



désengagement et de repli protestataire, il y a aussi la conscience qu'une telle réaction constituerait un autosabotage économique. Ces contraintes ont conduit des technologues du monde entier à imaginer des solutions de remplacement pour établir la confiance à plus grande échelle tout en la rendant plus intime et réciproque. Que la première monnaie numérique prospère, le bitcoin, soit entrée en scène en 2009 n'est pas une coïncidence: cette cryptomonnaie représente une réaction à ce désir croissant de transparence, d'accès et d'autonomisation.

Le bitcoin est une monnaie dont les transactions s'effectuent au moyen d'une blockchain, ou «chaîne de blocs»; il s'agit d'un réseau informatique décentralisé qui consigne dans un registre distribué toutes les transactions préalablement validées par un processus technique de consensus. Les blockchains révolutionnent les possibilités de gestion des échanges directs entre individus, échanges qui peuvent concerner non seulement des sommes d'argent, mais tout bien numérique.

On entend souvent dire que le bitcoin (et les chaînes de blocs en général) ne nécessite pas de confiance. Ce n'est pas tout à fait correct. Plus exactement, la confiance a été retirée aux acteurs humains et transférée à un système cryptographique, avec des incitations

matérielles (gain de bitcoins) à participer au système. En d'autres termes, la confiance est dépersonnalisée.

INSTAURER LA CONFIANCE EN LA DÉSHUMANISANT

De prime abord, cela peut sembler paradoxal. Toutes les formes de confiance ne reposent-elles pas, dans une certaine mesure, sur des humains? Tout au long de l'histoire humaine, la dynamique des migrations et du commerce a conduit à l'élargissement des réseaux de confiance, qui sont passés de petits groupes de personnes connues de tous à des communautés en grande partie constituées d'étrangers et d'adversaires. Pour s'implanter partout sur la planète, nourrir des populations croissantes, mener une guerre, construire des empires ou échanger des savoirs, les gens ont utilisé des techniques de la confiance qui se sont développées les unes à partir des autres, avec un certain recouvrement chronologique: la parenté et le don de cadeaux, la division du travail, la comptabilité (à l'origine du crédit et de la dette), la hiérarchie, la monnaie, les religions universelles et, plus récemment, la banque.

En ce début de ^{xxi}e siècle, la confiance connaît une nouvelle étape de son évolution. Ces mêmes banques qui ont soutenu l'essor du >

➤ capitalisme moderne en jouant le rôle d'intermédiaires de confiance fiables sont, à bien des égards, devenues un obstacle à son développement. Dans notre système financier actuel, les politiques conduites et les lois visent à décourager les pratiques d'exploitation des individus au moyen de sanctions. À l'avenir, les blockchains pourraient tout simplement être conçues de façon à rendre impossibles ces pratiques.

LES BLOCKCHAINS, UN OUTIL D'ÉMANCIPATION... OU D'ASSERVISSEMENT !

Les règles de consensus du bitcoin, qui fixent les incitations et les exigences encadrant la participation à la blockchain, maintiennent très bien un système de gouvernance distribué, ouvert et pair à pair (voir l'article de John Pavlus, page 28). Ses transactions sont publiques, bien que pseudonymes; le code source du logiciel utilisé est ouvert et maintenu par un réseau global de développeurs bénévoles. De plus, la blockchain du bitcoin ne stocke pas les données d'identification; en guise d'adresses, elle utilise des paires de clés publiques-privées, plutôt que des comptes.

Mais les transactions fondées sur une blockchain sont plus facilement traçables que les transactions en espèces; cela signifie qu'une fois qu'une paire de clés est reliée à une identité connue, l'analyse de la blockchain peut, par exemple, aider la police à retrouver des criminels. Cette réalité va à l'encontre de l'idée répandue selon laquelle les cryptomonnaies conviendraient mieux aux activités criminelles que d'autres types de monnaie.

En fait, les cryptomonnaies réintroduisent le spectre du capitalisme de surveillance. Car les blockchains ont des propriétés qui se prêtent à la fois à l'émancipation humaine et à un degré sans précédent de surveillance et de contrôle. Seront-elles, au bout du compte, au service de notre liberté ou de notre soumission? Tout dépendra de la façon dont le système logiciel, à savoir le protocole de la blockchain et l'application qui lui est adossée, gère les identités numériques de ses utilisateurs.

En ce qui concerne le protocole lui-même, il est important de comprendre qu'il existe plusieurs façons de concevoir une blockchain. Généralement, le terme «blockchain» se réfère à un type de système où un registre de transactions universellement reconnu est répliqué (c'est-à-dire dupliqué et maintenu cohérent sur plusieurs serveurs), mais il n'y a pas d'unanimité sur un ensemble de caractéristiques qu'un tel système doit présenter. D'innombrables modèles de blockchains ont été introduits à ce jour, et ils sont conçus afin d'apporter des solutions à des problèmes différents.

Considérons par exemple Ethereum, une blockchain publique qui se présente comme un

ordinateur distribué global, nommé Ethereum Virtual Machine. Cette blockchain stocke des contrats intelligents qui sont exécutés quand les conditions qu'ils spécifient sont remplies. Son créateur, le Russo-Canadien Vitalik Buterin, envisage que, contrairement au système du bitcoin, les utilisateurs les plus investis dans le réseau (déterminés par des dépôts de garantie en cryptomonnaie) valideront collectivement les nouveaux blocs. Les utilisateurs qui ne respectent pas les règles se verront automatiquement confisquer leur cryptomonnaie.

Certaines blockchains sont conçues pour des communautés où règne entre les membres une grande confiance. Ces blockchains restreintes (*permissioned blockchains* en anglais) reposent généralement sur une autorité centrale qui accorde à des utilisateurs particuliers le rôle de lire ou déposer des transactions. Pour s'assurer que tous les membres de la blockchain se comportent bien, les blockchains restreintes tendent à se reposer sur une autorité centrale plutôt que sur des incitations matérielles automatiques comme dans le système du bitcoin.



Les cryptomonnaies réintroduisent le spectre du capitalisme de surveillance



Un exemple en vue est Ripple, une blockchain conçue pour servir de réseau de règlement lors des transactions interbancaires. De la même façon, l'organisation à but non lucratif EEA (Enterprise Ethereum Alliance) regroupe quelque 200 associés qui construisent une boîte à outils à code source ouvert censé permettre aux entreprises de concevoir leurs propres versions privées de la blockchain Ethereum.

D'autres initiatives similaires sont considérées comme de simples registres distribués, car il leur manque une ou plusieurs des propriétés sous-jacentes des blockchains. Ce sont généralement des registres à accès restreint, où beaucoup de transactions restent privées. L'un des plus importants outils de développement de blockchains privées est R3 Corda, élaboré par un consortium de banques afin de faciliter le consensus concernant les accords financiers.