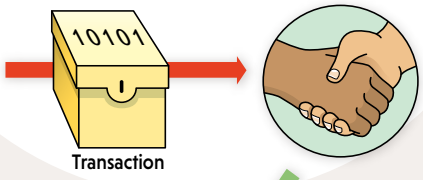
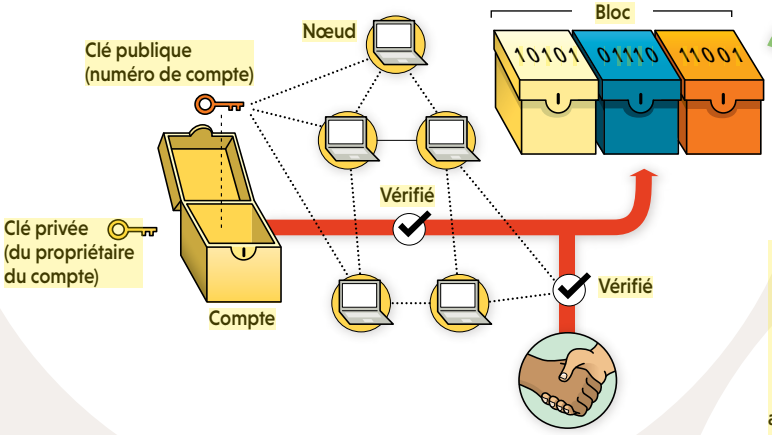
LE PRINCIPE D'UNE BLOCKCHAIN

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.)***

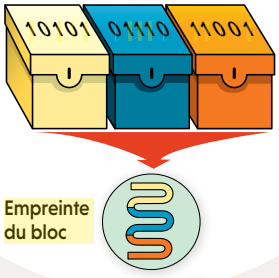
1 Une transaction à blockchain est lancée quand une partie envoie des données à une autre. Ces données peuvent être de toute nature : unités de monnaie (comme dans le cas du bitcoin) ou d'un autre instrument financier, contrats, actes notariés, titres de propriété, informations médicales, etc. L'objectif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



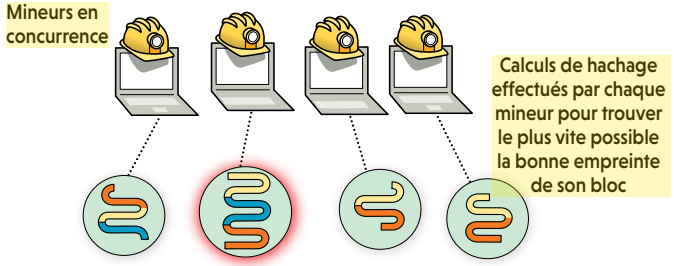
2 La transaction est diffusée pour vérification dans le réseau pair à pair d'ordinateurs qui gère la blockchain. Chaque nœud du réseau est équipé d'une procédure de vérification de la validité de la transaction (dans une transaction de bitcoins, par exemple, le réseau vérifie si ceux qui paient sont 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.



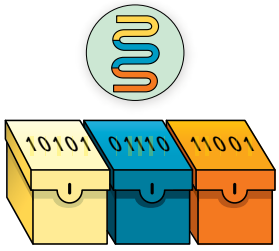
3 Chaque « mineur » du réseau choisit des transactions en attente pour composer un bloc qu'il cherche à ajouter à la chaîne des blocs précédents. Pour obtenir le droit d'ajouter ce bloc, il doit calculer, par une opération mathématique nommée hachage, une « empreinte » du bloc qui prend en compte l'empreinte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