LA FOLIE ÉLECTRIQUE DU BITCOIN

Les cryptomonnaies telles que le bitcoin se substitueront-elles un jour au dollar et à l'euro? Rien n'est moins sûr, si l'on considère l'effrayante consommation d'électricité liée au fonctionnement de ces monnaies numériques.

RENDEZ-VOUS

L'AUTEUR

JEAN-PAUL DELAHAYE
professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (Cristal)

Dans le numéro de *Pour la Science* de décembre 2013, cette rubrique présentait la cryptomonnaie nommée bitcoin et en expliquait le fonctionnement général (*voir l'encadré 1 pour un résumé*). La valeur d'un bitcoin était alors de 100 euros; le 1er janvier 2018, date à laquelle correspondront les chiffres et calculs indiqués ici, le bitcoin valait 11500 euros!

S'agit-il d'une bulle spéculative ou d'une valorisation ayant un fondement réel? Deux camps s'opposent. D'un côté, des économistes et des spécialistes des monnaies jugent qu'il s'agit d'une «fraude» (terme employé par Jamie Dimon, directeur de la banque JP Morgan Chase) et que tout va s'effondrer, c'est-à-dire que le cours chutera brusquement, voire deviendra nul. Ils sont presque aussi nombreux qu'en 2013.

Dans l'autre camp, les défenseurs des monnaies cryptographiques avancent divers arguments pour justifier la valeur du bitcoin et de ses sœurs. Pour eux, les caractéristiques des monnaies cryptographiques – anonymat, irréversibilité, décentralisation, ouverture à tous, émission fixée à l'avance et rapidité des transactions – en font des monnaies nouvelles sans équivalent, utiles pour une fluidité plus grande des déplacements d'argent sur le réseau et pour un meilleur fonctionnement général de l'économie.

Il faut attendre pour déterminer quel camp a raison. Un point cependant soulève l'inquiétude: le réseau informatique qui assure le fonctionnement des échanges de bitcoins et leur sécurisation a une importante consommation d'énergie électrique. Toujours à la date du 1er janvier 2018, le site internet spécialisé *Digiconomist* l'a évaluée à 36 térawattheures par an, ce qui correspond à la dépense électrique annuelle de plus de 3,4 millions de foyers américains, ou encore à 0,16 % de la production électrique mondiale.

Cette quantité d'énergie brûlée par le réseau est appelée à croître. Un raisonnement économique que nous détaillerons plus loin montre que la dépense électrique du réseau est proportionnelle au cours du bitcoin, avec un délai d'ajustement de plusieurs mois pour que les investissements de rattrapage se mettent en place quand le cours augmente (une sorte d'inertie). Comme le cours du bitcoin a été multiplié par plus de 14 en un an, l'ajustement de la consommation lié au cours actuel n'a pas totalement eu lieu et se fera en multipliant au moins par 2 ou 3 dans les prochains mois la consommation électrique du réseau actuel. C'est une certitude... sauf si le cours du bitcoin s'écroule.

ENTRE 70 ET 100 TÉRAWATTHEURES D'ÉLECTRICITÉ DÉPENSÉS PAR AN!

On aboutira alors à une consommation électrique du réseau informatique du bitcoin comprise entre 70 et 100 TWh par an, équivalente à celle d'un pays tel que la Belgique.

Les évaluations mentionnées sont approximatives, car il est impossible de savoir dans le détail qui dépense de l'électricité et combien pour l'extraction de nouveaux bitcoins.

Jean-Paul Delahaye a récemment publié: **Les Mathématiciens se plient au jeu**, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2017).

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.

© Marco Krohn CC BY-SA 4.0

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

rémunération des mineurs. Ces commissions évoluent de façon complexe, mais en gros elles augmentent en même temps que la valeur du bitcoin. Elles ont d'ailleurs été introduites par Satoshi Nakamoto pour compenser la division par deux tous les quatre ans et faire qu'il y ait toujours des gens intéressés pour surveiller et faire fonctionner le réseau. On peut faire l'hypothèse que, en première approximation, ce qu'a prévu le créateur du bitcoin se produira ; cela signifie que dans les prévisions des futures dépenses électriques, on peut ne pas prendre en compte la division par deux tous les quatre ans, qui est compensée par le système des commissions.

Qu'adviendrait-il si la valeur des bitcoins égalait celle des dollars ou des euros ?

Au 1er janvier 2018, la valeur de tous les bitcoins en circulation était d'environ 230 milliards de dollars. La valeur de tous les billets en dollars en circulation est, d'après la FED (la Réserve fédérale des États-Unis), de 1500 milliards de dollars (chiffres de décembre 2016). Pour l'euro, on a des chiffres du même ordre de grandeur. Il y a donc 6 fois plus de dollars sous forme de billets en circulation que de dollars sous forme de bitcoins. Si le volume des bitcoins en circulation devenait, en valeur, équivalent aux dollars circulant sous forme de billets, cela signifierait que le cours du bitcoin a été multiplié par 6. En effet, les bitcoins émis représentent 80 % des 21 millions de bitcoins prévus par Satoshi Nakamoto.

L'HORIZON DU BITCOIN BOUCHÉ PAR LE MUR DE LA DÉPENSE EN ÉLECTRICITÉ

Seule l'augmentation de la valeur unitaire du bitcoin peut amener à ce que leur total s'approche, en valeur, du total des billets de dollars en circulation. Cette multiplication par 6 de la valeur des bitcoins (ou par 5 si l'on veut prendre en compte les 20 % de bitcoins non émis) ne semble pas impossible au vu de ce qui s'est passé depuis deux ans.

Une telle multiplication par 5 conduirait la dépense électrique du réseau bitcoin à une valeur comprise entre 350 et 500 TWh par an pour les pessimistes, et entre 175 et 250 TWh par an pour les optimistes. Ce serait alors, en ordre de grandeur, comparable à la consommation électrique française annuelle.

Rien ne pourra arrêter cette croissance sans une volonté déterminée, soit de la communauté qui en a collectivement le pouvoir mais dont ce n'est pas l'intérêt, soit des États en imposant un contrôle ou en interdisant ce type de mécanisme numérique et économique diabolique.

Les chiffres cités correspondent à des évaluations assez imprécises, mais les ordres de grandeur sont corrects et bien sûr donnent le >

3

L'OR ET LE BITCOIN

On a souvent comparé le bitcoin et l'or. Certes, un point commun est que la quantité d'or disponible sur Terre, comme la quantité de bitcoins, ne résulte pas de la volonté d'un État ou d'une banque émettrice, mais est fixée par des contraintes impossibles à manipuler : les réserves terrestres dans le cas de l'or, et le protocole de Satoshi Nakamoto défini en 2008 qui fait qu'il n'y aura jamais plus de 21 millions de bitcoins.

Mais, en valeur, il y a beaucoup plus d'or que de bitcoins. On estime la valeur de tout l'or terrestre à 8 000 milliards de dollars, alors qu'il n'y a actuellement que quelque 230 milliards de dollars en bitcoins (au 1/1/2018). Le bitcoin ne peut donc pas aujourd'hui se substituer à l'or, contrairement à ce que certains prétendent.

Chaque année, on extrait environ 2 500 tonnes d'or. À raison de 41 000 dollars le kilogramme, cela fait environ 100 milliards de dollars. C'est, en ordre de grandeur, la valeur de la moitié des bitcoins existants et 10 fois plus que la valeur des bitcoins émis chaque année. Là encore, on voit que l'or domine par rapport au bitcoin.

Les défenseurs des monnaies cryptographiques font remarquer qu'on dépense donc beaucoup plus par an en moyens pour extraire de l'or (sans doute à peu près sa valeur, soit environ 100 milliards de dollars) que pour extraire des bitcoins (ce sera environ 10 milliards de dollars quand le coût de production se sera ajusté au cours du bitcoin le 1/1/2018). La dépense pour extraire de l'or a aussi, comme pour les bitcoins, un important coût écologique, aujourd'hui bien supérieur à celui de l'extraction des bitcoins. Ce dernier ne devrait donc pas nous effrayer, selon les partisans du bitcoin.

La réponse de ceux qui considèrent le bitcoin dangereux est que l'or est utile (par exemple en électronique) alors que les bitcoins produits ne servent à rien d'autre qu'à opérer des échanges. De plus, pour que les bitcoins émis puissent vraiment rivaliser avec une monnaie internationale, il faudrait que le cours du bitcoin soit multiplié par 15 pour atteindre la valeur des dollars en billets et sur les comptes à vue, ce qui conduirait alors à une dépense du réseau bitcoin supérieure au coût annuel de l'extraction de l'or : extraire les bitcoins sera alors plus cher qu'extraire l'or !

© Tschub / shutterstock.com

> vertige… Ils montrent simplement qu'il n'est guère envisageable que les bitcoins en circulation ou plus généralement les monnaies cryptographiques fonctionnant sur son modèle se substituent un jour aux monnaies internationales d'échange que sont le dollar et l'euro.

Notons aussi que nous avons seulement envisagé une augmentation du cours du bitcoin pour que leur total égale en valeur les billets en dollars, ce que les économistes nomment la « base monétaire » et notent M0. Si nous avions pris en compte la valeur de la masse monétaire M1, qui inclut en plus l'argent présent sur les comptes à vue des particuliers et des entreprises (M1 vaut environ le triple de M0), nous serions arrivés à une dépense électrique trois fois plus importante. Les chiffres seraient alors compris entre 1000 et 1500 TWh par an pour les pessimistes, et entre 500 et 750 TWh pour les optimistes. Dans le meilleur des cas, on atteindrait des chiffres comparables au huitième de la consommation électrique des États-Unis (4128 TWh en 2015) et, dans le pire des cas, au tiers.

LE SYSTÈME D'INCITATION EST EN CAUSE

Peut-on changer le mode de fonctionnement des monnaies cryptographiques pour éviter cette folle dépense électrique?

La consommation d'électricité liée au bitcoin n'est pas due aux coûts de la surveillance des transactions et à la gestion de son registre de comptes (la blockchain). Elle est due au mode de distribution des bitcoins émis toutes les 10 minutes, plus précisément au concours entre les nœuds du réseau qui désigne toutes les 10 minutes le gagnant des bitcoins émis et des commissions associées aux transactions. D'autres mécanismes fondés sur l'idée des blockchains n'utilisent pas ce système d'incitation et encore moins de concours entre les nœuds des réseaux associés, car ils n'en ont pas besoin.

Ainsi, les « blockchains privées », qui servent par exemple à gérer des échanges entre un consortium de banques en nombre fixé, ne sont pas du tout sujettes aux énormes dépenses électriques du bitcoin: elles n'ont pas besoin de systèmes d'incitation, puisque chaque acteur du réseau est intéressé par avance au bon fonctionnement du réseau. Seule la volonté de faire reposer le fonctionnement du bitcoin sur un réseau pair à pair, anonyme, décentralisé, ouvert et extensible oblige à mettre en place un système d'incitation assurant l'existence des volontaires s'occupant de gérer et surveiller le réseau, ainsi qu'un concours entre nœuds pour attribuer l'incitation. La véritable question est celle du concours pour l'attribution de la prime d'incitation.

Peut-on concevoir un autre type de concours qui n'entraînerait pas l'aberration électrique du bitcoin? La question n'est pas nouvelle et de nombreuses idées ont été proposées pour opérer autrement la distribution de l'incitation. Hélas, aucun système de remplacement n'a encore réussi à convaincre pleinement.

L'explication pourrait être liée à la notion de contenu en calcul, que nous avons traitée plusieurs fois dans cette rubrique (*voir « Qu'est-ce qu'un objet complexe? »*, Pour la Science, *mai 2013*). En effectuant leurs calculs pour remporter le concours toutes les 10 minutes, les nœuds du réseau consomment de l'électricité; le calcul produit la solution à un problème (peu intéressant, mais difficile) qui est mis dans le registre des comptes du bitcoin. Ce dépôt a pour conséquence que le registre est difficile à falsifier. Pour le falsifier et créer un registre pouvant se substituer au registre courant (et permettant de détourner des bitcoins d'un compte vers un autre), il faudrait calculer autant que ce qui a été calculé par tout le réseau, et donc dépenser autant d'énergie électrique que ce qui a été consommé par le réseau en entier, au moins sur la période qu'on souhaite falsifier. C'est donc impossible ou extrêmement coûteux. La robustesse du bitcoin semble essentiellement liée à cette impossibilité presque absolue de fabriquer un faux registre, impossibilité qui disparaît probablement quand on change la méthode de distribution par concours de calcul.

À EN VOULOIR TROP, ON RISQUE DE TOUT PERDRE

C'est la volonté d'avoir un système protégé par le placement d'une quantité colossale de calculs (et donc d'électricité) dans le registre des comptes pour le rendre infalsifiable qui est à l'origine du problème. Malheureusement, cette solidité presque parfaite a un prix: l'impossibilité que le cours du bitcoin augmente au point de devenir un jour un véritable concurrent du dollar ou de l'euro.

Entre les systèmes à blockchains privées, simples et électriquement viables, et les systèmes à blockchains publiques, totalement décentralisés, ouverts, anonymes et disposant d'une configuration extensible des nœuds – des systèmes qui, eux, semblent absurdes et finalement condamnés par avance –, il faut choisir ou inventer des systèmes intermédiaires. Pour donner naissance à une nouvelle monnaie internationale, il sera nécessaire de renoncer à certaines propriétés de la monnaie mise en route par le génial Satoshi Nakamoto. ■

BIBLIOGRAPHIE

J. Favier et A. Takkal Bataille, **Bitcoin, la monnaie acéphale**, CNRS Éditions, 2017.

M. Bevand, **Electricity consumption of bitcoin : A market-based and technical analysis**, http://blog.zorinaq.com/bitcoin-electricity-consumption/, 10 mars 2017.

Bitcoin energy consumption index, *Digiconomist*, consulté le 1/1/2018 (https://digiconomist.net/bitcoin-energy-consumption).

J.-P. Delahaye, **Mathématiques et mystères**, Belin/Pour la Science, 2016 (trois chapitres consacrés au bitcoin, aux preuves de travail et aux blockchains).