LOGIQUE & CALCUL

Les *blockchains*, clefs d'un nouveau monde

On sait maintenant réaliser des supports inscriptibles, partagés et infalsifiables. Ce qu'il est possible d'en faire est étonnant, formidable… et révolutionnaire.

Jean-Paul DELAHAYE

Imaginez qu'à la place de la Concorde à Paris, à côté de l'obélisque, on installe un très grand cahier que, librement et gratuitement, tout le monde puisse lire, sur lequel chacun puisse écrire, mais qui soit impossible à modifier et indestructible. Cela serait-il utile ? Il semble que oui.

On pourrait y consigner des engagements, comme : « Je promets de donner ma maison à celui qui prouvera la conjecture de Riemann ; signé Jacques Dupont, 11 rue Martin à Paris. » On pourrait y déposer la description de ses découvertes, afin qu'il soit impossible d'en être dépossédé. On pourrait y laisser des reconnaissances de dettes, considérées valides tant que le prêteur n'est pas venu indiquer sur le cahier qu'il a été remboursé.

On pourrait y déposer des messages adressés à des personnes qu'on a perdues de vue, en espérant qu'elles viennent les lire et reprennent contact. On pourrait y consigner des faits que l'on voudrait rendre publics définitivement, pour que l'histoire les connaisse, pour aider une personne dont on souhaite défendre la réputation, pour se venger, etc.

Pour que cela soit commode et pour empêcher les tricheurs de prendre des engagements en votre nom ou écrire en se faisant passer pour vous, il faudrait que l'on puisse signer les messages déposés de telle façon que personne ne puisse se substituer à vous. Il serait utile aussi que l'instant précis où est inscrit un texte soit indiqué à chaque fois (horodatage).

Imaginons que tout cela soit possible et qu'un tel cahier soit mis en place, auquel s'ajouteraient autant de pages nouvelles que nécessaire. Testaments, contrats, certificats de propriétés, messages publics ou adressés à une personne particulière, attestations de priorité pour une découverte, etc., tout cela deviendrait facile sans notaire ni huissier. Un tel cahier public, s'il était permanent, infalsifiable, indestructible et qu'on puisse y écrire librement et gratuitement tout ce qu'on veut, aurait une multitude d'usages.

Public, infalsifiable et indestructible

Un tel objet serait plus qu'un cahier de doléance ou un livre d'or, qui peuvent être détruits. Plus qu'un tableau d'affichage offert à tous sur les murs d'une entreprise, d'une école ou d'une ville, eux aussi temporaires. Plus que des enveloppes déposées chez un huissier, coûteuses et dont la lecture n'est pas autorisée à tous. Plus qu'un registre de brevets, dont la permanence est assurée, mais sur lesquels il est difficile d'écrire. Plus que les pages d'un quotidien, indestructibles car multipliées en milliers d'exemplaires, mais auxquelles peu de gens ont accès et dont le contenu est très contraint.

Bien sûr, ce cahier localisé en un point géographique unique ne serait pas très commode pour ceux qui habitent loin de Paris. Bien sûr, ceux qui y rechercheraient des informations en tournant les pages se gêneraient les uns les autres et gêneraient ceux venus y inscrire de nouveaux messages. Bien sûr encore, faire des recherches pour savoir ce qui est écrit dans le cahier deviendrait impossible en pratique quand le cahier serait devenu trop gros et que ses utilisateurs se seraient multipliés.

Ces trois inconvénients majeurs – localisation unique rendant l'accès malcommode et coûteux, impossibilité d'y lire ou écrire en nombre au même instant, difficultés de manipuler un grand cahier – peuvent être contournés. L'informatique moderne, avec la puissance de ses machines, y compris les smartphones et ses réseaux de communication, est en mesure de les surmonter.

Cette idée d'un grand cahier informatique, partagé, infalsifiable et indestructible

UN GRAND CAHIER IMPOSSIBLE À EFFACER

et mis à la disposition de tous, par exemple sur la place de la Concorde à Paris, serait-il utile ? Oui, si ce cahier est informatisé. Il pourrait donner plus de liberté et dispenser du recours à des autorités administratives, monétaires, juridiques, etc. De tels « grands cahiers partagés » existent aujourd'hui grâce au réseau Internet : les *blockchains*. Il s'en crée chaque jour de nouveaux. Les *blockchains* sont notamment à l'origine d'un nouveau type de monnaies – les cryptomonnaies, telles que le fameux bitcoin. Cependant, bien d'autres applications sont possibles : systèmes universels de courrier, instruments notariés et financiers décentralisés, systèmes de votes en ligne sécurisés, etc.

du fait même de sa conception est au cœur d'une nouvelle révolution, celle de la *blockchain*, ou plus explicitement et en français : la révolution de la programmation par un fichier partagé et infalsifiable.

Une idée mise en œuvre pour les bitcoins

Le terme *blockchain* vient du bitcoin, la monnaie cryptographique créée en janvier 2009 et qui a depuis connu un développement considérable et un succès réel, la valeur d'échange des bitcoins émis dépassant aujourd'hui deux milliards d'euros. Au cœur de cette monnaie, il y a effectivement un fichier informatique infalsifiable et ouvert. C'est celui de toutes les transactions, et son inventeur Satoshi Nakamoto l'a nommé *blockchain*.

C'est un fichier partagé : tout le monde peut le lire et chacun y écrit les transactions qui le concernent, ce qui les valide. La *blockchain* existe grâce à un réseau pair à pair, c'est-à-dire géré sans autorité centrale par les utilisateurs eux-mêmes. Certains de ces utilisateurs détiennent des copies de la *blockchain,* qui se trouve donc présente partout dans le monde. Ces centaines de copies sont sans cesse mises à jour simultanément, ce qui rend la *blockchain* totalement indestructible, à moins d'une catastrophe qui toucherait toute la planète. Ce fichier a été rendu infalsifiable par l'utilisation de procédés cryptographiques qui, depuis sa création en 2009, résistent à toutes les attaques : personne n'a pu effacer ou modifier le moindre message de transaction déjà inscrit dans la *blockchain* du bitcoin *(voir l'encadré page 83)*.

Le rêve du grand cahier de la place de la Concorde est ainsi devenu réalité. D'ailleurs, ce que l'informatique moderne, les réseaux et la cryptographie ont créé dans le monde numérique est bien supérieur à tout ce qu'on aurait pu faire avec du papier, du métal ou des dispositifs matériels usuels.

La *blockchain* évite les trois inconvénients majeurs cités précédemment. Grâce aux réseaux, on y accède instantanément de n'importe où dans le monde, pourvu qu'on dispose d'un ordinateur ou d'un smartphone. Des milliers d'utilisateurs peuvent le consulter simultanément sans se gêner. Et chacun peut, gratuitement et sans limitation, ajouter de nouveaux messages de transactions selon un procédé qui assure la cohérence et la robustesse du fichier *blockchain*.

La *blockchain* du bitcoin augmente en taille peu à peu, mais elle reste manipulable par les formidables machines dont nous disposons tous aujourd'hui. Elle comporte aujourd'hui 28 gigaoctets ($2{,}8 \times 10^{10}$ caractères), soit l'équivalent d'environ 28 000 ouvrages de 200 pages.

Avec un ordinateur et une connexion, on accède librement à tout le contenu de cette *blockchain,* presque instantanément

Philippe Boulanger

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