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 >

> compétitifs qu'en utilisant de telles puces, que l'on fabrique par millions et que l'on perfectionne d'année en année. Le minage de bitcoins est devenu une industrie, dont 70 % sont localisés en Chine.

La puissance totale du réseau, mesurée par sa capacité à calculer des fonctions SHA256, est devenue colossale. Environ 14 milliards de milliards de calculs de SHA256 sont effectués chaque seconde. Le coût électrique de cette activité est bien sûr important et, à moyen terme, c'est-à-dire en quelques mois, il devient égal à un certain pourcentage de la valeur des bitcoins émis et des commissions associées aux transactions.

Le raisonnement justifiant cette affirmation est simple. Lorsque les coûts des systèmes de minage sont supérieurs à ce qu'ils rapportent, on cesse de les utiliser ; lorsqu'ils sont inférieurs à ce qu'ils font gagner, de nouvelles « mines à bitcoins » sont créées. La logique de ce système est comparable à l'exploitation des mines d'or : quand le cours de l'or baisse, certaines mines d'or ne sont plus rentables et sont fermées ; quand le cours monte, des gisements inexploités deviennent intéressants, de nouvelles mines s'ouvrent et certaines mines qui avaient été fermées sont remises en exploitation. En quelques mois, par l'implacable logique de la recherche du profit, se produit un nouvel équilibre entre le coût d'extraction et les gains qu'on en tire.

2 UN TABLEAU DES DÉPENSES ÉNERGÉTIQUES

DÉPENSE ANNUELLE D'ÉLECTRICITÉ DUE À LA GESTION DU RÉSEAU BITCOIN

Les chiffres suivants, exprimés en térawattheures (TWh), ont été calculés à la date du 1er janvier 2018.
Dépense actuelle : 18 TWh (hypothèse optimiste) ou 36 TWh (hypothèse pessimiste).
Dépense après ajustement des coûts du minage aux gains obtenus par le minage : 35 à 50 TWh (hypothèse optimiste) ou 70 à 100 TWh (hypothèse pessimiste).
Dépense quand la capitalisation des bitcoins aura atteint celle des billets de dollars (M0) : 175 à 250 TWh (hypothèse optimiste) ou 350 à 500 TWh (hypothèse pessimiste).
Dépense quand la capitalisation des bitcoins aura atteint M1 (M0 + dépôts à vue) : 500 à 750 TWh (hypothèse optimiste) ou 1 000 à 1 500 TWh (hypothèse pessimiste).

CONSOMMATION ANNUELLE D'ÉLECTRICITÉ DE QUELQUES PAYS (EN 2015, D'APRÈS L'AIEA)

Luxembourg	8 TWh	Espagne	254 TWh
Tunisie	16 TWh	Royaume-Uni	330 TWh
Danemark	33 TWh	France	468 TWh
Portugal	50 TWh	Allemagne	573 TWh
Suisse	62 TWh	Russie	949 TWh
Belgique	87 TWh	États-Unis	4 128 TWh
Turquie	229 TWh	Monde	22 234 TWh

L'intérieur d'une usine de minage de bitcoins de la compagnie Genesis Mining, en Islande.

UNE DÉPENSE DE L'ORDRE DE 50 % DU GAIN APPORTÉ PAR LES BITCOINS

Le coût en électricité n'est pas le seul prix de la course aux calculs de la fonction SHA256, car il faut acheter les puces spécialisées et mettre en place les mines à bitcoins – aujourd'hui de véritables usines composées de plusieurs bâtiments et employant des dizaines d'ouvriers et techniciens. La consommation électrique représente un pourcentage assez stable du coût de fonctionnement et d'amortissement de ces mines numériques : après égalisation entre le coût et le gain, l'électricité dépensée est de l'ordre de 50 % de ce que rapportent les bitcoins créés et les commissions.

C'est principalement sur ce pourcentage difficile à évaluer que se disputent les optimistes et les pessimistes. Le désaccord sur sa valeur explique pour l'essentiel les chiffres contradictoires avancés par les deux partis : les optimistes emploient la valeur 30 % ou moins, les pessimistes utilisent 60 %, parfois plus. Mais, quelle que soit la valeur retenue, il résulte de cette implacable logique économique que plus le cours du bitcoin est élevé, plus il y a d'électricité dépensée par ceux qui veulent s'approprier les bitcoins émis et les commissions associées aux transactions.

Ce raisonnement n'est valable que pendant les périodes où l'émission de nouveaux bitcoins est stable. Or le protocole d'émission des bitcoins, fixé en 2008, a prévu une division par deux de l'émission tous les quatre ans. L'émission a été divisée par deux en 2016 (passage de 25 bitcoins à 12,5) ; elle le sera de nouveau en 2020 et passera de 12,5 à 6,25 bitcoins par tranche de 10 minutes. Il faudrait donc intégrer dans les prévisions à long terme de la dépense électrique du réseau une division par deux de la dépense électrique une fois tous les quatre ans. Mais il faudrait aussi intégrer dans ce calcul les commissions associées aux transactions, qui viennent s'ajouter aux bitcoins émis par le protocole et contribuent à la