

ANALYSE

# Le bitcoin, une monnaie qui tourne au charbon

Par Savinien de Rivet(<http://www.liberation.fr/auteur/17648-savinien-de-rivet>) — 5 janvier 2018 à 12:08



Au cours de l'année 2017, la consommation d'électricité du bitcoin a dépassé celle d'une centaine de pays, dont l'Uruguay, l'Islande, le Nigeria et le Danemark. Photo Justin Tallis. AFP

Les opérations de «minage» de la cryptomonnaie nécessitent aujourd'hui de brûler plus de 11 millions de tonnes de charbon par an. Un chiffre en constante augmentation.

---

La Chine ira-t-elle jusqu'à interdire le «minage» du bitcoin pour éviter  
En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour vous proposer des services et offres

un gaspillage énergétique ? Les dirigeants de la Banque centrale de Chine ont indiqué, d'après une information publiée mercredi par l'agence Reuters, que la consommation d'électricité des «mineurs» de bitcoins sur le sol chinois pourrait être prochainement régulée voire contingentée. Cette annonce, qui suit l'interdiction en septembre des plateformes d'échanges de bitcoins sur le territoire chinois, pourrait provoquer de nombreux remous au sein de la cryptomonnaie au cours spectaculaire, ([http://www.liberation.fr/futurs/2017/12/22/le-bitcoin-s-offre-une-gueule-de-bois-pre-reveillon\\_1618564](http://www.liberation.fr/futurs/2017/12/22/le-bitcoin-s-offre-une-gueule-de-bois-pre-reveillon_1618564)) dont l'équation énergétique est aujourd'hui catastrophique.

---

**A LIRE AUSSI :**

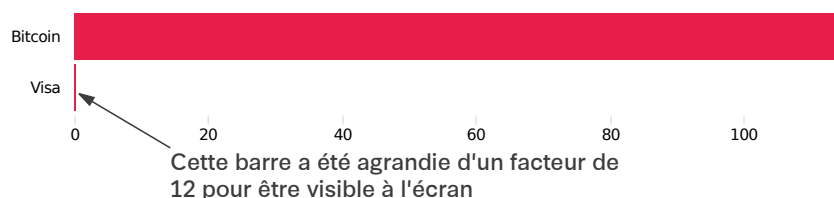
Le bitcoin, un mystère monétaire planétaire ([http://www.liberation.fr/futurs/2017/11/29/le-bitcoin-un-mystere-monetaire-planetaire\\_1613465](http://www.liberation.fr/futurs/2017/11/29/le-bitcoin-un-mystere-monetaire-planetaire_1613465))

---

## Une consommation d'électricité supérieure à celle du Danemark

Le site [Digiconomist](https://digiconomist.net/) (<https://digiconomist.net/>) a fait le bilan énergétique de la cryptomonnaie. Selon ses calculs, actuellement, le bitcoin nécessite 37 216 gigawattsheure par an pour sa consommation d'électricité, soit davantage que le Danemark. Avec l'énergie nécessaire pour une seule transaction, on pourrait charger entièrement la batterie d'une Tesla modèle S et effectuer un trajet de 500 kilomètres, ou fournir plus de onze jours d'électricité à un ménage américain. Une transaction en bitcoin consomme environ 115 kilos de CO<sub>2</sub>, soit environ 11 000 fois plus qu'une transaction par carte Visa.

## Le bitcoin consomme 11 000 fois plus par transaction que la carte Visa



Source: digiconomist.net

Les besoins en électricité du bitcoin ont largement crû l'an passé, parallèlement à la hausse des cours de la monnaie. Au cours de

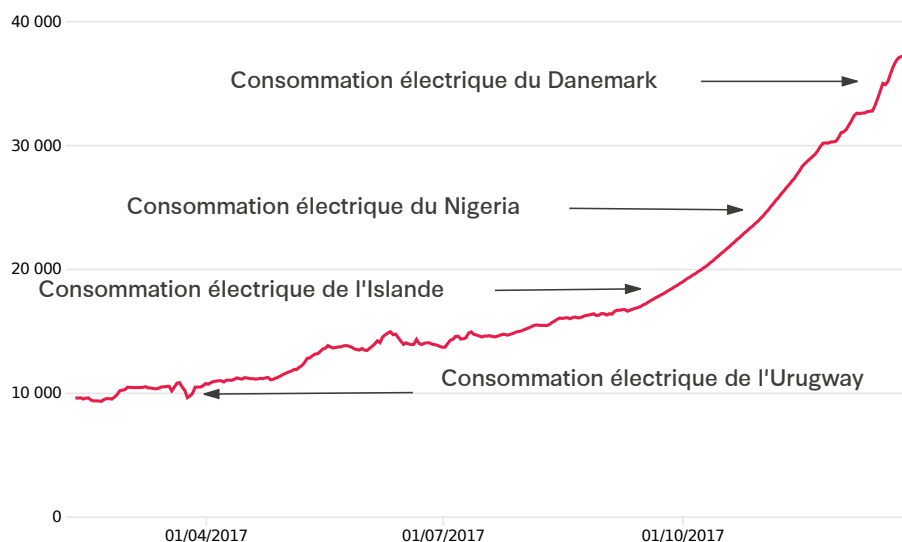
l'année 2017, la consommation d'électricité du bitcoin a dépassé celle

---

En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour vous proposer des services et offres

d'une centaine de pays, dont l'Uruguay, l'Islande, le Nigeria et le Danemark.

## Consommation du Bitcoin en Gigawatt/heure



Source: Digiconomist

Il y a dans le monde 163 pays (dont le Nigeria, pays de plus de 180 millions d'habitants) dont la consommation électrique est inférieure à celle du bitcoin. Au rythme actuel d'augmentation, le bitcoin consommerait d'ici un an la même quantité d'énergie que la France et en 2020, la totalité de l'électricité mondiale.

## Un principe de fonctionnement basé sur le «minage»

Comment en est-on arrivé là ? La source du problème se situe dans le fondement de l'algorithme. Lors d'une transaction bancaire classique (paiement par carte, virement...), une autorité centrale, ou tiers de confiance (en général une banque) vérifie sa validité – il faut par exemple, que le compte soit approvisionné – et s'en porte garant. Ceci n'est pas possible pour une monnaie décentralisée comme le bitcoin, bâtie sur le principe du refus d'une autorité centrale.

Les concepteurs de la monnaie ont donc décidé de confier la sécurisation des transactions à ses utilisateurs. Pour les inciter à être suffisamment nombreux à vérifier les transactions et éviter les fraudes, un système de récompense a été mis en place. Pour chaque groupe de

En pour un système de récompense a été mis en place. Pour chaque groupe de

transaction (on parle alors de «bloc»), de nombreux utilisateurs (on parle alors de «mineurs») se mettent en compétition pour être celui qui le vérifie et le valide. L'algorithme leur donne une suite de chiffres à trouver, suffisamment complexe pour que sa résolution nécessite de très nombreuses tentatives. Lorsqu'un mineur trouve la bonne suite de chiffres, il a le droit de valider le bloc, et les autres mineurs doivent confirmer la validité de la transaction. L'heureux gagnant se voit alors attribuer une certaine quantité de bitcoins (12,5 bitcoins en ce moment). Toutes les dix minutes, un nouveau bloc de transactions est validé.

Hash 0000000000000000018baeb2c91fe2b2d699f33f32a843a3cb5174289ab8700

Exemple de suite de chiffres (en hexadécimal) à trouver pour remporter la validation d'un bloc.

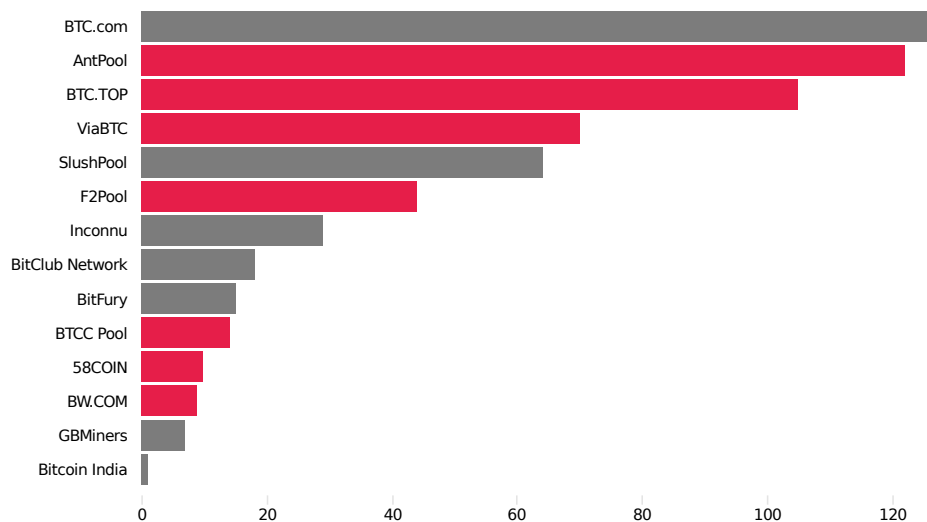
L'algorithme du bitcoin est ainsi paramétré pour augmenter la difficulté de trouver un bloc si la puissance de calcul augmente. Par ailleurs, plus la valeur de la monnaie est élevée, plus il est intéressant de remporter un bloc.

Pour profiter de l'aubaine, tout un écosystème s'est mis en place. Alors qu'à l'origine, il suffisait d'un simple ordinateur de bureau pour miner du bitcoin, aujourd'hui, il faut utiliser des machines ultraspécialisées. Des datacenters se sont installés, regroupant des milliers de serveurs fabriqués spécialement pour le minage du bitcoin.

### **Le charbon, source d'énergie principale**

Selon les estimations, entre 60 et 70% des mineurs de bitcoins opèrent depuis la Chine. Ce qui est confirmé par l'analyse de la répartition des gains de blocs du 1<sup>er</sup> au 4 janvier :

## La plupart des mineurs de bitcoin sont Chinois



Source: blockchain.info : nombre de blocs validés ces 4 derniers jours pour chaque pool de mineurs

Ces pools de mineurs de bitcoins utilisent donc l'électricité du réseau chinois pour faire tourner leurs serveurs. Or, environ les deux tiers de l'électricité chinoise sont produits à partir de charbon. Ce qui fait qu'à minima, entre 40 et 50% de l'électricité du bitcoin provient de la combustion du charbon. Selon nos calculs, ceci engendre la combustion d'au moins 11 millions de tonnes de charbon par an.

### Rendre le fonctionnement moins gourmand ?

Si on résume, les fondateurs du bitcoin ont fait mieux que les Shadoks qui pompaient dans le vide : ils ont créé un actif spéculatif qui nécessite de brûler à minima 11 millions de tonnes de charbon par an pour fonctionner. Serait-il possible de rendre son fonctionnement moins gourmand ?

Fabriquer des serveurs de minage de bitcoins plus performants ne changerait rien : les pools de mineurs adopteraient massivement ces nouveaux serveurs, et produiraient tous davantage de puissance de calcul. L'algorithme du bitcoin s'adapterait alors pour rendre les opérations plus compliquées.

L'autre solution serait de faire évoluer l'algorithme lui-même. C'est

En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour vous proposer des services et offres

possible, cela s'appelle un «fork» : il faut qu'une majorité de mineurs de bitcoins s'accorde pour le faire. Ils pourraient changer le protocole pour le rendre moins gourmand : passer de la preuve de travail à la preuve d'enjeu (1). Ou alors, faire en sorte que le calcul des opérations de minage ait une utilité scientifique. Ou encore, utiliser une forme de tiers de confiance. Ces trois différents protocoles sont utilisés par d'autres cryptomonnaies (successivement le «lisk», le «gridcoin» ou le «ripple»). Il ne semble cependant peu probable que le bitcoin adopte l'un ou l'autre de ces protocoles : les pools de mineurs ont massivement investi dans des serveurs utilisant le protocole actuel, il serait étonnant qu'ils décident en consensus de passer cet investissement par pertes et profits.

Pour éviter le rejet d'une quantité de plus en plus massive de tonnes de CO<sub>2</sub> dans l'atmosphère, la seule solution, outre un krach définitif de la cryptomonnaie, serait que les pouvoirs publics eux-mêmes en réglementent ou contingentent la consommation d'électricité. C'est ce qui pourrait se passer prochainement en Chine.

(1) Selon la preuve d'enjeu, ce sont les possesseurs de cryptomonnaie qui sont choisis aléatoirement pour sécuriser une transaction. Ils n'ont pour cela qu'à apporter la preuve qu'ils possèdent une certaine quantité de cette monnaie. Le protocole du bitcoin étant, pour sa part, la preuve de travail : il faut résoudre une équation nécessitant de très nombreuses tentatives pour remporter la mise.

[Savinien de Rivet \(http://www.liberation.fr/auteur/17648-savinien-de-rivet\)](http://www.liberation.fr/auteur/17648-savinien-de-rivet)