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

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.

© YiinPhoto/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

Mieux que *Leboncoin*, *eBay*, *Priceminister*, etc.

Le commerce entre particuliers sur Internet est freiné par un problème de confiance. Vous mettez en vente un magnifique vase, vous trouvez un acheteur, vous lui envoyez l'objet… et il ne vous paye jamais – ou, à l'inverse, il vous envoie l'argent et vous gardez le vase…

Même si c'est malhonnête, il est économiquement rationnel pour celui qui reçoit l'envoi de son correspondant de ne pas envoyer ce qu'il a promis en échange. *eBay* précise d'ailleurs : « Nous ne pouvons pas obliger le vendeur à remplir ses obligations. »

Leboncoin recommande l'échange en direct avec rencontre. L'envoi contre remboursement est une solution et certains sites (parfois associés à *Paypal*) proposent leurs services pour limiter les risques. Soit ils bloquent l'argent envoyé avant que le produit ne soit reçu ; soit ils proposent un système de notation qui indique si les personnes avec qui on fait affaire ont été correctes dans leurs précédentes transactions ; soit ils proposent une assurance.

Il existe pourtant une meilleure solution grâce aux *blockchains*. Oleg Andreev a proposé un système inspiré par la *blockchain* du bitcoin, qui résout le problème sans frais. L'idée s'applique à toute *blockchain* disposant d'un système d'unités monétaires permettant les transactions à plusieurs entrées et plusieurs sorties (c'est le cas de la *blockchain* du bitcoin).

Supposons qu'Alain veuille vendre un vase à 100 euros à Béatrice qui habite loin. Ils sont d'accord sur le prix, mais doivent faire l'échange à distance. Alain et Béatrice, indépendamment des 100 euros convenus, déposent chacun 200 euros sur un compte particulier. Lorsque l'échange sera terminé (envoi du vase et envoi des 100 euros pour le payer), Alain et Béatrice signeront la transaction qui débloquera les 400 euros, lesquels seront alors restitués : 200 pour Alain, 200 pour Béatrice.

La procédure de mise sous séquestre sur la *blockchain* est telle que personne ne peut s'emparer de cet argent, sauf Alain et Béatrice s'ils donnent tous deux leur accord. Seul, aucun d'eux ne peut rien faire. En conséquence, à moins d'être prêt à perdre 200 euros pour un objet qui en vaut 100, Béatrice aura intérêt à payer le vase. De même, si Béatrice paye avant de recevoir le vase, Alain aura intérêt à envoyer le vase (qui vaut 100 euros) pour récupérer ses 200 euros bloqués. Il est ainsi économiquement rationnel de se comporter honnêtement !

La somme de 200 euros pour une transaction concernant un objet qui en vaut 100 est modifiable, mais il faut que la somme mise sous séquestre par les deux acteurs soit supérieure à la valeur de l'objet échangé. Sinon, celui qui reçoit l'envoi de l'autre en premier aura intérêt à ne pas envoyer ce qu'il doit, quitte à perdre la somme séquestrée. Ce système à base de *blockchain* permet, sans l'action d'aucune autorité centrale, de mener une opération d'échange avec un risque très réduit de se faire escroquer (pour des précisions sur la mise en œuvre technique, voir http://bit.ly/1BuoupD ou http://voluntary.net/bitmarkets/).

son cours est difficile et incertain. De plus, chaque *blockchain* est une expérience aux risques d'autant plus grands qu'elle est récente et innovante. Une fois mis en place, le système des *sidechains* (ce n'est pas si simple et, aujourd'hui, aucune *sidechain* ne fonctionne) permettra de tester rapidement de nouvelles idées. Chacune pourra « importer » la monnaie d'une autre *blockchain*, sans doute le bitcoin, la monnaie la mieux installée et celle pour laquelle la confiance est la plus forte. Le système est conçu pour que la chaîne qui « prête » de l'argent à une autre n'engage pas plus que ce qu'elle prête ; elle ne prend donc pas de risque.

Avec un tel système, non seulement les diverses *blockchains* ne se concurrenceront plus nécessairement, toutes pouvant s'appuyer sur une seule ou un petit nombre d'entre elles, mais de plus toutes les expérimentations pourront être envisagées sans crainte, créant une dynamique propice aux innovations.

Plutôt que d'expliquer les architectures complexes et spécifiques de *Namecoin, Twistter* ou *Ethereum*, terminons en présentant les applications générales les plus simples d'une *blockchain*.

Des outils cryptographiques

Une *blockchain* est un fichier numérique accessible à tous en lecture et en écriture. Cela se fait par l'utilisation de logiciels parfois nommés *servents,* terme qui associe les deux mots *client* et *serveur* utilisés dans les réseaux centralisés. Ce mot marque que, dans un réseau pair à pair, chaque nœud est à la fois nœud central (serveur) et utilisateur (client).

Le fichier *blockchain* est rendu infalsifiable et indestructible par l'utilisation d'outils cryptographiques. Quand on ajoute quelque chose au fichier (on parle de *page* ou de *block*), on le fait en commençant l'ajout par un code calculé à partir de la version avant ajout (pour calculer ces codes, on utilise des fonctions de hachage). On ne pourra donc pas modifier la partie ancienne de la *blockchain* sans que cela se voie, ou alors il faudrait modifier chacun des codes commençant les pages : les codes rigidifient le fichier.

De plus, pour qu'il soit difficile de fabriquer une *blockchain* entièrement artificielle avec de bons codes en tête de chaque page ajoutée et qui prétendrait se substituer à la vraie *blockchain*, le protocole de gestion exige qu'on fasse un certain travail de calcul pour ajouter une page ; c'est la notion de *preuve de travail (voir l'encadré page 83)*. Par conséquent, fabriquer une fausse *blockchain*, ou même seulement une fausse partie finale de *blockchain*, est excessivement coûteux, voire impossible, en pratique. Au total, le fichier *blockchain* ne peut être ni modifié ni simulé. Comme la *blockchain* existe en une multitude de

copies (une chez chacun de ceux qui acceptent de participer à la bonne marche du protocole), la *blockchain* d'une application particulière est indestructible et impossible à truquer.

La taille de la *blockchain* augmente à mesure qu'y sont déposés de nouveaux messages ou de nouvelles pages regroupant plusieurs messages. Les multiples copies de la *blockchain* sont toutes maintenues identiques grâce aux échanges d'informations opérés par le réseau pair à pair.

L'accroissement de taille de la *blockchain* est bien sûr un grave problème. Aujourd'hui, on peut manipuler des *blockchains* de plusieurs dizaines de gigaoctets, mais on ne peut pas en manipuler qui seraient 1 000 fois plus grandes. La technologie de demain le permettra peut-être, mais il y aura toujours une limite, certes élevée, à prendre en compte.

Bien évidemment, une *blockchain* peut servir à déposer anonymement des messages. Grâce au logiciel installé sur sa machine (le *servent*) et propre à la *blockchain*, on ira écrire tout ce qu'on souhaite. Pour éviter que les interventions sur la *blockchain* se fassent avec une trop grande fréquence (ce qui rendrait difficile la synchronisation de tous les détenteurs d'une copie), le protocole de fonctionnement pourra ajouter les messages par page, chaque page en contenant plusieurs centaines ou milliers ; ainsi, pour le bitcoin, les transactions sont regroupées et ajoutées une fois toutes les dix minutes.

Les messages qu'on ajoutera sur une *blockchain* seront anonymes ou signés. Avec les systèmes de signature à double clef, tout le monde peut vérifier l'auteur d'un message signé et il est impossible que quelqu'un signe à la place d'un autre.

Les messages ajoutés seront en clair ou chiffrés. On pourra ainsi déposer un message chiffré qu'on ne rendra lisible que plus tard en publiant la clef de déchiffrement. Ce sera utile dans le cas d'un engagement (tel qu'une reconnaissance de dette) pris vis-à-vis d'un débiteur, vous par exemple. Votre engagement est présent signé, daté et crypté sur la *blockchain*. Si vous le respectez, il reste crypté. Sinon, celui envers qui vous êtes engagé publie la clef de déchiffrement et tout le monde voit que vous ne tenez pas votre engagement. Grâce à la signature, il n'y a pas de doute, c'est bien vous qui avez pris l'engagement. Cette publication détruit votre réputation ou même sert de preuve devant un tribunal.

Une *blockchain* peut servir à concevoir une messagerie universelle. Pour qu'il y ait confidentialité des messages et garantie sur leurs auteurs, on utilisera là aussi la cryptographie asymétrique. Celui qui veut déposer la démonstration d'un théorème qu'il a trouvée, mais sans la rendre publique, déposera la version cryptée avec une clef privée (créée pour cet usage) et il signera le dépôt. Quand, plus tard, il voudra prouver qu'il disposait bien, dès la date de dépôt, de la démonstration, il rendra publique la clef de déchiffrement. Plus besoin des enveloppes *Soleau* déposées à l'Institut national de la propriété industrielle. Bien sûr, on pourra de la même façon déposer des engagements, des testaments, des œuvres signées, etc.

Une forme numérique d'anarchisme

Insistons sur le fait qu'un tel système de *blockchains* permettant signatures, contrats, dépôt de testaments, etc. n'exige l'action d'aucune autorité centrale pour fonctionner. Tout ira bien pourvu que le fichier *blockchain* soit maintenu, c'est-à-dire qu'un minimum d'utilisateurs participe à son entretien en en gardant une copie chez eux, mise à jour en permanence (ce que leur ordinateur fait tout seul).

La complexité et la puissance de nos puces, de nos machines, de nos applications, de nos réseaux informatiques donnent naissance à de nouveaux objets numériques. Ces *blockchains* changent les règles du jeu : moins de centralisation, moins d'autorité, plus de partages sont possibles. Une forme d'anarchisme numérique qui existe déjà sur Internet va se développer et changera sans doute les rapports entre humains et entre entreprises. Le monde qui en émergera est difficile à imaginer, mais il se forme et il est imminent. ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'Université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

A. Back *et al.*, **Enabling blockchain innovations with pegged sidechains,** 2014 (http://static1.blockstream.com/sidechains.pdf).

S. Nakamoto, **Bitcoin : A peer-to-peer electronic cash system,** 2008 (https://www.bitcoin.org/bitcoin.pdf).

N. Szabo, **The idea of smart contracts,** 1997 (http://szabo.best.vwh.net/idea.html).

J. Haight, **Beyond bitcoin : Why the block chain is what really matters,** *Computerword*, novembre 2014, (www.computerworld.com/article/2851414/).

E. Rosenfield, **Forget currency, bitcointech is the revolution,** CNBC, novembre 2014 (www.cnbc.com/id/102178309#).

Références supplémentaires sur le site www.pourlascience.fr

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr