et de n'importe où. C'est ce qui, dans le cas du bitcoin, permet de calculer le solde des comptes. Les systèmes de signatures cryptographiques garantissent que les messages de transaction que vous inscrivez sur la *blockchain* ont été écrits et signés par vous et vous seul. L'ordre des inscriptions fournit aussi une datation des transactions (horodatage) et donc les ordonne. Tout cela est fait sans l'intervention d'une quelconque autorité centrale, puisque ce sont certains des utilisateurs (dénommés mineurs dans le cas du bitcoin) qui en opèrent la surveillance, et qui se contrôlent mutuellement, assurant l'honnêteté des sauvegardes et leur cohérence.

L'exemple de la monnaie bitcoin est la plus spectaculaire et la plus visible aujourd'hui des merveilles que réalise une *blockchain*. Qu'on ait pu ainsi créer une monnaie grâce à un fichier partagé semble incroyable. D'autant plus qu'il s'agit d'une monnaie d'un nouveau type : elle ne repose sur aucune autorité émettrice et autorise des transactions quasi instantanées et gratuites d'un point à l'autre du globe *(voir la rubrique Logique & calcul dans Pour la Science de décembre 2013)*.

Au-delà de l'exemple du bitcoin, c'est l'ensemble de tout ce que rend possible une *blockchain* que nous voulons évoquer, car un nouveau monde économique, social, administratif et politique pourrait en sortir, dont on n'a pas pris la mesure.

Le bitcoin utilise une *blockchain* qui lui est propre et ne sert, *a priori*, qu'à inscrire des transactions. Cependant, l'idée de cette *blockchain* se décline d'une multitude de manières qui donnent naissance à autant d'applications nouvelles. Il s'agit là d'un nouveau type d'objets contenant des informations d'une complexité presque sans limites. Nos ordinateurs aux extraordinaires capacités de calcul y accèdent instantanément, en explorant ce qui s'y trouve, en y déposant de nouveaux messages éventuellement cryptés, et en les extrayant rapidement. Ces nouveaux objets, du fait de leur nature numérique et de leurs robustesse et ubiquité, ont des propriétés tout à fait inédites.

Il existe aujourd'hui des centaines de variantes du modèle bitcoin. Ce sont essentiellement d'autres cryptomonnaies, dont chacune s'appuie sur une *blockchain* particulière. Comme l'idée de Nakamoto est beaucoup plus générale, d'autres systèmes à *blockchain* apparaissent ou sont en cours de développement.

Certaines des idées évoquées au départ peuvent se mettre en place soit grâce à une nouvelle *blockchain*, soit en essayant d'utiliser la *blockchain* du bitcoin qu'on détournera de sa fonction première pour lui faire réaliser des opérations non prévues par Satoshi Nakamoto. L'Américain Dom Steil, un entrepreneur s'occupant du bitcoin et auteur de nombreux articles sur les nouvelles technologies, a exprimé l'idée de cette révolution :

« La *blockchain* est intrinsèquement puissante du fait que c'est la colonne vertébrale d'un nouveau type de mécanisme de transfert et de stockage distribué et *open source*. Elle est le tiers nécessaire pour le fonctionnement de nombreux systèmes à base de confiance. Elle est la feuille universelle d'équilibrage utilisée pour savoir et vérifier qui détient divers droits numériques. De même qu'Internet a été la base de nombreuses applications autres que le courrier électronique, la *blockchain* sera la base de bien d'autres applications qu'un réseau de paiement. Nous en sommes aux premiers instants d'un âge nouveau pour tout ce qui est possible au travers d'un réseau décentralisé de communications et de calculs. »

« Une avancée technique majeure qui, à terme, pourrait révolutionner Internet et l'industrie de la finance. »

Le Canadien Jon Evans, un ingénieur informaticien et journaliste spécialisé dans les nouvelles technologies, partage cet enthousiasme : « La technologie *blockchain* au cœur du bitcoin est une avancée technique majeure qui, à terme, pourrait révolutionner Internet et l'industrie de la finance ; les premiers pas de cette révolution à venir ont maintenant été franchis. [...] La *blockchain*, le moteur qui sert de base au bitcoin, est un système distribué de consensus qui permet d'exécuter des transactions et d'autres opérations de manière sécurisée et contrôlée, sans autorité centrale de supervision, cela (en simplifiant) parce que les transactions et toutes les opérations sont validées par le réseau entier. Les opérations effectuées ne sont pas nécessairement financières et les données ne sont pas nécessairement de l'argent. Le moteur qui donne sa puissance au bitcoin est susceptible d'un large éventail d'autres applications. »

Parmi les *blockchains* autres que celle du bitcoin et ayant pour objets des applications non liées à la monnaie, il faut citer *Namecoin*, un système décentralisé d'enregistrement de noms : on écrit sur la *blockchain* de *Namecoin* des paires {nom, message}. L'un des objectifs de *Namecoin* est la mise en place d'un système d'adresses pour les ordinateurs connectés au réseau, système qui pourrait se substituer à l'actuel DNS (*Domain Name System*) en partie aux mains d'organisations américaines.

Les créateurs de cette *blockchain* affichent les objectifs suivants : protéger la liberté d'expression en ligne en rendant le Web plus résistant à la censure ; créer un nom de domaine « .bit » dont le contrôle serait totalement décentralisé ; mémoriser des informations d'identité telles que des adresses électroniques ou des clefs cryptographiques publiques. Ils évoquent aussi la possibilité d'organiser des votes ou des services notariés. Malheureusement, cette *blockchain* est aujourd'hui peu commode, car les dépôts d'informations y sont payants (en namecoins, une cryptomonnaie), et même si les coûts sont très faibles, ils compliquent son utilisation.

Plus récemment a été créé *Twister,* un système concurrent de *Twitter* (le système de microblogage bien connu), mais totalement décentralisé et donc libre de toute censure ou contrôle. La *blockchain* de *Twister* ne sert pas à stocker toute l'information de la plateforme de microblogage (distribuée sur un réseau pair à pair, ce qui évite que les nœuds du réseau aient à gérer

Pas de fausse *blockchain* !

Pour rendre une *blockchain* robuste et impossible à simuler, on utilise une fonction de hachage *h* (publique) qui à tout fichier F associe un code *h*(*F*), une courte suite de caractères dénommée empreinte.

Quand on change un seul caractère de F, le code *h*(F) est totalement changé et ce de façon imprévisible. Il est impossible en pratique de modifier F en F' de manière que *h*(F) = *h*(F') *(voir la rubrique Logique & calcul d'avril 2014).*

On utilise aussi une preuve de travail. C'est une fonction *p* qui, à toute valeur *V* donnée (en général, *V* est une suite de caractères qui détermine un problème), associe une solution *p*(*V*) qui ne s'obtient qu'en menant un long calcul, par exemple d'une durée d'une heure avec une machine de bureau ordinaire. En revanche, vérifier que *p*(*V*) est la bonne valeur associée à *V* est rapide. Calculer le résultat *R* de *p*(*V*) est difficile, mais vérifier que *p*(*V*) = *R* est facile. Un exemple est la décomposition d'un nombre en facteurs premiers, qui est difficile, alors que la vérification que le produit de ces facteurs donne le bon résultat est facile.

Construisons une *blockchain* en concaténant des *blocks* contenant des suites de caractères représentant des messages, ou des transactions : *blockchain* = *block*(1) - *block*(2) - ... - *block*(*n*)

Le *block*(*i*) commence par deux informations particulières *h*(*i*) et *p*(*i*) ajoutées aux messages qui en constituent le contenu. Ces informations *h*(*i*) et *p*(*i*) assurent qu'on ne pourra ni modifier la *blockchain*, ni fabriquer après coup de fausses *blockchains*.

h(*i*) sera l'empreinte de ce qui précède *block*(*i*). Autrement dit, *h*(*i*) = *h*[*block*(1) - ··· - *block*(*i* – 1)].

p(*i*) sera une preuve de travail associée à *h*(*i*) : *p*(*i*) = *p*[*h*(*i*)].

Le calcul des *h*(*i*) et *p*(*i*) se fera progressivement avec l'ajout des *blocks*. Chaque *p*(*i*) exige peut-être une heure de calcul en moyenne, mais résulte d'un calcul collectif qui a pris beaucoup moins qu'une heure par participant. Le calcul de tous les *p*(*i*) se fait progressivement : pour le bitcoin, on a ajouté un *block* toutes les dix minutes depuis janvier 2009 et l'on rétribue ceux qui mènent les calculs.

Quand la *blockchain* comporte de nombreuses pages (la *blockchain* du bitcoin en a environ 300 000), faire une fausse *blockchain* est impossible, car cela demande trop de calculs. Pour 300 000 pages « coûtant » chacune une heure de calcul, il faudrait faire un calcul de 300 000 heures, soit 34 années (et pour le bitcoin, il existe d'autres garde-fous qui font que le calcul est bien plus long). Cependant, vérifier que la *blockchain* est cohérente est facile :

1) On vérifie que chaque *h*(*i*) est convenable en recalculant sa valeur, ce qui est possible car tout est public. C'est rapide et cela assure que rien n'a été modifié dans les *blocks*. 2) On vérifie les *p*(*i*), ce qui est rapide aussi.

Une telle *blockchain* est un objet numérique que chacun peut contrôler rapidement, mais que personne ne peut modifier sans se faire repérer et que personne ne peut imiter, car pour cela il faudrait mener un énorme calcul.

© YinYinPhoto/shutterstock.com

de trop gros volumes de données), mais seulement les informations d'enregistrement et d'authentification. Les messages sont gérés par un système de dépôt distribué (c'est-à-dire répartis entre les utilisateurs) avec une table permettant de savoir où se trouvent les informations, comme cela se pratique dans les réseaux pair à pair de partage de musique.

Un projet plus ambitieux, car se voulant le support possible d'applications complexes fondé sur une notion de contrat *(smart-contract)*, est en cours de développement : il se nomme *Ethereum*. La *blockchain* associée émettra une monnaie (des *éthers*) sur le modèle du bitcoin, mais ce ne sera qu'une de ses fonctions.

Relier les chaînes

Une autre avancée toute récente dans ce domaine a été proposée par un groupe de chercheurs associé à Adam Back, inventeur britannique d'un système de preuve de travail *(voir cette rubrique dans Pour la Science d'avril 2014)* utilisé comme élément du protocole du bitcoin. Adam Back et ses collègues ont constaté que le bitcoin évolue très lentement, les décisions pour tout changement se faisant selon un processus où il faut un accord difficile à obtenir de la part de ceux qui travaillent à le surveiller et qui ne sont pas organisés en structure hiérarchique : c'est un problème avec les applications totalement décentralisées dont le contrôle n'est aux mains de personne.

Adam Back a aussi noté que beaucoup d'idées innovantes proposées par des *blockchains* nouvelles n'ont qu'un succès limité ; en valeur, le bitcoin reste très dominant parmi les monnaies cryptographiques. Lui et ses collègues ont donc mis au point une méthode liant les *blockchains*. Ce système de *sidechain* permettra de faire passer des unités monétaires d'une chaîne A vers une autre, B. Elles disparaîtront de la chaîne A pour réapparaître sur B et pourront éventuellement revenir dans A.

Chaque *blockchain* est un petit univers où il est utile de disposer d'une monnaie (comme sur *Namecoin*) ; cependant, faire accepter une nouvelle monnaie et stabiliser