

GLOSSAIRE

CRYPTOMONNAIE

Forme de monnaie numérique reposant sur des méthodes cryptographiques afin de contrôler comment et quand sont créées les unités de monnaie, et de garantir le transfert sécurisé des fonds.

RÉSEAU PAIR À PAIR

Réseau d'ordinateurs reliés de façon décentralisée, tout ordinateur pouvant communiquer de proche en proche avec tout autre sans passer par un serveur central ou un administrateur.

ŒUD

Ordinateur participant à un réseau pair à pair. Le réseau du bitcoin comporte aujourd'hui plusieurs milliers de nœuds.

REGISTRE DISTRIBUÉ

Liste de transactions inscrites et horodatées qui est simultanément diffusée, copiée et vérifiée par tous les nœuds d'un réseau pair à pair. Si chaque nœud du réseau a une copie identique du registre, il est facile de repérer les entrées falsifiées ou les versions corrompues.

BLOC

Groupe de transactions enregistrées sur une blockchain. Dans le réseau du bitcoin, de nouveaux blocs sont ajoutés à la chaîne toutes les 10 minutes.

HACHAGE

Méthode cryptographique qui utilise une fonction mathématique (une « fonction de hachage ») pour condenser un ensemble quelconque de données en une chaîne unique de caractères alphanumériques de longueur fixe donnée, nommée valeur de hachage. Cela crée une empreinte numérique des données hachées facilement vérifiable : il suffit qu'un seul bit des données originales soit modifié ou corrompu pour que l'empreinte donnée par la fonction de hachage soit complètement différente. Le hachage est « à sens unique » : les données ne peuvent pas être reconstituées à partir de leur empreinte.

MINAGE

Ce terme désigne le processus par lequel les nœuds d'un réseau de cryptomonnaie rivalisent entre eux pour ajouter de façon sécurisée un nouveau bloc de transactions à une blockchain. Des unités de monnaie sont attribuées en récompense – une incitation financière à assurer la sécurité. Le minage implique de télécharger la dernière version en date des transactions de la blockchain pour vérification, puis d'effectuer des calculs systématiques pour rechercher la solution à une énigme mathématique compliquée, créée via le hachage du bloc. Le premier nœud qui trouve la bonne solution « mine » ce bloc : il l'ajoute à la chaîne de blocs et décroche la récompense associée. Plus un mineur dispose de puissance de calcul pour rechercher la solution, plus il a de chances de la trouver, un processus dit de validation par preuve de travail.

BITCOIN ET BLOCKCHAIN, EST-CE LA MÊME CHOSE ?

Non, mais ils sont régulièrement confondus parce qu'ils ont été portés ensemble à la connaissance du public en 2008, quand Satoshi Nakamoto a publié son article décrivant comment créer la monnaie bitcoin grâce à la technologie des blockchains qu'il inventait. Le bitcoin est un type de cryptomonnaie parmi d'autres. Quant à la blockchain, c'est la technique grâce à laquelle le système du bitcoin peut exister ; il s'agit d'une infrastructure que l'on peut utiliser pour assurer le suivi de nombreux types de transactions. La technique des blockchains existe sans le bitcoin, mais l'inverse n'est pas vrai.

D'OÙ VIENT LA VALEUR D'UNE CRYPTOMONNAIE ?

Selon certains experts, une cryptomonnaie telle que le bitcoin a de la valeur en vertu de sa sécurité (la blockchain du bitcoin n'a jamais été piratée jusqu'à présent) ou de sa rareté imposée (17 millions de bitcoins sont en circulation à ce jour ; le nombre total de bitcoins émis a été limité à 21 millions, ce qui signifie que le bitcoin ne pourra jamais être dévalué en « faisant tourner la planche à billets »). D'autres affirment que la cryptomonnaie a une valeur intrinsèque, le minage étant un travail fastidieux qui renforce le réseau ; en d'autres termes, c'est l'effort qui confère de la valeur. Mais cela ne s'applique pas à une cryptomonnaie ne faisant pas appel au minage. Selon Christian Catalini, du MIT, « sa valeur découle du consensus. Nous sommes tous d'accord qu'elle a de la valeur ». La monnaie est un moyen social d'assurer le suivi des échanges et des dettes ; si les cryptomonnaies se révèlent plus efficaces pour assurer ce suivi, leur valeur est assurée, qu'elles représentent un bien matériel ou juste un nombre.

LE BITCOIN, MONNAIE DE DEMAIN OU FEU DE PAILLE ?

Le bitcoin est la monnaie virtuelle la plus populaire, mais elle est aussi largement spéculative et très volatile : par exemple, le bitcoin a perdu 40 % en deux semaines en septembre 2017, avant de rebondir et d'atteindre des sommets à la fin de l'année, puis de chuter violemment au début de janvier 2018. Pour certains experts, les limites techniques du réseau (sa gestion des transactions est lente) combinées à des coûts de minage importants grèvent l'avenir de cette cryptomonnaie. « Nous ne parions pas sur le bitcoin », affirme Charlie Morris, directeur des placements chez Next-Block Global, entreprise qui investit dans la technologie des blockchains.

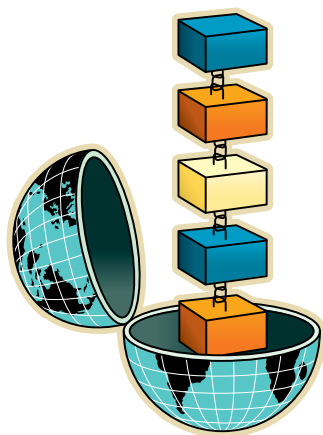
Ether, la deuxième plus grande monnaie virtuelle, a peut-être plus de ressorts pour durer. Ether n'est pas tant une monnaie analogue à des espèces qu'un « actif à blockchain », selon les mots de Charlie Morris, utilisé pour alimenter et sécuriser le réseau Ethereum. Un peu comme lors de la location de serveurs virtuels dans le cloud de Google, les développeurs souhaitant créer des applications à l'aide de la blockchain d'Ethereum doivent payer leur accès en unités monétaires appelées ethers. Plus Ethereum devient utile en tant que plateforme grand public, plus l'ether acquiert de valeur et de stabilité. De nouvelles plateformes et monnaies vont très probablement émerger – la course à la domination ne fait que commencer.

35 %

C'est la part approximative que représentent les bitcoins en termes de capitalisation, parmi l'ensemble des cryptomonnaies.

10 %

C'est la part du PIB mondial qui sera stockée dans des blockchains d'ici à 2025, d'après un rapport du Forum économique mondial datant de 2015.



VA-T-ON VERS LA FIN DES ESPÈCES ?

On pourrait avoir l'impression que les billets et les pièces de monnaie vont disparaître, mais, d'après les experts, on en est loin. On utilise encore beaucoup les espèces et le système actuel ne dysfonctionne pas au point qu'on veuille le défaire. Certes, le bitcoin et l'éther peuvent servir de valeurs ou d'unités d'échange, mais ils ne sont pas acceptés comme monnaie légale dans suffisamment d'endroits pour faire concurrence aux espèces.

Dans des pays tels que le Kenya, où peu de gens ont des comptes bancaires classiques et où des services financiers par téléphonie mobile tels que M-Pesa ont rendu les placements et les virements d'argent par téléphone beaucoup plus faciles que les échanges d'argent physique, les cryptomonnaies pourraient sembler tout adaptées. À condition que le minage se fasse ailleurs : il consomme beaucoup d'électricité, ressource peu disponible en Afrique, continent où les téléphones portables de base se vendent beaucoup mieux que les smartphones, et où les possesseurs d'ordinateurs personnels sont peu nombreux.

QUI SONT LES UTILISATEURS DE BLOCKCHAINS ?

Les blockchains ne servent pas qu'aux cyberlibertaires, et elles sont loin de ne concerner que la finance. Voici quelques exemples.

- **Institutions financières** : Des banques globales et organismes de placement travaillent sur des projets de blockchains, parfois en s'unissant au sein de consortiums. Depuis 2012, Ripple est un système prospère fondé sur une blockchain qui gère les transactions internationales entre banques. De jeunes pousses projettent de déployer des blockchains dans le domaine de l'évaluation du crédit ; elles espèrent ainsi mettre fin aux fuites de données, comme celle qu'a subie la société Equifax, victime d'un piratage.
- **Administrations** : Aux États-Unis, le Delaware et l'Illinois utilisent des registres distribués pour les certificats de naissance. Dubaï a intégré les blockchains à plusieurs de ses services administratifs, comme l'obtention de licences. En 2016, la Tunisie a commencé à émettre une version numérique de sa devise nationale adossée à une blockchain et appelée eDinar.
- **Entreprises de technologie** : Le réseau Ethereum (conçu comme support de nouvelles applications, et non en tant que simple écosystème pour monnaie virtuelle comme le réseau Bitcoin) est comparable à un App Store pour les jeunes pousses des blockchains. Des centaines de projets et d'entreprises l'exploitent, telle la société WePower, une plateforme d'échanges d'énergies renouvelables entre particuliers.
- **Droits d'auteur et propriété intellectuelle** : La musicienne britannique Imogen Heap a lancé Mycelia, un incubateur technologique qui assure le suivi des métadonnées associées aux œuvres de création, supprimant les intermédiaires tels que iTunes.
- **Organismes d'assistance et à but non lucratif** : La BitGive Foundation encourage et responsabilise le don caritatif. Et le programme alimentaire mondial des Nations Unies rationalise la façon dont elle assure le suivi et la distribution de l'aide aux réfugiés syriens en Jordanie.
- **Institutions académiques** : Le projet Blockcerts vise à rendre tous les diplômes et certificats professionnels plus fiables et faciles à partager.
- **Gestionnaires de biens** : L'entreprise Everledger, basée à Londres, cible l'industrie du diamant en enregistrant les attributs et la provenance de chaque pierre précieuse.
- **Journalistes** : Pour contrer les fausses informations, Civil offre aux journalistes une plateforme pour créer un journalisme inaltérable, sans publicité, protégé contre les intérêts extérieurs (Russie, Facebook...) et soutenu par les lecteurs.
- **Gens ordinaires** : Pour les travailleurs migrants qui envoient de l'argent à leur famille restée au pays, l'utilisation de bitcoins coûte moins que les transferts par Western Union ; ainsi, environ 20 % des transferts d'argent entre la Corée du Sud et les Philippines se font maintenant par ce biais.

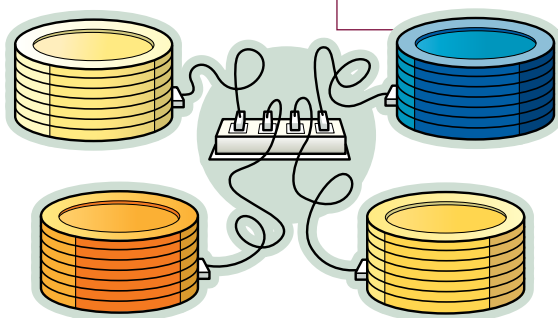
POURQUOI UTILISER UNE CRYPTOMONNAIE PLUTÔT QU'UNE DEVISE NATIONALE ?

Imaginez que vous déteniez un billet de 100 euros qui ne permette d'acheter que pour 50 euros de marchandise. Au Venezuela, où la monnaie officielle est en train de s'effondrer, ce scénario est une réalité. Chaque année, le revenu net d'un habitant y perd à peu près la moitié de sa valeur à cause de l'hyperinflation. Pour y remédier, certains achètent des bitcoins.

Comment en vient-on à préférer une cryptomonnaie difficile à comprendre, et dont la valeur n'est garantie par aucun État, à une matière première comme l'or, dont la valeur est reconnue depuis toujours ? D'abord, convertir des bolivars vénézuéliens en bitcoins est facile : quiconque a accès à Internet peut le faire. Ensuite, le bitcoin n'étant pas un objet matériel, il n'est pas besoin de le cacher dans un lieu peu sûr (comme un matelas ou, dans le cas du Venezuela, une banque). Et tandis que le bolivar a chuté brutalement, le cours du bitcoin a pour le moment une tendance moyenne à la hausse. Dans un pays où l'on attend une inflation dépassant 2 300 % en 2018 (d'après le Fonds monétaire international), la prise de risque paraît raisonnable.

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).