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