Comment rendre l’information infalsifiable ? Avec les blockchains | Le Net Expert Informatique

Comment rendre l’information infalsifiable ? Avec les blockchains

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

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 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…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.pourlascience.fr/ewb_pages/a/article-les-blockchains-clefs-d-apos-un-nouveau-monde-33873.php
Par Jean-Paul Delahaye et Philippe Boulanger