

La consommation énergétique est le talon d'Achille de Bitcoin

Description

La validation des transactions monétaires en bitcoins sur la blockchain anonyme rend impossible leur falsification. Mais elle repose sur une dépense énergétique de plus en plus décriée. Si la Chine était jusqu'au présent le pays concentrant la majorité des mineurs, le gouvernement a sonné le glas de cette activité, incitant ces derniers à relocaliser leurs activités ailleurs, notamment au Canada, en Russie, en Europe de l'Est ou encore en Islande.

L'opération de minage consiste à effectuer un calcul cryptographique appelé « validation par la preuve de travail » (*proof of work*, voir [La rem n°44, p.97](#)). Cette opération, fortement consommatrice en énergie, est cependant l'un des rouages permettant au protocole de sécuriser les transactions sur le réseau et de générer de nouveaux bitcoins. Les ordinateurs participant au minage sont en compétition pour valider, toutes les dix minutes, les nouveaux blocs de transactions, mais seul le premier qui retrouve le *hash* cryptographique est récompensé, actuellement 12,5 bitcoins. Andreas M. Antonopoulos, une figure emblématique de la communauté bitcoin, explique ainsi que « pour décrypter le minage, on pourrait utiliser l'exemple d'un gigantesque concours de sudoku où les participants recommencent une nouvelle grille dès que quelqu'un trouve une solution, et dont la difficulté s'ajuste pour qu'en moyenne une grille soit résolue toutes les dix minutes ». Alors qu'il était au début possible de miner des bitcoins avec un ordinateur personnel, le développement de la monnaie numérique depuis 2009 nécessite dorénavant une puissance de calcul bien supérieure. Le minage individuel a laissé place aux fermes de minage.

Il s'agit de grands hangars remplis d'ordinateurs qui calculent des fonctions de hachage cryptographiques et minent des monnaies numériques comme le bitcoin, mais aussi l'Ethereum ou encore le Litecoin. En août 2017, le site d'information Quartz a eu accès à une ferme de minage située à Ordos, perdue au milieu des steppes de Mongolie intérieure, dans une friche industrielle à 700 km à l'ouest de Pékin. Exploitée par Beijing Bitmain Technologies, une société chinoise leader dans le minage du bitcoin, elle employait une cinquantaine de personnes dont la tâche était d'assurer la surveillance de quelque 25 000 serveurs tournant jour et nuit pendant toute l'année. 21 000 de ces machines, entièrement dédiées au minage de bitcoins, représentaient à l'époque 4 % de la puissance de calcul du réseau mondial. La région, riche en charbon, offrait une électricité à bas coût dont le tarif était inférieur de 30 % supplémentaire par le gouvernement local pour attirer des entreprises dans ce parc industriel en ruine. Elle seule, cette ferme de minage dépensait 39 000 dollars d'électricité par jour.

Or, plus le nombre et la valeur du *bitcoin* augmentent, plus les calculs à effectuer sont complexes, nécessitant toujours plus d'énergie électrique pour y parvenir. Comme le note Jean-Paul Delahaye, mathématicien français, « la compétition entre mineurs crée un système où la dépense électrique est essentiellement proportionnelle au cours du *bitcoin* (qui a été multiplié par 14 dans l'année 2017). Si, comme cela vient de se produire, le cours du *bitcoin* devient trois fois plus élevé, alors les mineurs dépensent une quantité d'électricité d'importance raisonnable ». L'ensemble de ces installations informatiques sont extrêmement énergivores et représentent, selon le site spécialisé Digiconomist (Digiconomist.net) 23 TWh par an, soit l'équivalent de la consommation annuelle de plus de 2 millions de foyers américains, ou encore, 0,1 % de la production électrique mondiale. Même si un important débat concernant le calcul de ces estimations anime les crypto-enthousiastes face aux crypto-sceptiques, il apparaît que la consommation énergétique du *bitcoin* semble effectivement « raisonnable ».

La Chine, où le coût de l'électricité est particulièrement faible, avait incité, dès 2013, de nombreux investisseurs nationaux à installer des fermes de minage de cryptomonnaies. À tel point qu'en juillet 2017, une étude de l'université de Cambridge estimait qu'il s'y minait 58 % des *bitcoins* dans le monde. Mais, à partir de novembre 2017, le pays a mis un coup de frein au développement des fermes de minage. Après avoir interdit dès septembre, les plateformes d'échanges et les ICO (voir [La rem n°44, p.97](#)), la Chine incite, début 2018, les gouvernements des provinces à limiter la consommation d'énergie utilisée pour miner ces cryptomonnaies.

Les mineurs tentent de relocaliser leurs installations dans d'autres pays, notamment au Canada, en Islande, en Russie ou en Europe de l'Est. Avec ses 62 centrales hydroélectriques, Hydro-Québec, principal producteur d'électricité au Canada et l'un des plus grands producteurs mondiaux d'hydroélectricité, est ainsi sollicité par un nombre grandissant de fermes de minage. Mais, avec 70 dossiers en instance, un porte-parole de l'entreprise a déclaré que « *Hydro-Québec n'aura pas la capacité à long terme de répondre à cette demande* ». Interrogé par *Le Monde*, Johann Snorri Sigurbergsson, chargé de développement chez HS Orka, producteur et distributeur d'électricité en Islande, indique que les activités de minage « vont être multipliées par quatre ou par six dans les six prochains mois », en citant parmi ses nouveaux clients « une banque d'investissement canadienne, une société japonaise de jeux en ligne et une compagnie australienne ».

La dépense électrique du *bitcoin* n'est imputable ni aux coûts de la surveillance des transactions ni à la gestion de la *blockchain* à proprement parler, mais, comme l'explique Jean-Paul Delahaye, « au mode de distribution des *bitcoins* mis toutes les 10 minutes, et plus précisément encore, au concours entre les nœuds du réseau qui désignent toutes les 10 minutes le gagnant des *bitcoins* mis et des commissions associées aux transactions ». Ainsi, ce qui se révèle être le talon d'Achille de Bitcoin est, paradoxalement, la raison même pour laquelle les

transactions en *bitcoins* sont sécurisées : pour modifier un bloc de transactions, il faut en effet qu'un pirate mobilise lui tout seul plus de 51 % de la puissance de calcul de tous les mineurs, ce qui, au regard de la dépense énergétique actuelle, est devenu impossible.

Certaines *blockchains* publiques ne s'appuient pas sur la « preuve de travail » et la compétition entre certains nœuds du réseau pour valider les blocs de transactions. Citons notamment un autre système de validation des transactions appelé « preuve de participation » (*proof of stake*), mais dont la mise en œuvre n'est pas encore totalement réalisée sur une *blockchain* majeure. La preuve d'enjeu demande à l'utilisateur de « prouver la possession d'une certaine quantité de cryptomonnaie pour prétendre pouvoir valider des blocs supplémentaires dans la *blockchain* et pouvoir toucher la récompense, s'il y en a une, à l'addition de ces blocs ». Ce mécanisme de consensus consiste à résoudre un défi informatique appelé *minting* (monnayage), opéré par des « forgeurs ». Il ne nécessite pas de matériel informatique puissant et consomme peu d'électricité. Pour valider un bloc de transactions, le forgeur met en dépôt une certaine quantité de cryptomonnaie et recevra une récompense lorsqu'il valide un bloc pour le blocage de ce capital. Si le forgeur procède à une attaque informatique en insérant de faux blocs de transactions dans la *blockchain*, la communauté, à partir du moment où elle s'en rend compte pourrait procéder à un *hard fork* (voir [La rem n°40, p.29](#)), ce qui entraînerait la perte des dépôts de l'attaquant. Vitalik Buterin, cofondateur d'Ethereum explique : « la philosophie de la preuve d'enjeu résume en une phrase est donc pas à à la sécurité vient de l'énergie dépensée » mais plutôt « la sécurité vient des pertes économiques engendrées par une attaque ». Nombreux sont ceux qui considèrent que le mécanisme de consensus reposant sur la preuve d'enjeu est une « technologie verte » et qu'il constitue l'avenir des *blockchains*.

Le réseau Ethereum, la deuxième *blockchain* publique la plus capitalisée après le *bitcoin*, envisage de progressivement hybrider la validation des blocs par la preuve de travail et par la preuve d'enjeu, avant de basculer entièrement sur cette dernière, le projet étant actuellement en cours de développement.

Mais en l'état actuel des choses, si le système des *bitcoins* remplaçait le système des monnaies internationales usuelles comme le dollar ou l'euro, la consommation électrique du réseau serait équivalente à celle de la France ou même la dépasserait. Avec 468,4 TWh en 2015, celle-ci est classée au dixième rang des pays les plus consommateurs d'électricité au monde, après la Corée du Sud et devant le Royaume-Uni. La consommation énergétique du *bitcoin* semble, de loin, le défi majeur auquel devront répondre les développeurs informatiques de la monnaie numérique pour qu'elle perdure.

Sources :

- « A Proof of Stake Design Philosophy », Vitalik Buterin, medium.com/@VitalikButerin,

December 30, 2016.

- « Les consensus : Proof of work vs Proof of stake », David Teruzzi, Blogchaincafe.com, 14 mars 2016.
- « The lives of bitcoin miners digging for digital gold in Inner Mongolia », Zheping Huang et Joon Ian Wong, Qz.com, August 17, 2017.
- « L'Étrange quotidien des mineurs chinois dans les fermes géantes de bitcoins », Annabelle Laurent, Usbeketrica.com, 18 août 2017.
- « L'Électricité des crypto-monnaies », Jean-Paul Delahaye, Scilogs.fr, 18 octobre 2017.
- « A Deep Dive in a Real-World Bitcoin Mine », Digiconomist, October 25, 2017.
- « Le bitcoin, un fléau écologique », Emily Atkin, *The New Republic* (Washington), publié le 5 décembre 2017 in *Courrier international* n° 1416 du 21 décembre 2017 au 10 janvier 2018.
- « Ne nions pas le problème électrique du Bitcoin », Jean-Paul Delahaye, Scilogs.fr, 24 décembre 2017.
- « China to Curb Power Supply for Some Bitcoin Miners », Steven Yang, Bloomberg.com, January 4, 2018.
- « Bitcoin Miners Could Face Power Restrictions in China », Gareth Jenkinson, Cointelegraph.com, January 5, 2018.
- « Quel avenir pour le bitcoin spéculatif et énergivore ? », Forum, Valeursvertes.com, 10 janvier 2018.
- « Canada's Hydro Quebec unable to meet demand from digital currency miners », Allison Lampert, Reuters.com, January 19, 2018.
- « Even With Energy Surplus, Canada Unable to Meet Electricity Demands of Bitcoin Miners », Gareth Jenkinson, Cointelegraph.com, January 25, 2018.
- « Voyage au centre du bitcoin », Pierre Sorgue, *M, le Magazine du Monde*, 3 février 2018.
- « Nouveau tour de vis contre le bitcoin en Chine, Simon Lepître (Shanghai, correspondance), *Le Monde*, 6 février 2018.
- [Preuve d'enjeu](#), Wikipedia.

Categorie

1. Techniques

date créée

18 avril 2018

Auteur

jacquesandrefines