtainium a les propriétés d'un supraconducteur à température ambiante, Graal des physiciens des matériaux.