

rémunération des mineurs. Ces commissions évoluent de façon complexe, mais en gros elles augmentent en même temps que la valeur du bitcoin. Elles ont d'ailleurs été introduites par Satoshi Nakamoto pour compenser la division par deux tous les quatre ans et faire qu'il y ait toujours des gens intéressés pour surveiller et faire fonctionner le réseau. On peut faire l'hypothèse que, en première approximation, ce qu'a prévu le créateur du bitcoin se produira; cela signifie que dans les prévisions des futures dépenses électriques, on peut ne pas prendre en compte la division par deux tous les quatre ans, qui est compensée par le système des commissions.

Qu'advierait-il si la valeur des bitcoins égalait celle des dollars ou des euros?

Au 1^{er} janvier 2018, la valeur de tous les bitcoins en circulation était d'environ 230 milliards de dollars. La valeur de tous les billets en dollars en circulation est, d'après la FED (la Réserve fédérale des États-Unis), de 1500 milliards de dollars (chiffres de décembre 2016). Pour l'euro, on a des chiffres du même ordre de grandeur. Il y a donc 6 fois plus de dollars sous forme de billets en circulation que de dollars sous forme de bitcoins. Si le volume des bitcoins en circulation devenait, en valeur, équivalent aux dollars circulant sous forme de billets, cela signifierait que le cours du bitcoin a été multiplié par 6. En effet, les bitcoins émis représentent 80% des 21 millions de bitcoins prévus par Satoshi Nakamoto.

L'HORIZON DU BITCOIN BOUCHÉ PAR LE MUR DE LA DÉPENSE EN ÉLECTRICITÉ

Seule l'augmentation de la valeur unitaire du bitcoin peut amener à ce que leur total s'approche, en valeur, du total des billets de dollars en circulation. Cette multiplication par 6 de la valeur des bitcoins (ou par 5 si l'on veut prendre en compte les 20% de bitcoins non émis) ne semble pas impossible au vu de ce qui s'est passé depuis deux ans.

Une telle multiplication par 5 conduirait la dépense électrique du réseau bitcoin à une valeur comprise entre 350 et 500 TWh par an pour les pessimistes, et entre 175 et 250 TWh par an pour les optimistes. Ce serait alors, en ordre de grandeur, comparable à la consommation électrique française annuelle.

Rien ne pourra arrêter cette croissance sans une volonté déterminée, soit de la communauté qui en a collectivement le pouvoir mais dont ce n'est pas l'intérêt, soit des États en imposant un contrôle ou en interdisant ce type de mécanisme numérique et économique diabolique.

Les chiffres cités correspondent à des évaluations assez imprécises, mais les ordres de grandeur sont corrects et bien sûr donnent le

3

L'OR ET LE BITCOIN

On a souvent comparé le bitcoin et l'or. Certes, un point commun est que la quantité d'or disponible sur Terre, comme la quantité de bitcoins, ne résulte pas de la volonté d'un État ou d'une banque émettrice, mais est fixée par des contraintes impossibles à manipuler : les réserves terrestres dans le cas de l'or, et le protocole de Satoshi Nakamoto défini en 2008 qui fait qu'il n'y aura jamais plus de 21 millions de bitcoins.

Mais, en valeur, il y a beaucoup plus d'or que de bitcoins. On estime la valeur de tout l'or terrestre à 8 000 milliards de dollars, alors qu'il n'y a actuellement que quelque 230 milliards de dollars en bitcoins (au 1/1/2018). Le bitcoin ne peut donc pas aujourd'hui se substituer à l'or, contrairement à ce que certains prétendent.

Chaque année, on extrait environ 2 500 tonnes d'or. À raison de 41 000 dollars le kilogramme, cela fait environ 100 milliards de dollars. C'est, en ordre de grandeur, la valeur de la moitié des bitcoins existants et 10 fois plus que la valeur des bitcoins émis chaque année. Là encore, on voit que l'or domine par rapport au bitcoin.

Les défenseurs des monnaies cryptographiques

font remarquer qu'on dépense donc beaucoup plus par an en moyens pour extraire de l'or (sans doute à peu près sa valeur, soit environ 100 milliards de dollars) que pour extraire des bitcoins (ce sera environ 10 milliards de dollars quand le coût de production se sera ajusté au cours du bitcoin le 1/1/2018). La dépense pour extraire de l'or a aussi, comme pour les bitcoins, un important coût écologique, aujourd'hui bien supérieur à celui de l'extraction des bitcoins. Ce dernier ne devrait donc pas nous effrayer, selon les partisans du bitcoin.

La réponse de ceux qui considèrent le bitcoin dangereux est que l'or est utile (par exemple en électronique) alors que les bitcoins produits ne servent à rien d'autre qu'à opérer des échanges. De plus, pour que les bitcoins émis puissent vraiment rivaliser avec une monnaie internationale, il faudrait que le cours du bitcoin soit multiplié par 15 pour atteindre la valeur des dollars en billets et sur les comptes à vue, ce qui conduirait alors à une dépense du réseau bitcoin supérieure au coût annuel de l'extraction de l'or : extraire les bitcoins sera alors plus cher qu'extraire l'or !



> 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 M_0 . Si nous avions pris en compte la valeur de la masse monétaire M_1 , qui inclut en plus l'argent présent sur les comptes à vue des particuliers et des entreprises (M_1 vaut environ le triple de M_0), nous serions arrivés à une dépense électrique trois fois plus importante. Les chiffres seraient alors compris entre 1 000 et 1 500 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. Takal 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).