

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 déblocquera 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 *servants*, 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