LA CHRONIQUE DE
GÉRALD BRONNER

CAPTER À TOUT PRIX DU TEMPS DE CERVEAU

Pour attirer l'attention dans un monde saturé d'informations, certains sont prêts aux pires outrances. Avec la complicité effective de leurs spectateurs.

Se cimenter la tête dans un four à microondes et passer à deux doigts de la mort : Jimmy Swingler l'a fait pour rendre populaire sa chaîne de vidéos sur Youtube.

La Flat Earth Society, ou «Société de la Terre plate», soufflera ses 62 bougies cette année et les thèses qu'elle défend semblent connaître un étonnant regain d'adhésion. Certains sont si convaincus que notre planète est un disque plat dont le centre est le pôle Nord qu'ils sont prêts à investir de l'argent et à risquer leur vie pour le démontrer.

Ainsi, Mike Hugues, membre de cette société et chauffeur de limousine de son métier, a décidé de monter à bord d'une fusée de sa propre conception afin de trancher définitivement la question. Définitivement : le terme est un peu ironique si l'on songe à ses chances d'en ressortir indemne.

De tous les commentaires qu'a suscités cette affaire tragicomique, celui avertissant que Mike Hugues risque d'être un futur lauréat des Darwin Awards fut sans doute le plus avisé. Ce prix, inspiré par un humour très noir, récompense chaque année, assez souvent à titre posthume, un individu qui, par un acte stupide ayant conduit à sa mort ou à sa stérilisation, dispense l'humanité de la transmission de son code génétique.

Dans le même registre, une récente vidéo justifierait que son auteur, Jimmy Swingler, un youtubeur britannique de 22 ans, figure dans la catégorie «espoir» du prix. Sa drôle d'idée fut de se filmer après s'être cimenté la tête dans un four à microondes !

Le titre de la vidéo que Jimmy Swingler ne manqua pas de diffuser sur la toile : *Presque mort*. Le youtubeur n'a en effet dû sa survie qu'à l'intervention des pompiers, furieux par ailleurs d'avoir été mobilisés pendant près d'une heure pour le sauver. Le plus effrayant peut-être est que ce type de démarche n'est pas inspiré seulement par la bêtise. En effet, son auteur a pris soin d'accorder toutes sortes d'entretiens en expliquant qu'il s'agissait pour lui de rendre TGFbro, sa chaîne Youtube, populaire (ce qui peut être très rémunérateur), en tentant de capter du temps de cerveau disponible. La meilleure solution lui a paru de mettre, une fois de plus (car c'est un récidiviste), sa vie en danger d'une façon stupide. Malheureusement, son raisonnement se tient puisque la vidéo a été vue des millions de fois.

> **Le youtubeur britannique Jimmy Swingler risque d'être un jour lauréat des Darwin Awards**

D'ailleurs, souligne Jimmy Swingler, ceux qui contribuent au succès de ses films sont une des causes principales de ses prises de risque, et leur implication morale n'est donc pas nulle. Et en y réfléchissant, l'auteur de cette chronique, pas plus que tous les (nombreux) journalistes qui ont évoqué l'affaire ne peuvent être exonérés de leur responsabilité morale.

Sur ce marché saturé d'informations où l'offre et la demande sont intimement liées, ceux qui cherchent à capter du temps de cerveau disponible en jouant sur le fait que cet organe est sensible à toute proposition cognitive ne relevant pas de la routine pourront le faire en misant sur l'outrance, l'extrême stupidité, la peur et bien d'autres choses de cet ordre. Ici, la recette qui consiste à croiser des conséquences colossales (la mort) avec des motivations dérisoires (faire rire) a toutes les chances de susciter une épidémie d'attention un peu honteuse.

C'est sans doute avec ce sentiment ambigu, par exemple, que nous avons lu les articles concernant cette jeune étatsunienne, Monalisa Perez, qui a voulu répondre à une question vitale : une épaisse encyclopédie peut-elle protéger d'une balle tirée par un pistolet ? «Pas toujours», aurait pu répondre son petit ami Pedro Ruiz, qui n'a pas survécu à l'expérimentation. Le tout filmé sur leur chaîne Youtube, bien entendu. La jeune fille a plaidé coupable d'homicide involontaire.

Cette triste histoire l'illustre une fois de plus : toutes les conditions sont réunies pour que les candidats aux Darwin Awards deviennent de plus en plus nombreux. ■

GÉRALD BRONNER est professeur de sociologie à l'université Paris-Diderot.

Éditions de L'Observatoire

La philosophie et la physique sont-elles irréconciliables ?

ØCULTURE

Dans l'intérêt de la science

mathieu vidard | la tête au carré 14:05-15:00

france intervenez

franceinter.fr

Bitcoin et blockchain

Comment les cryptomonnaies changent le monde

Le bitcoin, qui fait aujourd'hui tant parler de lui, n'était qu'un début. Cette cryptomonnaie s'accompagne d'un outil informatique, la blockchain, dont les applications potentielles vont bien au-delà des systèmes décentralisés de monnaie numérique. Registres distribués et infalsifiables, les blockchains permettent d'instaurer sans intermédiaire humain des relations de confiance parmi les membres d'un réseau. Elles pourraient abolir certains des défauts du système financier et économique, mais elles soulèvent aussi des questions dérangeantes. Sommes-nous prêts à vivre dans un monde où n'importe quel bien, qu'il s'agisse de monnaie ou de données personnelles, peut être échangé et suivi à la trace dans des livres de compte indélébiles ? Et si cette technologie, initialement destinée à réduire le pouvoir des banques et des États, leur permettait en définitive d'exercer un contrôle sans précédent sur les citoyens ?

L'ESSENTIEL

> Le bitcoin, créé en 2009, est une monnaie numérique échangeable de pair à pair, sans instance centralisée. Cette monnaie repose sur un outil informatique nommé blockchain, qui fait office de grand registre distribué et sécurisé.

> Depuis 2009, un grand nombre d'autres « cryptomonnaies » fondées sur une blockchain sont apparues. Et les blockchains ont trouvé d'autres applications que les cryptomonnaies.

> Les cryptomonnaies et les blockchains sont en train de modifier le paysage économique et financier. Elles suscitent de nombreuses interrogations.

L'AUTEUR

JOHN PAVLUS
écrivain et cinéaste en sciences, techniques et design, vivant à Portland, aux États-Unis

Le nouveau monde des cryptomonnaies et des blockchains

Le bitcoin est la première grande monnaie numérique échangeable sans autorité centrale. De telles monnaies et les blockchains qui les rendent possibles modifient le paysage financier et économique. Comment, et jusqu'où ?

Bitcoin, cryptomonnaies, blockchains, contrats intelligents… Nombreux sont ceux qui ont entendu parler des évolutions rapides dans la technologie financière, mais rares sont ceux qui les comprennent vraiment. Des centaines de banques centrales et d'entreprises mûrissent une technologie qui change la donne : la blockchain, ou chaîne de blocs. Et les investisseurs parient des milliards dessus.

Pourtant, seuls 24 % des professionnels des services financiers internationaux interrogés en 2017 par PricewaterhouseCoopers (PwC) la connaissent « extrêmement bien » ou « très bien ». La plupart des non-initiés ont des doutes sur sa légalité et n'ont aucune idée de son mécanisme. Certains spécialistes affirment que les blockchains ont le pouvoir de bouleverser des systèmes économiques entiers. D'autres mettent en garde contre le grand nombre d'idées fantaisistes qui circulent autour de cette technologie.

Tout a commencé avec le pseudonyme Satoshi Nakamoto, derrière lequel se cache aujourd'hui le milliardaire le plus secret de la planète (s'il est encore en vie). En octobre 2008, Nakamoto publia, par le biais d'une obscure liste de diffusion sur Internet, un article où il détaillait l'idée de la blockchain : une base de données publique et distribuée, synchronisée toutes les 10 minutes sur des milliers d'ordinateurs, accessible à tous et néanmoins impossible à pirater par qui que ce soit. Son objectif ? Fournir, pour un nouveau système de monnaie numérique que Nakamoto a nommé bitcoin et qu'il lança en 2009, un enregistrement des échanges qui soit décentralisé et à toute épreuve.

Jusque-là, le problème des monnaies échangeables de pair à pair était l'impossibilité de garantir qu'on ne pouvait pas les dépenser deux fois (*voir l'article d'Alexander Lipton et Alex Pentland, page 36*). La technique des blockchains a levé la difficulté en inscrivant chaque transfert de bitcoins dans un « registre distribué » qui, en vertu de lois mathématiques et cryptographiques, est inviolable.

Cette technique a rapidement débordé vers d'autres applications, d'où une frénésie d'innovations. On peut voir la blockchain comme une structure qui enregistre n'importe quelles données dont la provenance doit être sécurisée : historiques financiers, documents de propriété, preuves d'identité… Reste que cette technique peut aussi être exploitée à des fins malveillantes, et certains tentent de modérer l'enthousiasme qu'elle suscite. Voici une visite, en questions-réponses, du paysage dans lequel le bitcoin et sa blockchain nous ont projetés. ■

BIBLIOGRAPHIE

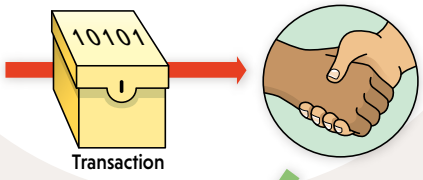
Pour plus de détails sur le fonctionnement du bitcoin et des blockchains, voir les articles de Jean-Paul Delahaye :
***Bitcoin*, la cryptomonnaie**, *Pour la Science* n° 434, décembre 2013 ;
Les preuves de travail, *Pour la Science* n° 438, avril 2014 ;
Les *blockchains*, clefs d'un nouveau monde, *Pour la Science* n° 449, mars 2015 ;
Du bitcoin à Ethereum : l'ordinateur-monde, *Pour la Science* n° 469, novembre 2016 ;
La folie électrique du bitcoin, *Pour la Science* n° 484, février 2018.

L. Leloup, **Blockchain. La révolution de la confiance**, Eyrolles, 2017.

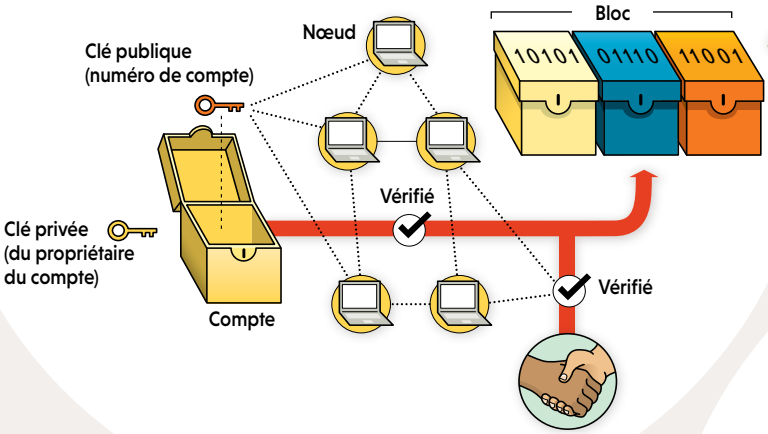
LE PRINCIPE D'UNE BLOCKCHAIN

Comment une monnaie numérique (ou une donnée de n'importe quelle autre nature) peut-elle s'échanger dans un réseau décentralisé constitué de nombreux inconnus qui n'ont aucune raison *a priori* de se faire confiance ? En créant un registre permanent de transactions qui ne peut être modifié par aucun membre du réseau. ***(Pour la définition de certains termes, voir le glossaire page suivante.)***

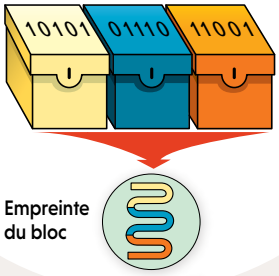
1 Une transaction à blockchain est lancée quand une partie envoie des données à une autre. Ces données peuvent être de toute nature : unités de monnaie (comme dans le cas du bitcoin) ou d'un autre instrument financier, contrats, actes notariés, titres de propriété, informations médicales, etc. L'objectif de la blockchain est de créer une trace permanente, vérifiable et infalsifiable de l'échange qui a eu lieu.



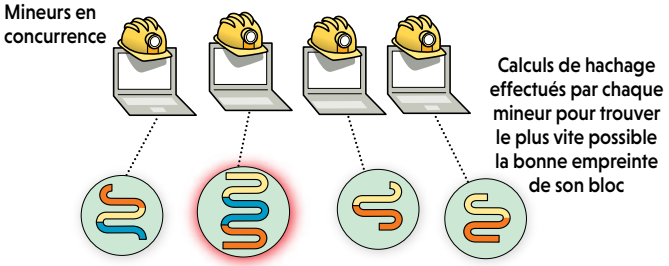
2 La transaction est diffusée pour vérification dans le réseau pair à pair d'ordinateurs qui gère la blockchain. Chaque nœud du réseau est équipé d'une procédure de vérification de la validité de la transaction (dans une transaction de bitcoins, par exemple, le réseau vérifie si ceux qui paient sont bien en possession du montant de bitcoins qu'ils prétendent détenir). Une fois la transaction vérifiée, elle est mise en attente. Elle est alors prête pour être associée à d'autres dans un bloc qui sera ajouté à la blockchain.



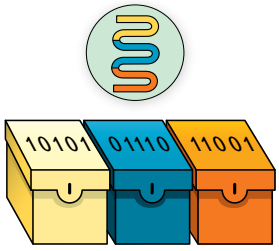
3 Chaque « mineur » du réseau choisit des transactions en attente pour composer un bloc qu'il cherche à ajouter à la chaîne des blocs précédents. Pour obtenir le droit d'ajouter ce bloc, il doit calculer, par une opération mathématique nommée hachage, une « empreinte » du bloc qui prend en compte l'empreinte des blocs précédents et qui vérifie une certaine propriété.



4 Les différents mineurs (faisant partie des nœuds du réseau) sont en concurrence pour gagner le droit d'ajouter à la chaîne de blocs le bloc choisi par chacun. Leurs ordinateurs effectuent de fastidieux calculs de hachage afin de produire une solution (l'empreinte du bloc) satisfaisant la propriété imposée (dans la blockchain du bitcoin, les mineurs cherchent des solutions, ou « valeurs de hachage », qui commencent par un nombre déterminé de zéros). Le mineur qui arrive le premier au bout de ce processus de « preuve de travail » en trouvant l'empreinte appropriée de son bloc « mine » celui-ci : il ajoute le bloc à la blockchain et gagne une récompense financière (de nouveaux bitcoins par exemple).



Le minage par preuve de travail étant très énergivore, certaines blockchains sont conçues de façon à fonctionner autrement. L'une des méthodes consiste à désigner au préalable des nœuds « validateurs », les seuls autorisés à enregistrer les transactions dans la blockchain.



5 Le bloc validé est ajouté à la chaîne de blocs avec son empreinte numérique, qui code aussi mathématiquement les empreintes validées de tous les blocs précédents. Ces empreintes gigognes sécurisent de façon croissante la blockchain à chaque bloc qui s'ajoute. En effet, l'altération de ne serait-ce qu'un seul bit d'information à un endroit quelconque de la chaîne modifierait non seulement l'empreinte de ce bloc particulier, mais aussi celle de tous les blocs ultérieurs de la chaîne.

GLOSSAIRE

CRYPTOMONNAIE
Forme de monnaie numérique reposant sur des méthodes cryptographiques afin de contrôler comment et quand sont créées les unités de monnaie, et de garantir le transfert sécurisé des fonds.

RÉSEAU PAIR À PAIR
Réseau d'ordinateurs reliés de façon décentralisée, tout ordinateur pouvant communiquer de proche en proche avec tout autre sans passer par un serveur central ou un administrateur.

NŒUD
Ordinateur participant à un réseau pair à pair. Le réseau du bitcoin comporte aujourd'hui plusieurs milliers de nœuds.

REGISTRE DISTRIBUÉ
Liste de transactions inscrites et horodatées qui est simultanément diffusée, copiée et vérifiée par tous les nœuds d'un réseau pair à pair. Si chaque nœud du réseau a une copie identique du registre, il est facile de repérer les entrées falsifiées ou les versions corrompues.

BLOC
Groupe de transactions enregistrées sur une blockchain. Dans le réseau du bitcoin, de nouveaux blocs sont ajoutés à la chaîne toutes les 10 minutes.

HACHAGE
Méthode cryptographique qui utilise une fonction mathématique (une « fonction de hachage ») pour condenser un ensemble quelconque de données en une chaîne unique de caractères alphanumériques de longueur fixe donnée, nommée valeur de hachage. Cela crée une empreinte numérique des données hachées facilement vérifiable : il suffit qu'un seul bit des données originales soit modifié ou corrompu pour que l'empreinte donnée par la fonction de hachage soit complètement différente. Le hachage est « à sens unique » : les données ne peuvent pas être reconstituées à partir de leur empreinte.

MINAGE
Ce terme désigne le processus par lequel les nœuds d'un réseau de cryptomonnaie rivalisent entre eux pour ajouter de façon sécurisée un nouveau bloc de transactions à une blockchain. Des unités de monnaie sont attribuées en récompense – une incitation financière à assurer la sécurité. Le minage implique de télécharger la dernière version en date des transactions de la blockchain pour vérification, puis d'effectuer des calculs systématiques pour rechercher la solution à une énigme mathématique compliquée, créée *via* le hachage du bloc. Le premier nœud qui trouve la bonne solution « mine » ce bloc : il l'ajoute à la chaîne de blocs et décroche la récompense associée. Plus un mineur dispose de puissance de calcul pour rechercher la solution, plus il a de chances de la trouver, un processus dit de validation par preuve de travail.

BITCOIN ET BLOCKCHAIN, EST-CE LA MÊME CHOSE ?

Non, mais ils sont régulièrement confondus parce qu'ils ont été portés ensemble à la connaissance du public en 2008, quand Satoshi Nakamoto a publié son article décrivant comment créer la monnaie bitcoin grâce à la technologie des blockchains qu'il inventait. Le bitcoin est un type de cryptomonnaie parmi d'autres. Quant à la blockchain, c'est la technique grâce à laquelle le système du bitcoin peut exister ; il s'agit d'une infrastructure que l'on peut utiliser pour assurer le suivi de nombreux types de transactions. La technique des blockchains existe sans le bitcoin, mais l'inverse n'est pas vrai.

D'OÙ VIENT LA VALEUR D'UNE CRYPTOMONNAIE ?

Selon certains experts, une cryptomonnaie telle que le bitcoin a de la valeur en vertu de sa sécurité (la blockchain du bitcoin n'a jamais été piratée jusqu'à présent) ou de sa rareté imposée (17 millions de bitcoins sont en circulation à ce jour ; le nombre total de bitcoins émis a été limité à 21 millions, ce qui signifie que le bitcoin ne pourra jamais être dévalué en « faisant tourner la planche à billets »). D'autres affirment que la cryptomonnaie a une valeur intrinsèque, le minage étant un travail fastidieux qui renforce le réseau ; en d'autres termes, c'est l'effort qui confère de la valeur. Mais cela ne s'applique pas à une cryptomonnaie ne faisant pas appel au minage. Selon Christian Catalini, du MIT, « sa valeur découle du consensus. Nous sommes tous d'accord qu'elle a de la valeur ». La monnaie est un moyen social d'assurer le suivi des échanges et des dettes ; si les cryptomonnaies se révèlent plus efficaces pour assurer ce suivi, leur valeur est assurée, qu'elles représentent un bien matériel ou juste un nombre.

LE BITCOIN, MONNAIE DE DEMAIN OU FEU DE PAILLE ?

Le bitcoin est la monnaie virtuelle la plus populaire, mais elle est aussi largement spéculative et très volatile : par exemple, le bitcoin a perdu 40 % en deux semaines en septembre 2017, avant de rebondir et d'atteindre des sommets à la fin de l'année, puis de chuter violemment au début de janvier 2018. Pour certains experts, les limites techniques du réseau (sa gestion des transactions est lente) combinées à des coûts de minage importants grèvent l'avenir de cette cryptomonnaie. « Nous ne parions pas sur le bitcoin », affirme Charlie Morris, directeur des placements chez Next-Block Global, entreprise qui investit dans la technologie des blockchains.

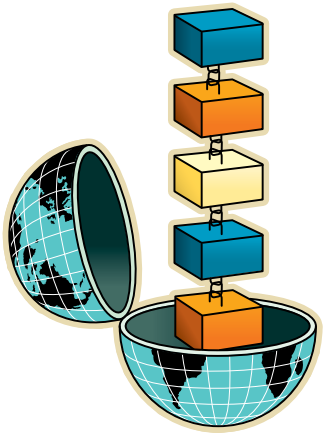
Ether, la deuxième plus grande monnaie virtuelle, a peut-être plus de ressorts pour durer. Ether n'est pas tant une monnaie analogue à des espèces qu'un « actif à blockchain », selon les mots de Charlie Morris, utilisé pour alimenter et sécuriser le réseau Ethereum. Un peu comme lors de la location de serveurs virtuels dans le *cloud* de Google, les développeurs souhaitant créer des applications à l'aide de la blockchain d'Ethereum doivent payer leur accès en unités monétaires appelées ethers. Plus Ethereum devient utile en tant que plateforme grand public, plus l'ether acquiert de valeur et de stabilité. De nouvelles plateformes et monnaies vont très probablement émerger – la course à la domination ne fait que commencer.

35 %

C'est la part approximative que représentent les bitcoins en termes de capitalisation, parmi l'ensemble des cryptomonnaies.

10 %

C'est la part du PIB mondial qui sera stockée dans des blockchains d'ici à 2025, d'après un rapport du Forum économique mondial datant de 2015.



VA-T-ON VERS LA FIN DES ESPÈCES ?

On pourrait avoir l'impression que les billets et les pièces de monnaie vont disparaître, mais, d'après les experts, on en est loin. On utilise encore beaucoup les espèces et le système actuel ne dysfonctionne pas au point qu'on veuille le défaire. Certes, le bitcoin et l'ether peuvent servir de valeurs ou d'unités d'échange, mais ils ne sont pas acceptés comme monnaie légale dans suffisamment d'endroits pour faire concurrence aux espèces.

Dans des pays tels que le Kenya, où peu de gens ont des comptes bancaires classiques et où des services financiers par téléphonie mobile tels que M-Pesa ont rendu les placements et les virements d'argent par téléphone beaucoup plus faciles que les échanges d'argent physique, les cryptomonnaies pourraient sembler tout adaptées. À condition que le minage se fasse ailleurs : il consomme beaucoup d'électricité, ressource peu disponible en Afrique, continent où les téléphones portables de base se vendent beaucoup mieux que les smartphones, et où les possesseurs d'ordinateurs personnels sont peu nombreux.

QUI SONT LES UTILISATEURS DE BLOCKCHAINS ?

Les blockchains ne servent pas qu'aux cyberlibertaires, et elles sont loin de ne concerner que la finance. Voici quelques exemples.

- **Institutions financières :** Des banques globales et organismes de placement travaillent sur des projets de blockchains, parfois en s'unissant au sein de consortiums. Depuis 2012, Ripple est un système prospère fondé sur une blockchain qui gère les transactions internationales entre banques. De jeunes pousses projettent de déployer des blockchains dans le domaine de l'évaluation du crédit ; elles espèrent ainsi mettre fin aux fuites de données, comme celle qu'a subie la société Equifax, victime d'un piratage.
- **Administrations :** Aux États-Unis, le Delaware et l'Illinois utilisent des registres distribués pour les certificats de naissance. Dubaï a intégré les blockchains à plusieurs de ses services administratifs, comme l'obtention de licences. En 2016, la Tunisie a commencé à émettre une version numérique de sa devise nationale adossée à une blockchain et appelée eDinar.
- **Entreprises de technologie :** Le réseau Ethereum (conçu comme support de nouvelles applications, et non en tant que simple écosystème pour monnaie virtuelle comme le réseau Bitcoin) est comparable à un App Store pour les jeunes pousses des blockchains. Des centaines de projets et d'entreprises l'exploitent, telle la société WePower, une plateforme d'échanges d'énergies renouvelables entre particuliers.
- **Droits d'auteur et propriété intellectuelle :** La musicienne britannique Imogen Heap a lancé Mycelia, un incubateur technologique qui assure le suivi des métadonnées associées aux œuvres de création, supprimant les intermédiaires tels que iTunes.
- **Organismes d'assistance et à but non lucratif :** La BitGive Foundation encourage et responsabilise le don caritatif. Et le programme alimentaire mondial des Nations Unies rationalise la façon dont elle assure le suivi et la distribution de l'aide aux réfugiés syriens en Jordanie.
- **Institutions académiques :** Le projet Blockcerts vise à rendre tous les diplômes et certificats professionnels plus fiables et faciles à partager.
- **Gestionnaires de biens :** L'entreprise Everledger, basée à Londres, cible l'industrie du diamant en enregistrant les attributs et la provenance de chaque pierre précieuse.
- **Journalistes :** Pour contrer les fausses informations, Civil offre aux journalistes une plateforme pour créer un journalisme inaltérable, sans publicité, protégé contre les intérêts extérieurs (Russie, Facebook...) et soutenu par les lecteurs.
- **Gens ordinaires :** Pour les travailleurs migrants qui envoient de l'argent à leur famille restée au pays, l'utilisation de bitcoins coûte moins que les transferts par Western Union ; ainsi, environ 20 % des transferts d'argent entre la Corée du Sud et les Philippines se font maintenant par ce biais.

POURQUOI UTILISER UNE CRYPTOMONNAIE PLUTÔT QU'UNE DEVISE NATIONALE ?

Imaginez que vous déteniez un billet de 100 euros qui ne permette d'acheter que pour 50 euros de marchandise. Au Venezuela, où la monnaie officielle est en train de s'effondrer, ce scénario est une réalité. Chaque année, le revenu net d'un habitant y perd à peu près la moitié de sa valeur à cause de l'hyperinflation. Pour y remédier, certains achètent des bitcoins.

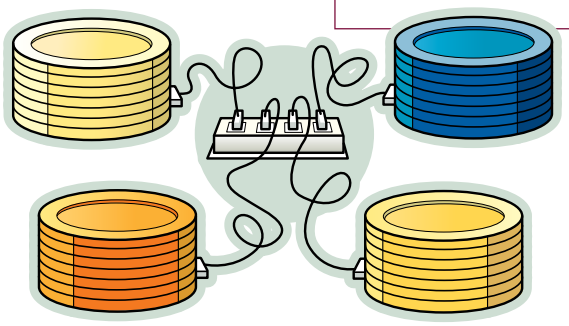
Comment en vient-on à préférer une cryptomonnaie difficile à comprendre, et dont la valeur n'est garantie par aucun État, à une matière première comme l'or, dont la valeur est reconnue depuis toujours ? D'abord, convertir des bolivars vénézuéliens en bitcoins est facile : quiconque a accès à Internet peut le faire. Ensuite, le bitcoin n'étant pas un objet matériel, il n'est pas besoin de le cacher dans un lieu peu sûr (comme un matelas ou, dans le cas du Venezuela, une banque). Et tandis que le bolivar a chuté brutalement, le cours du bitcoin a pour le moment une tendance moyenne à la hausse. Dans un pays où l'on attend une inflation dépassant 2 300 % en 2018 (d'après le Fonds monétaire international), la prise de risque paraît raisonnable.

LA BLOCKCHAIN EST-ELLE UNE NOUVELLE SORTE D'INTERNET ?

Non. La blockchain elle-même a besoin d'Internet pour déployer et maintenir son réseau pair à pair. Il convient aussi de noter que quand les gens parlent de « la » blockchain, sans plus de précisions, ils font presque toujours référence au système particulier que Satoshi Nakamoto a mis en place pour déployer le bitcoin. La blockchain du bitcoin a été le premier système de registre distribué ne faisant pas appel à un serveur centralisé ou une organisation pour son déploiement. Elle reste l'une des plus importantes : en janvier 2018, elle contenait plus de 154 gigaoctets (154 milliards d'octets) d'information, et chaque nouvelle transaction en augmente la taille. Mais cela reste très inférieur à la quantité de données présentes sur Internet, qui serait de l'ordre du yottaoctet (10^{24} octets, soit une différence de 13 ordres de grandeur).

1 500

C'est le nombre approximatif de cryptomonnaies en circulation à la fin de janvier 2018.



OÙ LE MINAGE SE FAIT-IL ?

70 %

environ des bitcoins sont minés en Chine ; le deuxième pays le plus actif est l'Inde, avec 4 %. N'essayez pas de miner seul chez vous. La tâche est aujourd'hui dominée par de gigantesques fermes de minage, et les chances qu'un particulier mine des bitcoins sont extrêmement faibles. Il dépenserait beaucoup plus en factures d'électricité qu'il ne pourrait espérer gagner en profits.

QUELLES SONT LES FUTURES APPLICATIONS POSSIBLES DES BLOCKCHAINS ?

En voici quelques exemples.

- **Des voitures autonomes en autogestion :** Au lieu de rouler pour Uber, votre voiture se conduirait toute seule pendant que vous travaillez ou que vous dormez. Des contrats intelligents garantis par des blockchains pourraient faire disparaître les intermédiaires comme Uber et Blablacar de l'équation du covoiturage en automatisant leurs deux fonctions de base : la mise en relation des chauffeurs et des passagers, et la facilitation des paiements.
- **Des données médicales portables :** La technique qui permet à deux personnes d'échanger des bitcoins sans nécessairement se faire confiance pourrait également garantir l'information médicale, dont le contrôle serait entièrement entre les mains du patient. C'est ce qu'explique Brian Behlendorf, directeur exécutif du projet Hyperledger de la Fondation Linux, une trousse à outils pour construire des applications à blockchains. Les patients se verraient attribuer un « portefeuille santé » où figurent leurs données et leurs antécédents. Un médecin pourrait accéder à un registre et demander votre groupe sanguin, émettant une demande d'accès sur le téléphone de l'utilisateur. « Vous aurez ainsi un historique des personnes avec qui vous avez partagé les données, et la possibilité d'effacer l'information communiquée une fois terminé le traitement », indique Brian Behlendorf.
- **Un superordinateur global :** Vous pourriez participer à un superordinateur décentralisé mondial en reliant vos appareils à des milliers d'autres dans un réseau pair à pair, une blockchain permettant de vous rémunérer pour cela. Pendant que vous dormez, votre ordinateur portable et votre tablette pourraient être loués par des scientifiques souhaitant faire tourner des simulations, par exemple. Un projet nommé Golem y travaille déjà. La puissance cumulée des ordinateurs portables inactifs, très supérieure à la puissance des centres de données, accélérerait considérablement les calculs dans des domaines tels que la modélisation du climat.

QUELLES SONT LES LIMITES ET LES DANGERS DES BLOCKCHAINS ?

Emin Gün Sirer, chercheur à l'université Cornell spécialisé dans les blockchains, explique que ces dernières constituent un support quasiment impossible à modifier après coup. Mais il prévient : « Cela ne signifie pas que tout ce qui est inscrit sur une blockchain est vrai ou souhaitable. Si je suis piraté et que quelqu'un me vole mes cryptopièces et essaie de les utiliser, j'aurai très envie d'annuler cette transaction. Et c'est là que l'immuabilité devient un inconvénient. »

Il est également facile de confondre l'immuabilité théorique de la blockchain avec la sécurité réelle des données : les blockchains publiques telles que Bitcoin et Ethereum ne chiffrent en fait aucune information. Brian Behlendorf, de la Fondation Linux, va même plus loin : « Le registre ne devrait jamais être utilisé pour stocker des données personnelles ou quoi que ce soit de sensible, pas même sous forme chiffrée, dit-il, parce que quoi que nous chiffrions aujourd'hui, nous serons probablement en mesure de le déchiffrer dans quarante ou cinquante ans » avec les progrès de la technologie.

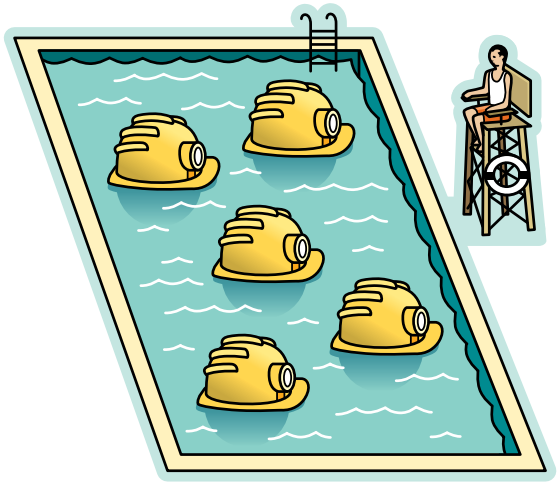
Certains partisans présentent les blockchains comme une panacée pour tout problème social où la confiance est un facteur important, mais c'est être aveuglément optimiste que de le croire (*voir l'article de Natalie Smolenski, page 44*).

QUELLE ÉNERGIE LES CRYPTOMONNAIES NÉCESSITENT-ELLES ?

Ce n'est pas parce que les cryptomonnaies n'ont pas d'attributs matériels que les utiliser ne coûte rien. Le processus volontairement intensif de minage des nouveaux bitcoins (la façon dont les nouvelles transactions sont ajoutées au registre, et qui permet aux mineurs de gagner des bitcoins) impose à l'ensemble du réseau pair à pair une grande masse de calculs pour valider les transactions de la blockchain. Tout ce traitement consomme de l'énergie.

Combien d'énergie au juste ? Commençons par la quantité de calculs. Début 2018, le taux de hachage du réseau Bitcoin tournait autour de 21 milliards de milliards de calculs par seconde de la fonction de hachage notée SHA256. Tirer de ce chiffre une estimation précise de la consommation énergétique est impossible parce que le réseau étant décentralisé, on ne peut connaître la consommation des nœuds individuels. Mais des estimations fiables placent la consommation électrique annuelle du réseau Bitcoin aux alentours de 40 térawattheures, soit à peu près 10 % de celle de la France entière. Pour chaque transaction, le réseau consommerait en moyenne plus de 500 kilowattheures, d'après le site Digiconomics (1 kilowattheure est l'énergie consommée par un radiateur de 1 000 watts au bout de 1 heure de fonctionnement). Celui-ci estime l'empreinte carbone de la consommation du réseau Bitcoin à 23 millions de tonnes de dioxyde de carbone (l'équivalent de l'empreinte carbone d'un pays tel que la Tunisie).

Le créateur d'Ethereum, Vitalik Buterin, envisage de faire basculer la blockchain du réseau vers un mécanisme de validation différent nommé preuve d'enjeu, qui ne repose pas du tout sur le minage. Il est peu probable que le réseau Bitcoin, plus vaste et plus décentralisé, en fasse de même à court échéance. Mais Vinay Gupta, qui a conçu la stratégie de Dubaï en matière de blockchain, pense que l'appât du gain, qui motive les mineurs à transformer les kilowatts en cryptomonnaie, finira bien par les pousser à innover pour résoudre ce problème d'extensibilité. Selon l'investisseur en capital-risque Charlie Morris, quand les cryptomonnaies à preuve d'enjeu feront leurs preuves sur les marchés, « le minage ne sera plus qu'une petite aberration de l'histoire ». « Les gens diront : "Vous vous rappelez quand nous faisions tous ça ? C'était franchement ridicule, non ?" »



LES BLOCKCHAINS SONT-ELLES LÉGALES ?

Oui. Mais leur nature décentralisée et leur association avec le bitcoin (qui a été utilisé dans des transactions illégales telles que des ventes d'armes et de drogue) ont contribué à donner aux blockchains une réputation d'activité hors-la-loi qu'elles ne méritent pas forcément. Les blockchains peuvent être utilisées à des fins très variées, bonnes ou mauvaises, tout comme Facebook, le courrier électronique ou toute autre technologie Internet.

77 %

des organismes ou entreprises du secteur financier dans le monde devraient adopter les blockchains d'ici à 2020, selon PwC.

QUE PENSE LE PUBLIC DES CRYPTOMONNAIES ET DES BLOCKCHAINS ?

62 %

des Américains pensent que les cryptomonnaies sont utilisées pour réaliser des achats illégaux, ou ne savent pas du tout qu'elles sont utilisées, d'après un sondage de YouGov réalisé en 2017.

59 %

des consommateurs du monde entier sondés en 2017 par HSBC affirment ne pas avoir entendu parler de la technologie de la blockchain ; 80 % de ceux qui ont entendu parler de la technologie ne comprennent pas de quoi il s'agit.

39 %

des cadres supérieurs des grandes entreprises américaines admettent qu'ils connaissent peu ou pas du tout la technologie de la blockchain, d'après un sondage réalisé en 2017 par le cabinet Deloitte.

À QUOI TIENNENT LA SÉCURITÉ ET LA FIABILITÉ DES CRYPTOMONNAIES ?

Les cryptomonnaies n'étant *in fine* que des logiciels, leur fiabilité provient de leur code source. N'importe qui peut créer une cryptomonnaie et lever des fonds en la vendant par l'intermédiaire d'une offre initiale d'unités de monnaie ; mais ce n'est pas un hasard si les deux cryptomonnaies les plus populaires, le bitcoin et l'ether, ont été développées par des spécialistes en informatique. Cela dit, même des monnaies reposant sur des systèmes techniques impressionnants peuvent être exposées au risque. L'« organisation autonome décentralisée » nommée The DAO, un fonds d'investissement en ethers utilisant le système Ethereum, et qui a levé plus de 100 millions de dollars en 2016, souffrait d'un bug grâce auquel des pirates ont subtilisé des ethers pour une valeur de 50 millions de dollars.

33 %

des conversions entre bitcoins et monnaies usuelles ont été piratées entre 2009 et 2015, selon un rapport de 2017 du département de la Sécurité intérieure des États-Unis.

COMMENT RÉGULER UN SYSTÈME DÉCENTRALISÉ ?

Étant donné la réputation sulfureuse des monnaies virtuelles décentralisées, on pourrait supposer qu'elles ont été créées pour supprimer la réglementation financière, ou au moins lui échapper. Mais ce n'est pas tout à fait exact. Le système du bitcoin est lui-même doté de nombreuses règles, après tout ; simplement, elles sont définies et implémentées par le code source (et l'activité collective de son réseau pair à pair) plutôt que par des États ou des institutions financières. « Toute l'innovation du système Bitcoin réside dans le fait qu'il évite une gestion humaine de la tenue de dossiers », dit Patrick Murck, juriste qui travaille sur la politique et la réglementation des blockchains à l'université Harvard. L'objectif déclaré d'Ethereum, soutenir le déploiement de contrats intelligents autonomes, est essentiellement un objectif de contrôle. Et une blockchain n'est rien d'autre qu'un système de règles dictant mathématiquement ce qui peut être fait ou non avec l'enregistrement des données dans une base.

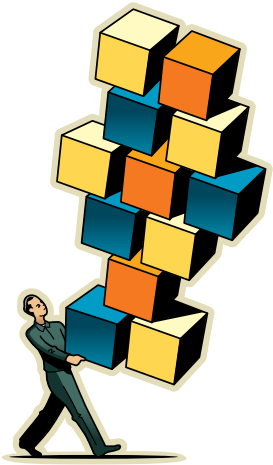
Ce qui est toujours important avec la régulation financière, qu'elle soit décentralisée ou non, c'est qui a le privilège de réguler, et comment. D'ailleurs, les États interviennent parfois pour réguler de l'extérieur l'usage des cryptomonnaies. Ainsi, en 2013, la Chine a interdit les cryptomonnaies dans son système bancaire, et en septembre dernier elle a bloqué l'accès aux bourses d'échange de cryptomonnaies (permettant par exemple d'acheter ou vendre des bitcoins contre des monnaies nationales). Les États-Unis et le Japon sont en train d'intervenir pour réguler ce type de plateformes et les « offres initiales d'unités de compte » avec la même vigilance que celle qu'ils exercent dans le cadre des ventes d'actions et des activités de placements bancaires.

Une application future de la technologie des blockchains concerne la sécurisation des identités numériques. D'après l'investisseur en capital-risque Charlie Morris, il pourrait émerger de nouvelles cryptomonnaies qui réunissent identité numérique et information financière. Elles n'auraient pas l'anonymat du système Bitcoin (Charlie Morris estime que seuls quelques centaines de détenteurs de bitcoins paient honnêtement leurs impôts sur ces avoirs). Mais quand la monnaie numérique se généralisera, le compromis entre sécurité perçue et stabilité rendra peut-être la surveillance tolérable, voire souhaitable. Comme l'exprime Patrick Murck : « Si je vous confie un bien à garder en mon nom et avec lequel vous pouvez effectuer des transactions, qu'il s'agisse de bitcoins ou d'ours en peluche, alors vous êtes soit régulé, soit sur le point de l'être. »

LES BLOCKCHAINS SONT-ELLES VULNÉRABLES ?

Jusqu'à présent, la blockchain du bitcoin, qui est la première, et à ce jour la plus vaste et la plus utilisée, n'a jamais été défaillante ou piratée. Mais cela ne signifie pas que toute blockchain est invulnérable par définition. « Il n'existe pas de technologie parfaite », prévient Emin Gün Sirer, de l'université Cornell, codirecteur de l'Initiative pour les cryptomonnaies et contrats. Voici trois points faibles que peut présenter une blockchain :

L'attaque des 51 %. La sécurité des réseaux de cryptomonnaie à base de blockchain repose sur deux ressources sans fond : la rapidité et l'appât du gain de leurs mineurs. Mais il est en théorie possible de vaincre ces deux obstacles. Pour subvertir le mécanisme de consensus de la blockchain, les pirates devraient prendre le contrôle d'une majorité (51 %) de la puissance du réseau. Ils pourraient alors, par exemple, bloquer la validation des transactions d'autres utilisateurs. Le réseau Bitcoin, avec ses milliers de nœuds, semble assez bien protégé contre une telle attaque. Mais des cryptomonnaies plus modestes sont exposées : l'une d'elles, Krypton, a ainsi été attaquée en 2016 par un groupe nommé 51crew. Même les blockchains ne faisant pas appel au procédé du minage sont vulnérables parce qu'elles reposent encore sur « l'hypothèse qu'une majorité de nœuds de leur réseau sont bienveillants », prévient Emin Gün Sirer.



La bonne vieille erreur humaine. Pour affecter la blockchain elle-même, il faudrait certes déplacer des montagnes (ou l'équivalent informatique). Mais le reste est vulnérable. En 2014, Mt. Gox, une plateforme d'échange entre devises classiques et bitcoins, a été victime d'une mauvaise gestion et d'un code défectueux ; elle a ainsi perdu 850 000 bitcoins (valant 620 millions de dollars à l'époque). Par ailleurs, si votre portefeuille numérique est rempli de cryptomonnaie et que vous perdez votre mot de passe, cet argent est presque certainement perdu. Comble de l'ironie, certains utilisateurs de cryptomonnaies gardent une copie de leurs codes confidentiels dans un coffre bancaire...

L'engorgement. Comme chaque nouveau bloc ajouté à une blockchain revalide tous les blocs précédents, chaque nœud effectuant la validation a besoin d'une copie de la dernière version en date de la chaîne entière. Avec déjà plus de 150 gigaoctets, la blockchain du bitcoin devient difficile à manipuler. Le registre d'Ethereum, conçu pour être plus flexible (afin de gérer des transactions plus complexes, telles que des contrats intelligents), est déjà plus gros que celui du bitcoin. Si tout le monde se mettait à l'utiliser, les superordinateurs à haute performance seraient-ils les seuls à pouvoir gérer la charge de données ? Il en résulterait une recentralisation du réseau, contraire à l'objectif des registres distribués !

ABONNEZ-VOUS À POUR LA SCIENCE

FORMULE INTÉGRALE -41%

99€

FORMULE PASSION -27%

79€

FORMULE DÉCOUVERTE -25%

59€

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à : Pour la Science - Service abonnements - 19 rue de l'industrie - BP 90 053 - 67 402 Illkirch cedex

❑ OUI, JE M'ABONNE À *POUR LA SCIENCE* POUR 1 AN, JE CHOISIS MA FORMULE CI-DESSOUS :

❑ FORMULE **INTÉGRALE**
12 n° de *Pour la Science* + 4 Hors-Séries
+ Accès illimité aux archives en ligne depuis 1996
I1A99E

99€ Au lieu de ~~168,45€~~*

❑ FORMULE **PASSION**
12 n° de *Pour la Science*
+ 4 Hors-Séries
P1A79E

79€ Au lieu de ~~108,45€~~*

❑ FORMULE **DÉCOUVERTE**
12 n° de *Pour la Science*
D1A59E

59€ Au lieu de ~~78,45€~~*

J'INDIQUE MES COORDONNÉES

❑ M. ❑ Mme

Nom : _____ Prénom : _____

Adresse : _____

_____

Code postal _____ Ville : _____

Téléphone _____

• Mon e-mail : (à remplir en majuscule)

_____@_____

J'accepte de recevoir les informations de *Pour la Science* ❑ OUI ❑ NON
et de ses partenaires ❑ OUI ❑ NON

• Je choisis mon mode de règlement :

❑ Par chèque à l'ordre de *Pour la Science*

❑ Par carte bancaire

N° _____ _____ _____ _____

Date d'expiration : _____ _____ Clé (Les 3 chiffres au dos de votre CB) : _____

Signature obligatoire

PAG18485STDC

* Par rapport au prix de vente en kiosque, l'accès numérique aux archives. Délai de livraison : dans le mois suivant l'enregistrement de votre règlement. Offre réservée aux nouveaux abonnés, valable jusqu'au 30/06/2018 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site www.pourlascience.fr. Conformément à la loi "Informatique et libertés" du 6 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant en adressant un courrier à *Pour la Science*. Photos non contractuelles.

Groupe Pour la Science - Siège social : 170 bis, boulevard du Montparnasse, CS20012, 75680 Paris cedex 14 - Sarl au capital de 32 000€ - RCS Paris B 311 797 393 - Siret : 311 797 393 000 23 - APE 58.14 Z

L'ESSENTIEL

> Augmenter la transparence du système financier moderne réduirait les risques qui lui sont associés, mais cela suppose de modéliser le circuit monétaire à un niveau de détail qui dépasse les capacités techniques actuelles.

> Avec les cryptomonnaies, il est désormais possible de mémoriser et analyser tous les échanges ou transactions. Ces outils permettraient d'élaborer des réseaux financiers plus efficaces et de décentraliser le contrôle de l'argent.

> Bien conçus et utilisés, ces réseaux numériques favoriseront l'équité et la responsabilité. Mais ils pourraient tout aussi bien servir à un contrôle centralisé extrême.

LES AUTEURS

ALEXANDER LIPTON
membre du groupe MIT Connection Science à l'institut de technologie du Massachusetts (MIT), aux États-Unis

ALEX « SANDY » PENTLAND
professeur au MIT et directeur du groupe MIT Connection Science

Faire sauter la banque avec des cryptomonnaies

Les monnaies numériques fondées sur la technologie des blockchains ont un fonctionnement transparent. Elles préfigurent peut-être de nouveaux réseaux financiers qui mettront un terme à la concentration des richesses et qui stimuleront l'économie.

Par une belle journée de printemps, il y a plus de cinq mille ans, dans la cité mésopotamienne d'Ur, un commerçant étranger vendit sa marchandise en échange d'une bonne quantité de métal précieux, de l'argent. Il ne voulait pas ramener ce lot chez lui, sachant qu'il reviendrait à la fin de la saison des moissons acheter du grain. Il décida donc plutôt de se rendre au temple local, où étaient souvent conservés des objets de valeur, et demanda au prêtre de garder le lot d'argent pour lui.

Quelque temps après, le neveu du prêtre se présenta chez son oncle pour solliciter un prêt. Il souhaitait acheter des semences pour avoir ses propres récoltes, souhait qui fit vibrer la corde sensible de l'oncle. Ce dernier prêta donc au jeune homme une partie de l'argent qu'on lui avait confié, faisant le raisonnement que si jamais son neveu ne parvenait pas à le rembourser avant que le commerçant étranger ne le lui réclame, il pourrait remplacer le métal manquant en puisant dans ses fonds propres ou emprunter l'équivalent auprès de ses amis. En utilisant un contrat à long terme avec le commerçant pour financer un prêt à court terme à son neveu, le prêtre doublait le nombre de transactions commerciales effectuées avec le même montant. En d'autres termes, il avait inventé le système de « réserves fractionnaires » (ou de « couverture partielle »).

D'après des données archéologiques, nous savons que des scénarios de ce type se sont joués en Mésopotamie. Et cela a profondément changé l'environnement financier de deux façons : tout d'abord, en augmentant la productivité globale de l'économie – ainsi, le neveu était désormais en mesure de se payer des semences ; en second lieu, en introduisant le risque – puisque le neveu ne serait peut-être pas en mesure de rembourser l'argent à temps.

Quelques millénaires plus tard, dans l'Europe du XVII^e siècle, l'émergence de banques centrales adossées aux États a créé le lien entre de telles « doubles dépenses » et la perception de taxes. Le roi empruntait de l'argent aux marchands afin de financer ses guerres ou la construction de routes, et l'utilisait pour payer >

> les fabricants et fournisseurs d'armes, ainsi que ses troupes. Cet argent commençait à circuler et à engendrer de l'activité économique et des profits, et à chaque étape la quantité d'argent était doublée (ou plus). Généralement, le roi remboursait les prêts à l'aide des impôts levés sur les bénéfices. L'ensemble de ce processus constituait un prototype de circuit monétaire qui a marqué la naissance du système bancaire en vigueur aujourd'hui.

Très schématiquement, le circuit moderne fonctionne de la façon suivante. Tout d'abord, une entreprise emprunte de l'argent à des banques privées telles que JPMorgan Chase ou HSBC pour payer les salaires de ses employés et d'autres frais. C'est l'étape où la monnaie est créée. Puis les consommateurs achètent les biens produits par les entreprises ou déposent leurs liquidités sous forme d'économies à la banque. Enfin, ces entreprises utilisent les sommes qu'elles ont perçues pour rembourser les banques, et la boucle est bouclée. À ce stade, l'argent prêté au départ disparaît, mais les intérêts versés restent dans le système.

C'est ainsi que les banques privées peuvent stimuler les économies en créant de la monnaie *ex nihilo*. Leur capacité à procéder de la sorte est régulée en partie par les banques centrales, qui imposent des limites à la quantité de capital et de liquidités que les banques privées doivent toujours détenir pour financer leurs activités de prêt.

LE SYSTÈME MONÉTAIRE ACTUEL EST DEVENU TROP COMPLIQUÉ À GÉRER ET À RÉGULER

Si seulement tout était si simple ! Le circuit monétaire introduit hélas des problèmes de société fondamentaux. Pour commencer, il se crée inévitablement une poignée de milliardaires qui contrôlent une vaste concentration de la richesse totale. Il est également affligeant de voir combien il est courant de créer de la monnaie par le crédit (par effet de levier) sans en comprendre suffisamment les risques ou s'en soucier. C'est ainsi que se produisent les krachs financiers, tel celui de 2008 : quand les banques et les autorités politiques ont encouragé une demande insatiable d'emprunts, cette demande a été satisfaite par une augmentation notable de la masse monétaire créée, et une augmentation encore plus grande du risque.

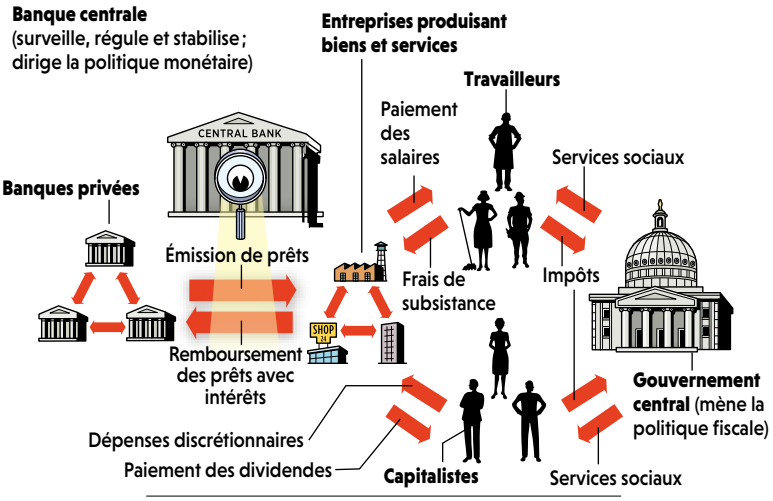
Il peut sembler évident d'imputer ces problèmes au circuit financier lui-même. Mais ce n'est pas le fond de la question. La création d'argent par effet de levier fonctionne bien tant que nous sommes capables de comprendre et de maîtriser ses risques inhérents tout en empêchant une concentration indésirable de richesses. Mais aujourd'hui, un écheveau de facteurs tels que l'explosion démographique, l'internationalisation du commerce et la

TROIS TYPES DE SYSTÈMES FINANCIERS

Le circuit monétaire actuel est devenu trop complexe pour être compris. Des technologies émergentes à « chaînes de blocs », ou blockchains, comme celle qui sert de base au bitcoin, décentralisent (et clarifient) le système. De nouveaux réseaux, tel celui du tradecoin, sont en cours de développement.

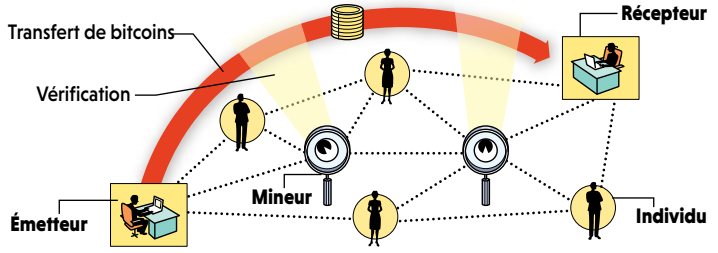
LE SYSTÈME DE RÉSERVES FRACTIONNAIRES (CIRCUIT MONÉTAIRE ACTUEL)

Les banques créent de la monnaie *ex nihilo* lorsqu'elles émettent des prêts aux entreprises. Les entreprises paient les salaires et les dividendes aux ménages. Les ménages achètent des biens et des services aux entreprises. Quand les prêts sont remboursés, la monnaie « créée » est détruite, mais les intérêts versés restent dans le système.



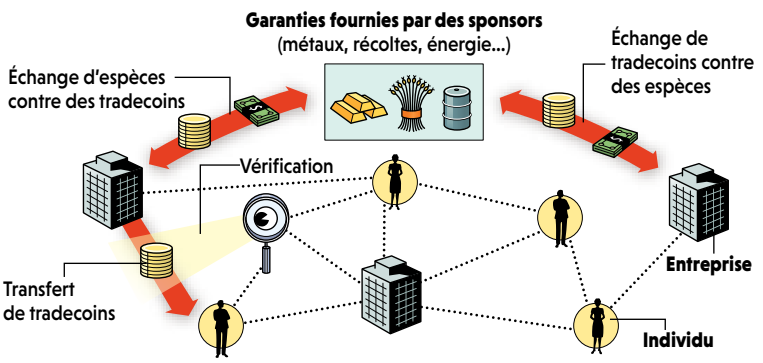
LE RÉSEAU PAIR À PAIR DU BITCOIN

Les transactions se font directement entre utilisateurs, sans l'aide d'intermédiaires désignés. Elles sont publiquement diffusées et enregistrées dans une blockchain. Le consensus est assuré par des « mineurs » qui gagnent des bitcoins s'ils enregistrent de nouveaux blocs. Le bitcoin n'a pas de valeur intrinsèque ; son cours est donc par nature instable.



LE RÉSEAU PAIR À PAIR DU TRADECOIN

Comme avec le bitcoin, les transactions se feront directement entre utilisateurs et seront enregistrées publiquement dans une blockchain. Mais le consensus sera assuré par des validateurs désignés. La valeur du tradecoin sera couverte par des biens réels liés à des sponsors ; son cours sera donc relativement stable.



puissance des ordinateurs rendent le système beaucoup trop compliqué à gérer et à réguler, et à plus forte raison à comprendre.

Le plus inquiétant dans cette affaire, c'est que le principal cadre que nous utilisons pour guider l'activité macroéconomique est fondé sur des paradigmes dépassés. Les modèles généralement utilisés pour régir la création de monnaie et les taux d'intérêt, par exemple, traitent encore les banques privées comme de simples intermédiaires, en ignorant le fait qu'elles constituent des protagonistes majeurs, qui créent activement de l'argent. Les banques ont leurs propres motivations, et leurs stratégies pour engranger des bénéfices introduisent dans le système une grande opacité. Il n'est guère étonnant que la crise des *subprimes* (prêts hypothécaires à risque) de 2008 ait été difficile à voir venir.

Il faudrait modéliser le très complexe circuit monétaire actuel avec un luxe de détails sans précédent pour que nous puissions le comprendre. Les limites technologiques ont longtemps rendu impossible une tâche aussi pharaonique. Mais avec la disponibilité de données massives ainsi que l'émergence des monnaies virtuelles et des contrats numériques, la situation est en train de changer. Plutôt que de s'appuyer sur des moyennes historiques pour estimer ce qui pourrait arriver à un système économique donné, il devient enfin possible de simuler la totalité des échanges et transactions individuels et d'en analyser toutes les conséquences possibles. Cette perspective est en passe d'ébranler le fonctionnement et l'idéologie de la finance globale, et ses implications pourraient grandement améliorer la sécurité économique – ou la dégrader considérablement…

Il y a à peine une dizaine d'années, des techniques autorisant une réinvention de notre système financier sont apparues. Presque tout le monde a entendu parler du bitcoin, mais ce dernier n'est qu'un élément d'une vaste industrie montante de technologies financières, caractérisée par le buzz et la spéculation. Ce qu'il est important de savoir, c'est que l'invention centrale est un « registre distribué », une base de données partagée et gérée par de multiples participants – une sorte de système informatisé et commun de comptabilité.

LES BLOCKCHAINS, TECHNOLOGIE FONDATRICE DES CRYPTOMONNAIES

Ce registre distribué constitue la technologie fondatrice qui a rendu possible l'avènement de cryptomonnaies – des monnaies cryptées numériquement – telles que le bitcoin. Sa structure de données sous-jacente, nommée blockchain, ou chaîne de blocs, consiste en une série de blocs enchaînés les uns à la suite des autres, chaque bloc regroupant un grand nombre de transactions sous forme de données numérisées. La chaîne est mise à jour de façon consensuelle par ajouts de nouveaux blocs au moyen de divers mécanismes de « preuve » faisant intervenir à la fois des humains et des ordinateurs (*voir l'article de John Pavlus, page 28*).

Conceptuellement parlant, les chaînes de blocs et les registres distribués ne sont pas nouveaux; par exemple, des enchaînements se produisent naturellement chaque fois que du pouvoir, des terres ou des biens changent de mains. Ce qui est nouveau, c'est l'association des deux concepts dans un système informatique infalsifiable qui peut être appliqué à un grand éventail de problèmes pratiques. Grâce aux nouvelles techniques de registres distribués fondés sur les blockchains, il est possible de créer des devises numériques beaucoup plus efficaces que le dollar américain ou l'euro, et même plus efficaces que le bitcoin.

Ces outils nous permettraient de suivre et d'analyser les transactions à un niveau suffisamment granulaire pour que nous puissions enfin comprendre le circuit monétaire. Avec un niveau de clarté sans précédent, nous pourrions apprendre à reconnaître de précoces signaux d'alerte se manifestant dans les milliers de milliards de transactions consignées dans le registre, et réagir de façon appropriée, ce qui augmenterait la stabilité et la sécurité du système.

Ce type de suivi à livre ouvert en temps réel serait également plus sûr pour l'ensemble de la communauté. Dans le krach de 2008, par exemple, la capacité administrative était insuffisante pour traiter les pertes individuelles de dizaines de millions de citoyens. En conséquence, les régulateurs se sont concentrés sur le sauvetage des grandes banques, relativement peu nombreuses, laissant les individus ordinaires payer le prix fort. >

BIBLIOGRAPHIE

J. Barrdear et M. Kumhof, **The macroeconomics of central bank issued digital currencies**, document de travail n° 605, Banque d'Angleterre, juillet 2016.

A. Lipton, **Modern monetary circuit theory, stability of interconnected banking network, and balance sheet optimization for individual banks**, *International Journal of Theoretical and Applied Finance*, vol. 19(6), article 1650034, 2016.

T. Hardjono *et al.* (éd.), **Trust : Data. A New Framework for Identity and Data Sharing**, Visionary Future, 2016.

A. Laurent et V. Monvoisin, **Les nouvelles monnaies numériques : au-delà de la dématérialisation**

> À l'heure où cette technologie en évolution rapide commence à être exploitée pour des applications de plus en plus nombreuses et variées, la confusion règne dans de nombreux esprits. Comme le bitcoin est actuellement la forme de monnaie numérique la plus connue (en bien ou en mal, les avis sont partagés), il est utile de revenir un peu en arrière pour explorer ses origines et ses faiblesses, et comprendre en quoi elle diffère des versions plus prometteuses qui sont maintenant à l'étude.

La monnaie bitcoin a été conçue comme un système de paiement numérique pair à pair qui fonctionne sans autorité centrale. N'importe qui peut y adhérer, ce qui est à la fois une force et une faiblesse. Les utilisateurs effectuent entre eux des transactions financières directes (par exemple l'achat d'un bien), sans l'aide d'intermédiaires. Ces transactions sont inscrites dans un registre à blockchain distribué publiquement, que tous les participants peuvent (théoriquement) voir. Depuis la création du bitcoin en 2009, son cours a augmenté de plusieurs ordres de grandeur, ce qui en fait la coqueluche des spéculateurs.

Les promesses du système des bitcoins sont grandes. Ses partisans – essentiellement des idéalistes et libertaires férus de technologie, mais aussi certains criminels – s'attendent à ce que le bitcoin devienne une devise mondiale qui finira par supplanter les devises nationales, facilement manipulables selon eux. Certains enthousiastes voient même dans le bitcoin une version numérique de l'or, oubliant peut-être que l'or tient sa stabilité à la fois de ses attributs physiques et de ses milliards de détenteurs, et que dans le monde numérique les bonnes techniques sont régulièrement dépassées par de meilleures encore.

Le bitcoin n'est d'ailleurs pas la première monnaie virtuelle, et ce ne sera très probablement pas la dernière non plus à jouer dans la cour des grands. Elle souffre par ailleurs de sérieuses contraintes logistiques.

LE BITCOIN N'EST PAS LA PANACÉE

Par exemple, le nombre de transactions qui peuvent être traitées à chaque seconde tourne autour de 7, à comparer avec les 2000 que traite en moyenne le système Visa de cartes de paiement.

De plus, c'est un gouffre à énergie : le minage (le processus par lequel les membres du réseau de cryptomonnaie se font la compétition pour ajouter de nouveaux blocs de transactions à la blockchain, et ainsi gagner des bitcoins) consomme une énorme quantité d'électricité. Dans les pays où l'électricité coûte cher, les mineurs font rapidement faillite s'ils ne peuvent honorer les factures d'électricité des systèmes informatiques. On ne connaît pas

© Borja Bonaque

les chiffres exacts, mais on estime que le système des bitcoins consomme autant d'électricité qu'eBay, Facebook et Google réunis.

Le bitcoin a également été mis en place pour que l'autorité soit répartie entre de nombreux mineurs ; or en se rassemblant pour former de gigantesques pools, un petit nombre de groupes sont devenus suffisamment puissants pour contrôler le système. Peut-on encore parler de pair à pair ?

L'utilisation du bitcoin est de plus limitée. Le terme « monnaie » peut être défini par ses trois types d'utilisation : pour les transactions, comme réserve de valeur et en tant qu'unité de compte. Comme le cours du bitcoin par rapport aux monnaies légales, reconnues par les États, est extrêmement instable, il est difficile à utiliser au quotidien. Le bitcoin et l'ether, une autre grande cryptomonnaie, ne sont pas couverts par des biens réels ni même par des engagements gouvernementaux. Par conséquent, ils sont purement spéculatifs. En termes familiers, cela signifie que ces monnaies numériques ne sont pas de l'argent « véritable » : ce qui n'a pas de valeur ne peut avoir de prix. Certains enthousiastes du bitcoin présentent cette absence de valeur comme un avantage et affirment que, dans le futur, tout l'argent sera du même type que le bitcoin. Cela est hautement improbable, pour des raisons à la fois techniques et politiques.

Cependant, en tant que première monnaie virtuelle décentralisée prospère, le bitcoin

À PROPOS DES AUTEURS

ALEXANDER LIPTON
a fondé une jeune entreprise, StrongHold Labs. Il a auparavant occupé plusieurs hautes fonctions à la Bank of America, et des postes de professeur invité à l'université d'Oxford et à l'Imperial College de Londres.

ALEX « SANDY » PENTLAND
dirige le laboratoire Human Dynamics du MIT, et est notamment membre de l'Académie d'ingénierie des États-Unis.
Son dernier ouvrage en date est *Social Physics* (Penguin Books, 2015).

représente une percée impressionnante. La technologie sous-jacente et la philosophie d'un système financier pair à pair non régulé par une autorité centrale sont innovantes.

Le bitcoin n'est bien sûr que l'une des applications des registres distribués fondés sur des chaînes de blocs. La blockchain, après tout, est une technique, et non une idéologie particulière : on ne devrait pas la confondre avec la philosophie qui anime le système du bitcoin ou avec les motivations de l'une quelconque de ses applications actuelles ou futures. Les blockchains ont certes le potentiel de résoudre certains des problèmes existants de notre système financier, mais on pourrait tout autant les utiliser pour les exacerber. Et quand on considère qu'un élément clé de la puissance est le contrôle de la monnaie (à la fois la masse monétaire existante et la future création de monnaie), on peut déjà avoir un petit aperçu de la boîte de Pandore de dangers moraux que cette technologie a ouverte.

Prenons les banques centrales des principales monnaies de réserve, telles que la Réserve fédérale des États-Unis et la Banque d'Angleterre. La confiance qu'on leur accorde est souvent liée à leur taille (plus c'est grand, plus c'est fiable), mais ces acteurs ont prouvé qu'un tel raisonnement est erroné. Ces banques centrales ont maintes fois pris le parti d'appauvrir les petites gens en diluant leurs obligations financières par le biais de l'inflation, la suppression des taux d'intérêts et autres politiques. Elles ont récemment testé des taux d'intérêt négatifs et envisagé des moyens de se débarrasser de l'argent liquide.

Plus alarmant encore, certaines banques centrales réfléchissent à la possibilité de rendre numériques toutes leurs monnaies et de consigner les achats directement dans un registre. Cela pourrait court-circuiter la contribution des banques privées et conférer aux gouvernements le contrôle absolu de l'économie. Cela signifie également que le gouvernement disposerait d'une trace de tout ce que vous achetez, y compris ce que vous achetez aujourd'hui en espèces précisément pour éviter de laisser une trace écrite.

Cette possibilité semble de moins en moins relever de la science-fiction, et des pays tels que la Chine, le Royaume-Uni, Singapour et la Suède ont annoncé des projets d'étude et éventuellement d'implémentation d'une telle stratégie. La conclusion de tout cela est que la technologie elle-même a beau être décentralisée par conception, on peut l'utiliser pour créer des systèmes à contrôle centralisé.

Il est clair que l'invention des chaînes de blocs et des registres distribués n'éradiquera pas les problèmes de krachs financiers ou d'inflation malsaine, du moins pas à court terme. Mais elle rend possible la création de substituts légitimes aux grands et puissants acteurs. La technologie permet désormais de former des systèmes de monnaie globale spécialisés qui, auparavant, n'auraient pas joui d'une ampleur, d'une confiance ou d'une stabilité politique suffisantes pour se poser en concurrents. C'est pourquoi une prochaine étape naturelle serait que les petits acteurs, tels que des économies émergentes ou un grand nombre de citoyens, se groupent pour former des substituts aux banques centrales.

LE TRADECOIN, POUR UN SYSTÈME FINANCIER PLUS STABLE

En ayant cette possibilité à l'esprit, notre laboratoire au MIT (l'institut de technologie du Massachusetts) travaille à la création d'une monnaie numérique adaptée aux transactions à grande échelle. Dénommée tradecoin, cette monnaie sera enregistrée de manière indélébile dans une chaîne de blocs et adossée à tout instant à un panier de biens réels tels que des récoltes agricoles, de l'énergie ou des minéraux. Cela aidera à stabiliser sa valeur et à la rendre plus fiable aux yeux du public. L'idée centrale est que, pour que son utilité ne soit pas limitée, une monnaie doit à la fois inspirer confiance et reposer sur des systèmes de transaction efficaces.

Un tradecoin numérique et fondé sur un registre distribué permettrait à des alliances de petites nations, d'entreprises, de commerçants, d'associations coopératives d'épargne et de crédit, ou même de fermiers de rassembler suffisamment de biens pour garantir une grande monnaie liquide qui serait potentiellement aussi fiable et au moins aussi efficace que les devises nationales utilisées par la Banque mondiale et le Fonds monétaire international. Les membres de l'alliance Tradecoin seraient dans une certaine mesure protégés des politiques égoïstes adoptées par les gros acteurs. Grâce à la structure cryptographique du système, il serait pour eux plus facile, plus sûr et moins coûteux de se lancer dans le commerce international. Si les membres de l'alliance sont géographiquement et politiquement diversifiés, ils seront probablement mieux immunisés contre le risque de cessation de paiement que s'ils étaient couverts par une unique grosse entité. De fait, c'est exactement ainsi que la Banque d'Angleterre a fait ses débuts en 1694 : en tant qu'alliance de marchands.

Par conception, les principes sur lesquels reposent les monnaies telles que le tradecoin sont fondamentalement différents de ceux des cryptomonnaies telles que le bitcoin, qui ne sont pas garanties par des biens réels et ne font pas intervenir d'alliances. Le tradecoin >

UNE BRÈVE HISTOIRE DE LA MONNAIE

VII^e SIÈCLE AVANT NOTRE ÈRE
Les Lydiens et les Grecs introduisent les pièces de monnaie en métal.

XIV^e SIÈCLE
Les banques marchandes telles que celle des Médicis étendent leur activité à la finance internationale, au commerce et à l'industrie.

XVII^e SIÈCLE
En prêtant la valeur de l'argent déposé, les banquiers stimulent la productivité économique, mais créent aussi de nouvelles sources de risque qui produisent régulièrement des krachs locaux, voire de grandes dépressions. Les banques centrales, qui lient l'activité bancaire et l'impôt, apparaissent.

XVIII^e SIÈCLE
On adopte l'étalon-or, dérivé de systèmes antérieurs où la circulation de monnaie était contrôlée sans grande rigueur par une réserve de métaux précieux. Il en résulte une réduction du risque.

XX^e SIÈCLE
Avec les Accords de Bâle (à partir de 1988), l'étalon-or est remplacé : ces accords stipulent que détenir des biens faciles à vendre est aussi valable que de détenir de l'or.

> permet également d'éviter le processus énergivore de minage en utilisant un réseau de nœuds « validateurs » variés et fiables, désignés au préalable. Les participants peuvent choisir un ensemble de nœuds de validateurs suffisamment divers pour que personne ne puisse soudoyer 51 % des validateurs en même temps. Le résultat est un instrument financier rapide, évolutif et respectueux de l'environnement. Il combine les techniques les plus récentes avec la vieille idée que la pièce d'or possède une valeur intrinsèque, grâce à laquelle elle est suffisamment fiable pour être utilisée loin de son lieu d'origine.

Les monnaies telles que le tradecoin seraient encore plus sûres que les monnaies d'aujourd'hui, car on peut les concevoir de façon à faire apparaître les détails du circuit monétaire, qui sera ainsi plus facile à surveiller. Un contrôle par des partenaires humains reste nécessaire, un peu comme l'Icann (Internet Corporation for Assigned Names and Numbers) contrôle Internet, ou comme des régulateurs tels que le Conseil de la Réserve fédérale supervisent le système bancaire aux États-Unis. De telles monnaies autorisent une comptabilité distribuée simple, ce qui signifie que l'on est capable de modéliser et prédire les risques avec une meilleure fiabilité.

Actuellement, ce type de transparence est impossible, les détails des transactions financières et des contrats étant très confidentiels. Mais si un tel système avait été en place en 2008, il aurait pu effectuer un suivi de la concentration extrême, chez certains opérateurs boursiers, d'obligations adossées à des créances hypothécaires, et on aurait pu simuler en détail les conséquences des changements de valeur de l'immobilier d'habitation. Au lieu de rester cachés, ces lots de crédits immobiliers toxiques auraient pu attirer l'attention comme autant de drapeaux rouges.

DES SYSTÈMES LOGICIELS POUR « RÉSEAUX DE CONFIANCE »

Nous nous sommes attaqués à ces défis concernant la transparence. Par exemple, nous construisons des systèmes logiciels de « réseau de confiance » que les États de l'Union européenne et des sociétés financières aux États-Unis utiliseront comme programme pilote. Ils permettront d'enregistrer et de « rejouer » les transactions et les contrats entre les différentes parties sans révéler les données propriétaires ou violer la confidentialité. Ces logiciels forment également le système au cœur du tradecoin. Nous explorons les façons de piloter deux monnaies tradecoin : l'une à destination du commerce international et garantie par une alliance de petits États, et l'autre garantie par des agriculteurs pour une utilisation sur les marchés des matières premières. Nous sommes en train de recruter des membres pour constituer l'alliance qui testera l'idée.

On entrevoit des monnaies numériques mondiales à l'abri des politiques égoïstes des banques centrales

Il est passionnant d'entrevoir, pour la première fois dans l'histoire, la concrétisation de monnaies numériques mondiales qui soient en grande partie à l'abri des politiques égoïstes des riches banques centrales, lesquelles contrôlent jusqu'ici l'essentiel des masses monétaires. Et de fait, émergera probablement une vague de nouveaux systèmes dont quelques-uns pourraient, à terme, prendre suffisamment d'importance pour se hisser au même niveau que les plus grandes monnaies de réserve et leur faire concurrence.

Le fait que nous soyons aujourd'hui en mesure de créer des systèmes monétaires véritablement compréhensibles signifie que nous avons le potentiel de construire les outils pour minimiser les risques, éviter les krachs et protéger les libertés individuelles face aux gouvernements intrusifs et aux corporations trop puissantes. Et parce qu'elles seront garanties par (et convertibles en) des biens traditionnels, elles auront une valeur de référence réelle. Cela signifie qu'elles risqueront moins d'être la cible d'attaques spéculatives et qu'elles résisteront bien tant aux manipulations politiques qu'à l'inflation due aux problèmes particuliers de certains États.

Ensemble, les cryptomonnaies de la prochaine génération telles que le tradecoin pourraient réduire considérablement les frictions dans le commerce international, même dans le chaos du climat politique et économique actuel. En conséquence, les principales devises telles que le dollar américain pourraient perdre leur position de domination absolue, ou bien le système financier américain se verrait obligé d'améliorer son comportement. On espère ainsi que ces systèmes distribués, garantis par de vastes alliances d'acteurs variés, apporteront au monde davantage de transparence, de responsabilité et d'équité. ■

BIBLIOGRAPHIE

J. Barrdear et M. Kumhof, **The macroeconomics of central bank issued digital currencies**, document de travail n° 605, Banque d'Angleterre, juillet 2016.

A. Lipton, **Modern monetary circuit theory, stability of interconnected banking network, and balance sheet optimization for individual banks**, *International Journal of Theoretical and Applied Finance*, vol. 19(6), article 1650034, 2016.

T. Hardjono *et al.* (éd.), **Trust : Data. A New Framework for Identity and Data Sharing**, Visionary Future, 2016.

A. Laurent et V. Monvoisin, **Les nouvelles monnaies numériques : au-delà de la dématérialisation de la monnaie et de la contestation des banques**, *Revue de la régulation*, vol. 18, pp. 1-24, 2015, (http://journals.openedition.org/regulation/11524).

ABONNEZ-VOUS À POUR LA SCIENCE EN TOUTE LIBERTÉ

FORMULE INTÉGRALE -42%

8,20€*

FORMULE PASSION -28%

6,50€*

FORMULE DÉCOUVERTE -25%

4,90€*

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à : Pour la Science - Service abonnements - 19 rue de l'industrie - BP 90 053 - 67 402 Illkirch cedex

❑ OUI, JE M'ABONNE À *POUR LA SCIENCE* EN PRÉLÈVEMENT AUTOMATIQUE, JE CHOISIS MA FORMULE ET JE COMPLÈTE L'AUTORISATION DE PRÉLÈVEMENT CI-DESSOUS.

❑ FORMULE **INTÉGRALE**
12 n° de *Pour la Science* + 4 Hors-Séries
+ Accès illimité aux archives en ligne depuis 1996

8,20€ Par mois -42%
IPV8E20

❑ FORMULE **PASSION**
12 n° de *Pour la Science*
+ 4 Hors-Séries

6,50€ Par mois -28%
PPV6E50

❑ FORMULE **DÉCOUVERTE**
12 n° de *Pour la Science*

4,90€ Par mois -25%
DPV4E90

MES COORDONNÉES

Nom : _____
Prénom : _____
Adresse : _____
_____
Code postal |_|_|_|_|_|
Ville : _____
Tél. Pour le suivi client (facultatif) : |_|_|_|_|_|_|_|_|_|_|
E-mail obligatoire : _____@_____

J'accepte de recevoir les informations de *Pour la Science* ❑ OUI ❑ NON
et de ses partenaires ❑ OUI ❑ NON

MANDAT DE PRÉLÈVEMENT SEPA

PAG18485STDP

En signant ce mandat SEPA, j'autorise Pour la Science à transmettre des instructions à ma banque pour le prélèvement de mon abonnement dès réception de mon bulletin. Je bénéficie d'un droit de rétractation dans la limite de 8 semaines suivant le premier prélèvement. Plus d'informations auprès de mon établissement bancaire.

TYPE DE PAIEMENT : PAIEMENT RÉCURRENT

Titulaire du compte
Nom : _____
Adresse : _____
Code postal |_|_|_|_|_| Ville : _____

Désignation du compte à débiter
BIC (Identification internationale de la banque) |_|_|_|_|_|_|_|_|_|_|_|
IBAN |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
(Numéro d'identification international du compte bancaire)

Établissement teneur du compte
Nom : _____
Adresse : _____
Code postal |_|_|_|_|_| Ville : _____

Date et signature

Organisme Créancier : Pour la Science
170 bis, bd. du Montparnasse – 75014 Paris
N° ICS FR92ZZZ426900
N° de référence unique de mandat (RUM)

Merci de joindre impérativement un RIB

Partie réservée au service abonnement. Ne rien inscrire

* Par mois et par rapport au prix de vente en kiosque, l'accès numérique aux archives. Délai de livraison : dans le mois suivant l'enregistrement de votre règlement. Offre réservée aux nouveaux abonnés, valable jusqu'au 30/06/2018 en France métropolitaine. Pour un abonnement à l'étranger, merci de consulter notre site www.pourlascience.fr. Conformément à la loi "Informatique et libertés" du 6 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant en adressant un courrier à *Pour la Science*. Votre abonnement en prélèvement est reconduit automatiquement et peut être interrompu par simple lettre. Photos non contractuelles.

Groupe Pour la Science - Siège social : 170 bis, boulevard du Montparnasse, CS20012, 75680 Paris cedex 14 - Sarl au capital de 32 000€ - RCS Paris B 311 797 393 - Siret : 311 797 393 000 23 - APE 58.14 Z