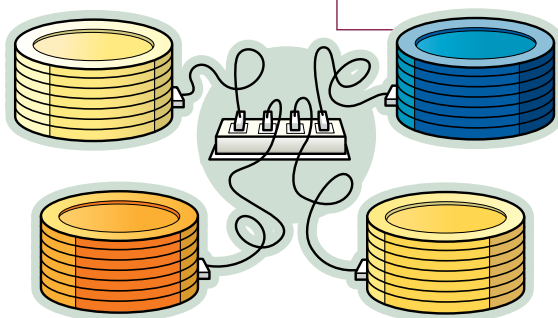


LA BLOCKCHAIN EST-ELLE UNE NOUVELLE SORTE D'INTERNET?

Non. La blockchain elle-même a besoin d'Internet pour déployer et maintenir son réseau pair à pair. Il convient aussi de noter que quand les gens parlent de « la » blockchain, sans plus de précisions, ils font presque toujours référence au système particulier que Satoshi Nakamoto a mis en place pour déployer le bitcoin. La blockchain du bitcoin a été le premier système de registre distribué ne faisant pas appel à un serveur centralisé ou une organisation pour son déploiement. Elle reste l'une des plus importantes : en janvier 2018, elle contenait plus de 154 gigaoctets (154 milliards d'octets) d'information, et chaque nouvelle transaction en augmente la taille. Mais cela reste très inférieur à la quantité de données présentes sur Internet, qui serait de l'ordre du yottaoctet (10^{24} octets, soit une différence de 13 ordres de grandeur).



1 500

C'est le nombre approximatif de cryptomonnaies en circulation à la fin de janvier 2018.

OÙ LE MINAGE SE FAIT-IL?

70 %

environ des bitcoins sont minés en Chine ; le deuxième pays le plus actif est l'Inde, avec 4 %. N'essayez pas de miner seul chez vous. La tâche est aujourd'hui dominée par de gigantesques fermes de minage, et les chances qu'un particulier mine des bitcoins sont extrêmement faibles. Il dépenserait beaucoup plus en factures d'électricité qu'il ne pourrait espérer gagner en profits.

QUELLES SONT LES FUTURES APPLICATIONS POSSIBLES DES BLOCKCHAINS ?

En voici quelques exemples.

- **Des voitures autonomes en autogestion** : Au lieu de rouler pour Uber, votre voiture se conduirait toute seule pendant que vous travaillez ou que vous dormez. Des contrats intelligents garantis par des blockchains pourraient faire disparaître les intermédiaires comme Uber et Blablacar de l'équation du covoiturage en automatisant leurs deux fonctions de base : la mise en relation des chauffeurs et des passagers, et la facilitation des paiements.
- **Des données médicales portables** : La technique qui permet à deux personnes d'échanger des bitcoins sans nécessairement se faire confiance pourrait également garantir l'information médicale, dont le contrôle serait entièrement entre les mains du patient. C'est ce qu'explique Brian Behlendorf, directeur exécutif du projet Hyperledger de la Fondation Linux, une trousse à outils pour construire des applications à blockchains. Les patients se verraient attribuer un « portefeuille santé » où figurent leurs données et leurs antécédents. Un médecin pourrait accéder à un registre et demander votre groupe sanguin, émettant une demande d'accès sur le téléphone de l'utilisateur. « Vous aurez ainsi un historique des personnes avec qui vous avez partagé les données, et la possibilité d'effacer l'information communiquée une fois terminé le traitement », indique Brian Behlendorf.
- **Un superordinateur global** : Vous pourriez participer à un superordinateur décentralisé mondial en reliant vos appareils à des milliers d'autres dans un réseau pair à pair, une blockchain permettant de vous rémunérer pour cela. Pendant que vous dormez, votre ordinateur portable et votre tablette pourraient être loués par des scientifiques souhaitant faire tourner des simulations, par exemple. Un projet nommé Golem y travaille déjà. La puissance cumulée des ordinateurs portables inactifs, très supérieure à la puissance des centres de données, accélérerait considérablement les calculs dans des domaines tels que la modélisation du climat.

QUELLES SONT LES LIMITES ET LES DANGERS DES BLOCKCHAINS ?

Emin Gün Sirer, chercheur à l'université Cornell spécialisé dans les blockchains, explique que ces dernières constituent un support quasiment impossible à modifier après coup. Mais il prévient : « Cela ne signifie pas que tout ce qui est inscrit sur une blockchain est vrai ou souhaitable. Si je suis piraté et que quelqu'un me vole mes cryptopièces et essaie de les utiliser, j'aurai très envie d'annuler cette transaction. Et c'est là que l'immuabilité devient un inconvénient. »

Il est également facile de confondre l'immuabilité théorique de la blockchain avec la sécurité réelle des données : les blockchains publiques telles que Bitcoin et Ethereum ne chiffrent en fait aucune information. Brian Behlendorf, de la Fondation Linux, va même plus loin : « Le registre ne devrait jamais être utilisé pour stocker des données personnelles ou quoi que ce soit de sensible, pas même sous forme chiffrée, dit-il, parce que quoi que nous chiffrions aujourd'hui, nous serons probablement en mesure de le déchiffrer dans quarante ou cinquante ans » avec les progrès de la technologie.

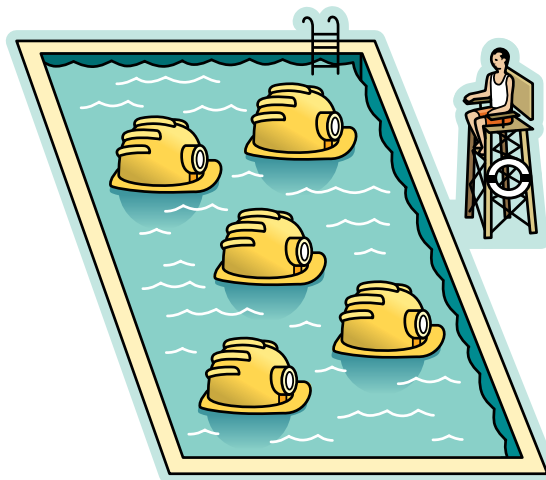
Certains partisans présentent les blockchains comme une panacée pour tout problème social où la confiance est un facteur important, mais c'est être aveuglément optimiste que de le croire (voir l'article de Natalie Smolenski, page 44).

QUELLE ÉNERGIE LES CRYPTOMONNAIES NÉCESSITENT-ELLES ?

Ce n'est pas parce que les cryptomonnaies n'ont pas d'attributs matériels que les utiliser ne coûte rien. Le processus volontairement intensif de minage des nouveaux bitcoins (la façon dont les nouvelles transactions sont ajoutées au registre, et qui permet aux mineurs de gagner des bitcoins) impose à l'ensemble du réseau pair à pair une grande masse de calculs pour valider les transactions de la blockchain. Tout ce traitement consomme de l'énergie.

Combien d'énergie au juste ? Commençons par la quantité de calculs. Début 2018, le taux de hachage du réseau Bitcoin tournait autour de 21 milliards de milliards de calculs par seconde de la fonction de hachage notée SHA256. Tirer de ce chiffre une estimation précise de la consommation énergétique est impossible parce que le réseau étant décentralisé, on ne peut connaître la consommation des nœuds individuels. Mais des estimations fiables placent la consommation électrique annuelle du réseau Bitcoin aux alentours de 40 térawattheures, soit à peu près 10 % de celle de la France entière. Pour chaque transaction, le réseau consommerait en moyenne plus de 500 kilowattheures, d'après le site Digiconomics (1 kilowattheure est l'énergie consommée par un radiateur de 1 000 watts au bout de 1 heure de fonctionnement). Celui-ci estime l'empreinte carbone de la consommation du réseau Bitcoin à 23 millions de tonnes de dioxyde de carbone (l'équivalent de l'empreinte carbone d'un pays tel que la Tunisie).

Le créateur d'Ethereum, Vitalik Buterin, envisage de faire basculer la blockchain du réseau vers un mécanisme de validation différent nommé preuve d'enjeu, qui ne repose pas du tout sur le minage. Il est peu probable que le réseau Bitcoin, plus vaste et plus décentralisé, en fasse de même à courte échéance. Mais Vinay Gupta, qui a conçu la stratégie de Dubaï en matière de blockchain, pense que l'appât du gain, qui motive les mineurs à transformer les kilowatts en cryptomonnaie, finira bien par les pousser à innover pour résoudre ce problème d'extensibilité. Selon l'investisseur en capital-risque Charlie Morris, quand les cryptomonnaies à preuve d'enjeu feront leurs preuves sur les marchés, « le minage ne sera plus qu'une petite aberration de l'histoire ». « Les gens diront : "Vous vous rappelez quand nous faisons tous ça ? C'était franchement ridicule, non ?" »



77 %

des organismes ou entreprises du secteur financier dans le monde devraient adopter les blockchains d'ici à 2020, selon PwC.

LES BLOCKCHAINS SONT-ELLES LÉGALES ?

Oui. Mais leur nature décentralisée et leur association avec le bitcoin (qui a été utilisé dans des transactions illégales telles que des ventes d'armes et de drogue) ont contribué à donner aux blockchains une réputation d'activité hors-la-loi qu'elles ne méritent pas forcément. Les blockchains peuvent être utilisées à des fins très variées, bonnes ou mauvaises, tout comme Facebook, le courrier électronique ou toute autre technologie Internet.

QUE PENSE LE PUBLIC DES CRYPTOMONNAIES ET DES BLOCKCHAINS ?

62 %

des Américains pensent que les cryptomonnaies sont utilisées pour réaliser des achats illégaux, ou ne savent pas du tout qu'elles sont utilisées, d'après un sondage de YouGov réalisé en 2017.

59 %

des consommateurs du monde entier sondés en 2017 par HSBC affirment ne pas avoir entendu parler de la technologie de la blockchain ; 80 % de ceux qui ont entendu parler de la technologie ne comprennent pas de quoi il s'agit.

39 %

des cadres supérieurs des grandes entreprises américaines admettent qu'ils connaissent peu ou pas du tout la technologie de la blockchain, d'après un sondage réalisé en 2017 par le cabinet Deloitte.