EN PARTENARIAT AVEC

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

CRYPTOMONNAIES, UN AUTRE DÉFI POUR LA TRANSITION ÉNERGÉTIQUE

Après des débuts timides, les cryptoactifs, bitcoins en tête, sont de plus en plus prisés. Or, la consommation d'électricité et de terres rares de cette industrie pose un problème planétaire, trop peu pris en compte. Explications d'**Olivier Pironneau,** qui esquisse des solutions.

Dans le cadre de notre partenariat avec l'Académie des sciences, des académiciennes et académiciens analysent et apportent leur éclairage sur les grands enjeux du monde contemporain au travers de questions scientifiques qui font l'actualité.

Il n'y a guère plus que dans les films que l'on paye avec une valise pleine de billets. La plupart des transactions financières sont électroniques, placées principalement sous le contrôle d'organismes financiers – banques, Visa, PayPal… –, qui prélèvent des frais de transactions et qui peuvent également exercer des moyens de pression, à l'instar du gouvernement américain sur les transactions en dollars.
En 2008, en pleine crise financière, Satoshi Nakamoto, pseudonyme d'un inconnu ou d'un groupe dont l'anonymat est resté préservé, a proposé la première monnaie numérique réellement utilisable, décentralisée et cryptée : le bitcoin. Depuis, il est possible d'en acheter et d'en vendre librement et en toute confiance, les fortes fluctuations du marché mises à part. Le moyen le plus simple pour cela est de s'adresser à une plateforme d'échange telle que Binance, d'y ouvrir un compte et d'y acheter des bitcoins. L'acheteur reçoit un code cryptographique qu'il doit garder à l'abri des regards indiscrets et qu'il utilisera pour les revendre.

SI ELLE N'EMPLOIE QUE 200 000 PERSONNES ENVIRON DANS LE MONDE, L'INDUSTRIE DU BITCOIN DÉPENSE L'ÉQUIVALENT D'UN QUART DE LA CONSOMMATION ÉLECTRIQUE FRANÇAISE.

Le succès du bitcoin repose sur sa sécurité, car jusqu'à présent il n'y a pas eu d'attaque réussie sur le système, et peut-être aussi sur sa volatilité, car on peut espérer réaliser d'importants bénéfices en quelques mois. Jusque-là, tout va bien, même si l'anonymat des transactions permet le blanchiment d'argent, l'évasion de capitaux, etc. Notons que le logiciel de bitcoin, le bitcoin core, est libre et que, dans ce cadre, ses développeurs ne sont pas tout-puissants (les responsables choisissent entre eux un chef, révocable en cas de désaccord), de sorte que l'on peut dire que personne ne contrôle le bitcoin.

LA TECHNOLOGIE « BLOCKCHAIN »

Ces bases étant posées, venons-en plus précisément à notre sujet. Vous avez peut-être déjà lu que le bitcoin consomme autant d'électricité que l'Argentine (1). Comment se fait-il qu'une situation aussi choquante perdure dans le contexte de la lutte contre le changement climatique ? Pour comprendre l'origine de cette énorme consommation d'énergie, il faut étudier le mécanisme qui garantit la sécurité du bitcoin. L'achat de celui-ci sera enregistré dans la base de toutes les transactions qui est organisée en « chaîne de blocs » – ou « blockchain », comme on le lit et l'entend couramment. Il faut donc intégrer cet achat dans un bloc de transactions et valider ce nouveau bloc en vue de son ajout à la base de données bitcoin. Évidemment, il est impératif d'empêcher que quelqu'un insère un bloc non validé qui lui permettrait de s'approprier des bitcoins sans les payer.

Une fois la validation du bloc effectuée, l'achat décrit plus haut est pratiquement ineffaçable, car la chaîne de blocs bitcoin réside sur Internet en de multiples exemplaires en pair à pair (ou « peer-to-peer », ou P2P). Cette technologie anonyme et décentralisée permet l'échange direct de données entre ordinateurs reliés à Internet, sans passer par un serveur central. Elle a été popularisée par un étudiant américain qui a créé en 1999 le service de partage en ligne Napster pour poster des morceaux de musique sur le réseau et permettre leur téléchargement (généralement illégal) sans laisser de trace.
La validation du bloc est effectuée par un « mineur » avec un algorithme dit de « preuve de travail ». A priori, le mineur peut être monsieur Tout-le-monde disposant d'un PC puissant doté d'un logiciel approprié. Ce logiciel lui demande d'accomplir une tâche coûteuse en temps de calcul : calculer l'« empreinte digitale » du bloc, son « hash code » ou code de hachage (2). Dès qu'il réussit, le mineur publie son résultat et, s'il est le premier à l'avoir fait, il gagne et reçoit des bitcoins en récompense. Sinon, il aura travaillé en vain.
Il y a donc deux causes de forte consommation électrique : la difficulté du problème à résoudre, qui conduit à effectuer des calculs importants, et le fait que plusieurs mineurs s'y attellent en même temps, multipliant par là même les coûts de calcul. En 2010, un de mes neveux s'est fait une petite fortune avec son seul PC, mais aujourd'hui il ne le pourrait plus, car il faut des moyens informatiques gigantesques pour gagner la course de vitesse qui valide le travail. Le minage consomme une part substantielle de l'énergie utilisée par l'ensemble des data centers du monde. Néanmoins, il reste très rentable, surtout s'il est réalisé dans un pays où l'électricité n'est pas trop chère.

PROFIL
Professeur émérite à Sorbonne Université en mathématiques appliquées, Olivier Pironneau est membre de l'Académie des sciences et de la fondation Natixis pour la finance quantitative. Ses travaux se situent à l'interface entre les mathématiques, l'informatique, la mécanique des fluides et la finance numérique.

ON ESTIME QUE LA FABRICATION D'UN SEUL BITCOIN REQUIERT AUTANT DE TERRES RARES QUE CELLE DE DEUX IPHONES 12.

DES ALGORITHMES MOINS ÉCOCIDAIRES

La Chine a décidé d'interdire le minage. Malgré cela, il semble qu'il y reste encore 20 % de mineurs illégaux (3). Les autres ont principalement émigré au Kazakhstan, où l'électricité est produite par des énergies fossiles – ce qui est le cas presque partout, sauf en Islande. Le Texas offre un exemple peut-être encore plus alarmant. L'électricité y est produite à partir de pétrole et de gaz de schiste, elle n'est pas surabondante, mais les gros consommateurs ont la possibilité de conclure des accords distincts avec les fournisseurs d'électricité, leur garantissant ainsi une demande constante. En cas de plainte, on répond que le bitcoin n'utilise que de l'électricité excédentaire, à des heures creuses, etc. : une allégation facile à réfuter.
L'industrie des cryptomonnaies emploie un petit nombre de personnes – probablement près de 200 000 –, mais sa consommation électrique est phénoménale (voir la figure p. 48) comme nous l'avons dit – l'équivalent d'un quart de la consommation électrique française. Le Français soucieux de sa trace carbone hésite à prendre l'avion alors que les 10 % qui possèdent du bitcoin – un chiffre en progression, ils étaient 8 % en 2021 et 3 % en 2020 (4) – sont, même indirectement, de gros pollueurs, car la transaction bitcoin qu'ils vont réaliser va aller dans un bloc qui sera miné ! Les partisans du système arguent que la consommation des »»

sèche-linge aux États-Unis est similaire ; certes, mais plus de 130 millions de ménages en profitent. Le minage pose un autre problème écologique : l'usage excessif de terres rares, composant crucial dans la fabrication des matériels utilisés. Les ordinateurs devenant vite dépassés, il faut les renouveler ; en outre, le recyclage des cartes dédiées au minage, dites Asic (Application Specific Integrated Circuit ; en français, circuit intégré propre à une application), est mal organisé. On estime que la fabrication d'un bitcoin requiert autant de terres rares que celle de deux IPhone 12 ; comme 20 millions de bitcoins ont été minés depuis leur apparition, je vous laisse faire le calcul…

Le bitcoin pose donc un problème planétaire incompatible avec la transition énergétique. Quelles sont les solutions ? On pourrait interdire toutes les cryptomonnaies, mais il y a de nombreuses raisons pour ne pas le faire. D'abord parce qu'il existe des algorithmes moins écocidaires, comme la « preuve d'enjeu » dont nous allons parler, pour assurer la sécurité d'une cryptomonnaie. Ensuite, parce que les banques centrales de nombreux États et celle de l'UE envisagent de se doter de cryptomonnaies pour lutter contre les fraudes aux cartes bancaires et les faux virements, et pour faire diminuer les coûts des transactions par leur procédé même. Par ailleurs, les progrès de l'informatique apporteront d'autres solutions ; la France est très bien placée pour la recherche en cryptologie et les applications des chaînes de blocs.

L'ETHEREUM

La deuxième solution consiste à ne rien faire et attendre que le bitcoin meure étouffé par sa croissance exponentielle (voir la figure ci-dessus). En effet, plus le minage est rentable, plus les mineurs sont nombreux à se faire concurrence, jusqu'au jour où il ne sera plus rentable ; par ailleurs, la difficulté du minage augmente, exigeant un hash code de plus en plus complexe, et la rétribution va diminuer au fur et à mesure que l'on s'approche de la limite fatidique des 21 millions de bitcoins disponibles. Ce processus va certainement entraîner une concentration des acteurs ; l'anonymat sera plus difficile et peut-être pourra-t-on alors taxer le minage.

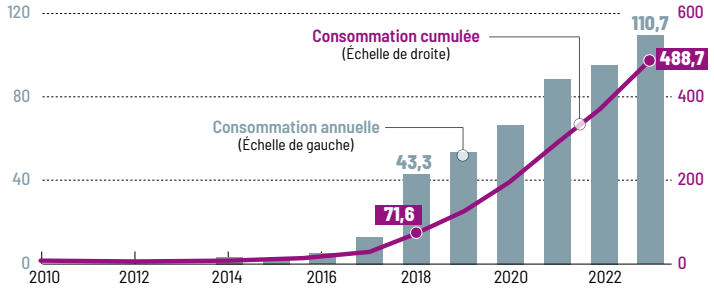
La troisième solution est la plus raisonnable, mais elle est difficile à mettre en œuvre : décourager l'usage de l'algorithme de « preuve de travail » et le remplacer par exemple par la « preuve d'enjeu ». Avec celle-ci, les participants qui sont prêts à risquer une somme importante essayent de se mettre d'accord entre eux et désignent celui qui va valider le bloc – contrairement à la preuve de travail, beaucoup plus énergivore, les mineurs concourant individuellement et la « prime » revenant uniquement au premier qui gagne la course de vitesse engagée. Ethereum est la deuxième cryptomonnaie en termes de taille après le bitcoin. Conscient du problème énergétique, le consortium qui la produit est passé (partiellement) en septembre 2022 à la preuve d'enjeu. Si l'Ethereum n'est pas « hacké », alors on aura validé cette approche qui divise la consommation électrique par 10 000, au moins. Malheureusement, les acteurs du bitcoin semblent assez réfractaires à ce changement.

La dernière solution, certes un peu utopique, est d'interdire les cryptomonnaies qui sont basées sur la preuve de travail. Pour qu'elle puisse être réellement appliquée, cette décision doit être prise à la fois au niveau des États et des organisations internationales, telles que le Giec et l'ONU. Cela nécessitera une prise de conscience et un courage politique qui ne semblent pas encore au rendez-vous. Puisse la diffusion de l'état des connaissances sur ce problème y contribuer. ●

LA SOLUTION LA PLUS RAISONNABLE : DÉCOURAGER L'USAGE DE L'ALGORITHME DE « PREUVE DE TRAVAIL » ET LE REMPLACER PAR LA « PREUVE D'ENJEU ».

CONSOMMATION D'ÉLECTRICITÉ DE L'INDUSTRIE DU BITCOIN

En térawattheure (1 000 milliards de wattheures)



L'indice de consommation d'électricité de Cambridge Bitcoin (Université de Cambridge) fournit notamment une estimation annualisée : ici, de 2010 à 2023.

SOURCE : THE CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE

INFOGRAPHIE L'HUMANITÉ

EN SAVOIR PLUS

Le site de l'Académie des sciences : www.academie-sciences.fr

« Au-delà du bitcoin. Dans l'univers de la blockchain et des cryptomonnaies » de Jean-Paul Delahaye, Dunod, 2022.

« Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies », rapport n° 584 du Sénat, 20 juin 2018 ; texte intégral, résumé et synthèse sur senat.fr

« Blockchain : consolider nos atouts », rapport de l'Institut Montaigne, juin 2023, sur institutmontaigne.org

(1) Voir la partie « Comparisons » (comparaisons) sur le site du Cambridge Centre for Alternative Finance : ccaf.io/cbnsi/cbeci

(2) Code qui résulte de la transformation, au moyen d'une fonction de hachage cryptographique, d'un ensemble de données en une séquence alphanumérique de taille réduite, et qui permet d'identifier les données de départ sans y accéder.

(3) Voir la carte « Bitcoin Mining Map » sur le site ccaf.io/cbnsi/cbeci

(4) Selon la seconde édition de l'enquête réalisée par KPMG pour l'Association pour le développement des actifs numériques (Adan), avril 2023 ; voir adan.eu