LES PRINCIPES DE BASE DU BITCOIN

1

La monnaie cryptographique bitcoin a été conçue par Satoshi Nakamoto (c'est un pseudonyme) en 2008 et mis en fonctionnement en janvier 2009. En voici les principes.

Un réseau d'ordinateurs auquel tout le monde peut participer gère un registre de comptes (la blockchain) qui indique combien de bitcoins sont détenus par les comptes. Tout le monde peut créer un compte sur ce registre. Le réseau est composé de nœuds principaux, chacun détenant le registre complet des comptes et enregistrant les transactions en bitcoins entre détenteurs de comptes. Tous ces nœuds ont les mêmes droits ; on parle de réseau décentralisé pair à pair.

Le registre et les transactions sont protégés par cryptographie. On aboutit ainsi à un accord unanime sur le contenu de chaque compte, et de cet accord naît la confiance à l'origine de la montée des cours du bitcoin. Depuis neuf ans que le réseau fonctionne, personne n'a pu en empêcher le fonctionnement ou le pirater, à l'exception d'un incident vite contrôlé et réparé en août 2010.

Le fonctionnement du réseau exige qu'il y ait des nœuds volontaires opérant les contrôles et gardant le registre de comptes. Un système de rémunération est prévu pour inciter à être l'un de ces nœuds : de nouveaux bitcoins sont émis et attribués aux nœuds volontaires. Tous les bitcoins en circulation ont été créés dans cet objectif par un concours répété toutes les 10 minutes.

UNITÉS D'ÉNERGIE

Le térawattheure (TWh) est l'énergie dépensée au bout de 1 heure par un dispositif ayant une puissance de 1 térawatt (TW). Le térawattheure est égal à 1 000 gigawattheures (GWh), c'est-à-dire 1 milliard de kilowattheures (kWh). En 1 heure, un radiateur ayant une puissance de 1 000 watts consomme 1 kWh d'électricité ; dans la même durée, un réacteur électronucléaire de 1 gigawatt, ou 1 000 mégawatts, produit 1 GWh, ou 1 milliard de kWh, d'électricité.

À nouveau, deux camps s'affrontent pour cette évaluation. Il y a ceux, peut-être un peu pessimistes, qui arrivent aux chiffres élevés mentionnés. Le site *Digiconomist*, créé par le Néerlandais Alex de Vries, est le plus sérieux représentant de ce camp qui exprime une inquiétude et finalement de la méfiance vis-à-vis des cryptomonnaies, dont l'empreinte écologique semble déraisonnable.

Un autre camp, plus optimiste, arrive à des chiffres en gros deux fois plus faibles. Son représentant le plus précis est Marc Bevand, un Français vivant aux États-Unis, qui s'exprime aussi sur Internet (*voir la bibliographie*).

L'ÉQUIVALENT D'AU MOINS 10 % DE LA CONSOMMATION FRANÇAISE D'ÉLECTRICITÉ

Même pour les optimistes, la dépense électrique est importante et atteint 5 % de la consommation électrique française. Elle ira en croissant si l'intérêt pour les cryptomonnaies se confirme et que leurs cours montent. En prenant en compte les autres monnaies cryptographiques analogues au bitcoin, il faut doubler l'évaluation optimiste; c'est donc au moins l'équivalent de 10 % de la consommation française d'électricité que les monnaies cryptographiques représenteraient... et bien plus dans le futur.

Pour inciter les acteurs (les nœuds) à participer à la gestion et à la surveillance du réseau bitcoin (ce qui permet son fonctionnement sans autorité centrale de contrôle), un système de rémunération a été prévu dès la conception du bitcoin en 2008 par le mystérieux Satoshi Nakamoto. Les nœuds du réseau qui le font fonctionner sont rémunérés en nouveaux bitcoins créés périodiquement selon un programme fixé une fois pour toutes: 12,5 bitcoins sont émis toutes les 10 minutes. Ces nouveaux bitcoins, ainsi que des commissions liées aux transactions qui s'ajoutent aux 12,5 bitcoins, sont attribués à un seul nœud du réseau à la suite d'une compétition.

Ce concours consiste à résoudre un problème de nature mathématique. On a d'autant plus de chances de le résoudre en premier, donc de gagner les 12,5 bitcoins émis et les commissions liées aux transactions, qu'on est capable de calculer rapidement une fonction notée SHA256. Ceux qui participent à ce concours, les « mineurs », ainsi nommés par analogie avec les mineurs dans une mine d'or, sont pris dans une course, chacun essayant d'avoir la capacité maximale à calculer la fonction SHA256.

Au début, on effectuait les calculs de la compétition avec des machines courantes ou même sur des ordinateurs de bureau ou portables. Certains participants ont rapidement compris que les cartes graphiques étaient plus efficaces, donc dépensaient moins d'électricité, pour calculer la fonction SHA256. Ils les ont donc utilisés massivement. Rapidement encore, un second pas a été franchi en concevant et en fabriquant des puces spécialisées Asic (*Application-specific integrated circuit*) qui calculent la fonction SHA256 et ne font rien d'autre. Aujourd'hui, ceux qui participent à la course au calcul du SHA256 ne restent >