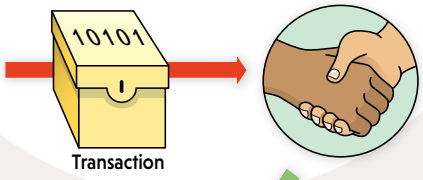
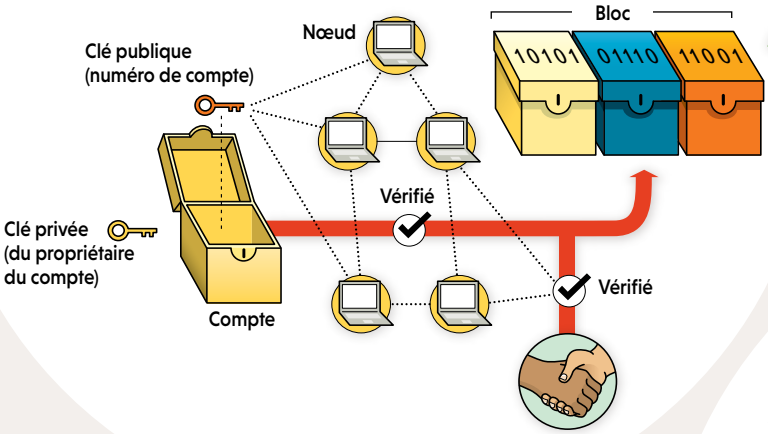
## LE PRINCIPE D'UNE BLOCKCHAIN

**Comment une monnaie numérique (ou une donnée de n'importe quelle autre nature) peut-elle s'échanger dans un réseau décentralisé constitué de nombreux inconnus qui n'ont aucune raison *a priori* de se faire confiance ? En créant un registre permanent de transactions qui ne peut être modifié par aucun membre du réseau.** ***(Pour la définition de certains termes, voir le glossaire page suivante.)***

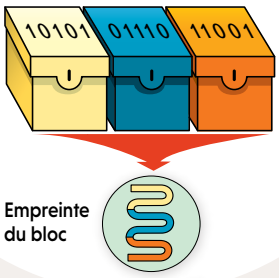
**1** Une transaction à blockchain est lancée quand une partie envoie des données à une autre. Ces données peuvent être de toute nature : unités de monnaie (comme dans le cas du bitcoin) ou d'un autre instrument financier, contrats, actes notariés, titres de propriété, informations médicales, etc. L'objectif de la blockchain est de créer une trace permanente, vérifiable et infalsifiable de l'échange qui a eu lieu.



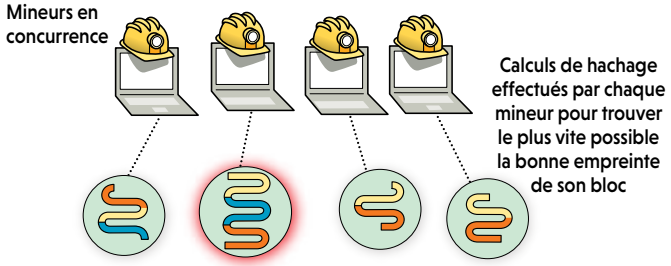

**2** La transaction est diffusée pour vérification dans le réseau pair à pair d'ordinateurs qui gère la blockchain. Chaque nœud du réseau est équipé d'une procédure de vérification de la validité de la transaction (dans une transaction de bitcoins, par exemple, le réseau vérifie si ceux qui paient sont bien en possession du montant de bitcoins qu'ils prétendent détenir). Une fois la transaction vérifiée, elle est mise en attente. Elle est alors prête pour être associée à d'autres dans un bloc qui sera ajouté à la blockchain.



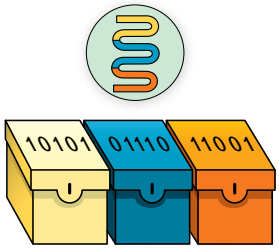

**3** Chaque « mineur » du réseau choisit des transactions en attente pour composer un bloc qu'il cherche à ajouter à la chaîne des blocs précédents. Pour obtenir le droit d'ajouter ce bloc, il doit calculer, par une opération mathématique nommée hachage, une « empreinte » du bloc qui prend en compte l'empreinte des blocs précédents et qui vérifie une certaine propriété.




**4** Les différents mineurs (faisant partie des nœuds du réseau) sont en concurrence pour gagner le droit d'ajouter à la chaîne de blocs le bloc choisi par chacun. Leurs ordinateurs effectuent de fastidieux calculs de hachage afin de produire une solution (l'empreinte du bloc) satisfaisant la propriété imposée (dans la blockchain du bitcoin, les mineurs cherchent des solutions, ou « valeurs de hachage », qui commencent par un nombre déterminé de zéros). Le mineur qui arrive le premier au bout de ce processus de « preuve de travail » en trouvant l'empreinte appropriée de son bloc « mine » celui-ci : il ajoute le bloc à la blockchain et gagne une récompense financière (de nouveaux bitcoins par exemple).




Le minage par preuve de travail étant très énergivore, certaines blockchains sont conçues de façon à fonctionner autrement. L'une des méthodes consiste à désigner au préalable des nœuds « validateurs », les seuls autorisés à enregistrer les transactions dans la blockchain.




**5** Le bloc validé est ajouté à la chaîne de blocs avec son empreinte numérique, qui code aussi mathématiquement les empreintes validées de tous les blocs précédents. Ces empreintes gigognes sécurisent de façon croissante la blockchain à chaque bloc qui s'ajoute. En effet, l'altération de ne serait-ce qu'un seul bit d'information à un endroit quelconque de la chaîne modifierait non seulement l'empreinte de ce bloc particulier, mais aussi celle de tous les blocs ultérieurs de la chaîne.

## 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.

**NŒUD**
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.