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