> vertige… Ils montrent simplement qu'il n'est guère envisageable que les bitcoins en circulation ou plus généralement les monnaies cryptographiques fonctionnant sur son modèle se substituent un jour aux monnaies internationales d'échange que sont le dollar et l'euro.

Notons aussi que nous avons seulement envisagé une augmentation du cours du bitcoin pour que leur total égale en valeur les billets en dollars, ce que les économistes nomment la « base monétaire » et notent M0. Si nous avions pris en compte la valeur de la masse monétaire M1, qui inclut en plus l'argent présent sur les comptes à vue des particuliers et des entreprises (M1 vaut environ le triple de M0), nous serions arrivés à une dépense électrique trois fois plus importante. Les chiffres seraient alors compris entre 1000 et 1500 TWh par an pour les pessimistes, et entre 500 et 750 TWh pour les optimistes. Dans le meilleur des cas, on atteindrait des chiffres comparables au huitième de la consommation électrique des États-Unis (4128 TWh en 2015) et, dans le pire des cas, au tiers.

LE SYSTÈME D'INCITATION EST EN CAUSE

Peut-on changer le mode de fonctionnement des monnaies cryptographiques pour éviter cette folle dépense électrique?

La consommation d'électricité liée au bitcoin n'est pas due aux coûts de la surveillance des transactions et à la gestion de son registre de comptes (la blockchain). Elle est due au mode de distribution des bitcoins émis toutes les 10 minutes, plus précisément au concours entre les nœuds du réseau qui désigne toutes les 10 minutes le gagnant des bitcoins émis et des commissions associées aux transactions. D'autres mécanismes fondés sur l'idée des blockchains n'utilisent pas ce système d'incitation et encore moins de concours entre les nœuds des réseaux associés, car ils n'en ont pas besoin.

Ainsi, les « blockchains privées », qui servent par exemple à gérer des échanges entre un consortium de banques en nombre fixé, ne sont pas du tout sujettes aux énormes dépenses électriques du bitcoin: elles n'ont pas besoin de systèmes d'incitation, puisque chaque acteur du réseau est intéressé par avance au bon fonctionnement du réseau. Seule la volonté de faire reposer le fonctionnement du bitcoin sur un réseau pair à pair, anonyme, décentralisé, ouvert et extensible oblige à mettre en place un système d'incitation assurant l'existence des volontaires s'occupant de gérer et surveiller le réseau, ainsi qu'un concours entre nœuds pour attribuer l'incitation. La véritable question est celle du concours pour l'attribution de la prime d'incitation.

Peut-on concevoir un autre type de concours qui n'entraînerait pas l'aberration électrique du bitcoin? La question n'est pas nouvelle et de nombreuses idées ont été proposées pour opérer autrement la distribution de l'incitation. Hélas, aucun système de remplacement n'a encore réussi à convaincre pleinement.

L'explication pourrait être liée à la notion de contenu en calcul, que nous avons traitée plusieurs fois dans cette rubrique (*voir « Qu'est-ce qu'un objet complexe? »*, Pour la Science, *mai 2013*). En effectuant leurs calculs pour remporter le concours toutes les 10 minutes, les nœuds du réseau consomment de l'électricité; le calcul produit la solution à un problème (peu intéressant, mais difficile) qui est mis dans le registre des comptes du bitcoin. Ce dépôt a pour conséquence que le registre est difficile à falsifier. Pour le falsifier et créer un registre pouvant se substituer au registre courant (et permettant de détourner des bitcoins d'un compte vers un autre), il faudrait calculer autant que ce qui a été calculé par tout le réseau, et donc dépenser autant d'énergie électrique que ce qui a été consommé par le réseau en entier, au moins sur la période qu'on souhaite falsifier. C'est donc impossible ou extrêmement coûteux. La robustesse du bitcoin semble essentiellement liée à cette impossibilité presque absolue de fabriquer un faux registre, impossibilité qui disparaît probablement quand on change la méthode de distribution par concours de calcul.

À EN VOULOIR TROP, ON RISQUE DE TOUT PERDRE

C'est la volonté d'avoir un système protégé par le placement d'une quantité colossale de calculs (et donc d'électricité) dans le registre des comptes pour le rendre infalsifiable qui est à l'origine du problème. Malheureusement, cette solidité presque parfaite a un prix: l'impossibilité que le cours du bitcoin augmente au point de devenir un jour un véritable concurrent du dollar ou de l'euro.

Entre les systèmes à blockchains privées, simples et électriquement viables, et les systèmes à blockchains publiques, totalement décentralisés, ouverts, anonymes et disposant d'une configuration extensible des nœuds – des systèmes qui, eux, semblent absurdes et finalement condamnés par avance –, il faut choisir ou inventer des systèmes intermédiaires. Pour donner naissance à une nouvelle monnaie internationale, il sera nécessaire de renoncer à certaines propriétés de la monnaie mise en route par le génial Satoshi Nakamoto. ■

BIBLIOGRAPHIE

J. Favier et A. Takkal Bataille, **Bitcoin, la monnaie acéphale**, CNRS Éditions, 2017.

M. Bevand, **Electricity consumption of bitcoin : A market-based and technical analysis**, http://blog.zorinaq.com/bitcoin-electricity-consumption/, 10 mars 2017.

Bitcoin energy consumption index, *Digiconomist*, consulté le 1/1/2018 (https://digiconomist.net/bitcoin-energy-consumption).

J.-P. Delahaye, **Mathématiques et mystères**, Belin/Pour la Science, 2016 (trois chapitres consacrés au bitcoin, aux preuves de travail et aux blockchains).