

> 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.

Les blockchains privées et les registres distribués ont vu le jour en partie pour inclure une forme de contrôle de l'identité des validateurs et de ceux qui effectuent des transactions (par conception, le protocole de la blockchain du bitcoin ne contient pas lui-même de mécanisme de vérification d'identité). L'identité est le terrain sur lequel se jouera le caractère émancipatoire ou oppressif, sur le plan social, des chaînes de blocs. Car plus il est facile de relier les transactions de quelqu'un à une identité (et plus l'identité numérique d'un individu devient centralisée et contrôlée de l'extérieur), plus les possibilités d'abus se multiplient.

DES APPLICATIONS À LA FOIS CONVIVIALES ET DÉPOURVUES DE CONTRÔLE CENTRALISÉ ?

L'individu lambda ne peut pas utiliser directement une blockchain, de la même façon qu'Internet ne peut pas être utilisé directement. En réalité, l'individu utilise des applications qui se servent de la blockchain sous-jacente d'une manière ou d'une autre. C'est dans cette couche d'applications que peuvent régner une grande confusion et, souvent, la mauvaise foi.

L'histoire du système bitcoin, par exemple, est jonchée d'échanges de cryptomonnaie et de fournisseurs de portefeuilles qui ont laissé des failles de sécurité béantes dans leurs applications, ce qui a donné lieu à des piratages retentissants et à des accusations de détournement de fonds.

Dans le cas du réseau Ethereum, des vulnérabilités ont permis le vol ou la perte de millions de dollars de sa cryptomonnaie, l'ether, les utilisateurs lésés n'ayant disposé de pratiquement aucun recours. En général, l'utilisation de n'importe quelle application développée par un tiers auquel on fait confiance pour conserver des biens numériques fondés sur une chaîne de blocs reste une démarche hautement risquée.

C'est là tout le problème insoluble des blockchains: le public ne les utilisera pas s'il ne dispose pas d'applications conviviales. Mais pour être conviviales, les applications recourent souvent à la centralisation, qui reproduit les conditions d'un contrôle centralisé que les blockchains visaient précisément à éviter.

Si l'on veut que les chaînes de blocs deviennent utiles à grande échelle, un certain lien entre l'identité et les transactions sera toutefois nécessaire. Peut-être cette identité n'exigera-t-elle pas de révéler complètement qui vous êtes. Comme l'ont affirmé certains membres de la communauté du bitcoin, la focalisation actuelle sur la vérification de l'identité est en grande partie injustifiée; en général, ce que les gens veulent savoir, c'est si une affirmation particulière à votre propos est vraie:

avez-vous plus de 21 ans? Avez-vous réellement obtenu un doctorat au MIT? Êtes-vous citoyen américain? Nous avons été habitués par les structures incitatives du capitalisme de surveillance à croire qu'il est nécessaire de livrer une multitude de données personnelles pour suivre notre chemin dans la vie de tous les jours. Changer ce présupposé est l'un des effets les plus radicaux que les techniques de chaînes de blocs pourraient avoir.

Imaginez, par exemple, l'avenir du vote électronique. Une commission électorale doit pouvoir relier une opération de vote à un électeur inscrit afin que cette personne soit notée «a voté». Mais ce processus n'a pas nécessairement besoin de révéler l'identité de l'individu à la commission: celle-ci pourrait simplement vérifier que le votant est inscrit pour participer à cette élection, et enregistrer qu'il ou elle a voté une fois son choix fait, le tout sans corréler le vote et l'électeur.

Les projets qui minimisent la dissémination de ce qu'on appelle les données à caractère personnel sont encore rares, en partie parce qu'ils ne sont pas faciles à monétiser, que ce soit en devise ou en contrepartie de données personnelles.

Un exemple de projet allant dans ce sens est Blockcerts, une série de bibliothèques de référence gratuites développée par le MIT Media Lab et l'entreprise Learning Machine, où je travaille. Blockcerts permet aux individus de conserver leurs avoirs numériques dans un portefeuille privé hébergé sur leur propre matériel électronique. Les documents communiqués à une personne ne sont associés à aucune identité, à moins que le récipiendaire n'en fasse le choix. Le code source du logiciel est ouvert: on peut donc l'inspecter pour en vérifier l'intégrité et n'importe qui peut l'utiliser en vue de créer ses propres applications pour envoyer, stocker, partager et vérifier des documents officiels. Cette approche est un pas vers ce que certains, dans le domaine de l'identité numérique, ont appelé identité autosouveraine, ce qui signifie que les individus ont le contrôle sur leurs propres données.

Les blockchains sont véritablement une technologie de rupture, qui remet en cause les manières d'envisager la confiance. Mais si les applications s'appuyant sur ces outils ne sont pas conçues dans un souci d'autosouveraineté numérique, rien en principe n'empêchera de traiter les humains comme autant d'objets dans une chaîne logistique, dont chaque mouvement et activité est enregistré, peut-être de façon permanente. Créer des identités numériques dont l'existence soit indépendante des États et des grandes entreprises est le prochain grand défi que nous posent les blockchains – un défi que cette technologie pourrait aussi nous aider à résoudre. ■

BIBLIOGRAPHIE

Les nouveaux équilibres de la confiance, entre algorithmes et contrat social, *Cahier de veille de la fondation Mines-Télécom n° 9*, juin 2017 (téléchargeable sur www.imt.fr/cahier-de-veille-confiance-numerique/).

M. Casey et P. Vigna, **The Age of Cryptocurrency : How Bitcoin and Digital Money Are Challenging the Global Economic Order**, St. Martin's Press, 2015.

S. Zuboff, **Big Other : Surveillance capitalism and the prospects of an information civilization**, *Journal of Information Technology*, vol. 30(1), pp. 75-89, 2015.

D. Graeber, **Debt : The First 5,000 Years**, Melville House, 2014.