

# Blockchain

## L'essentiel en bref

Une blockchain est une base de données numérique publique dont les données sont classées chronologiquement et gérées dans une infrastructure décentralisée. Pour ce faire, les différents blocs de données d'une chaîne en croissance continue sont ordonnés. Ce principe explique le nom de « blockchain ».

Grâce à des mécanismes cryptographiques, les données enregistrées peuvent être vérifiées par tous, mais ne peuvent plus être modifiées.

## Technologie de la chaîne blocs

### Origine

Dès les années 1990, on a tenté, sur la base de connaissances cryptographiques, de trouver un nouveau type de technologie pour un moyen de paiement numérique permettant d'effectuer des transactions en toute sécurité sans avoir à révéler sa propre identité. En 2008, un document a été publié sous le pseudonyme de Satoshi Nakamoto, présentant un algorithme qui devait permettre une version purement *peer-to-peer* de l'argent électronique. C'était la naissance du bitcoin.

En raison de la blockchain, dans un système *peer-to-peer*, aucun intermédiaire n'est nécessaire pour garantir la confiance. Dans l'environnement financier, c'est le système bancaire qui joue ce rôle. Cela permet d'effectuer des transactions directement entre des portefeuilles numériques (qui appartiennent à des personnes différentes). Chaque portefeuille possède une adresse publique et une clé privée. Les transactions peuvent ainsi être effectuées directement entre les portefeuilles et la blockchain tient le rôle de banque. La confiance est ainsi établie par la cryptographie et la technologie. Il existe des chaînes de blocs qui valident les transactions à l'aide d'une puissance de calcul (*Proof of Work*) ou qui les sécurisent via des propriétaires existants (*Proof of Stake*).

### Possibilités d'utilisation

L'avantage de la blockchain réside dans le fait que les données sont enregistrées immédiatement et stockées sur l'ensemble du réseau. Elles sont donc protégées contre les manipulations. En outre, chaque transaction ou modification peut être retracée. Ces caractéristiques permettent une multitude d'applications différentes.

Les cryptomonnaies sont le domaine d'application le plus connu de la technologie blockchain. En principe, tous les éléments réels peuvent être représentés numériquement. Par exemple, les contrats peuvent être exécutés via une blockchain ou les identités peuvent être représentées numériquement et utilisées pour la vérification. La technologie a également un grand potentiel dans la gestion de la chaîne d'approvisionnement, notamment, pour le suivi des chaînes d'approvisionnement. C'est ce que l'on appelle la technologie *Distributed Ledger Technology, DLT*.

## Crypto-monnaies

Une crypto-monnaie est une monnaie « numérique » fondée sur un système de chaîne de blocs. Contrairement au franc suisse ou à l'euro, il n'y a pas d'autorité centrale qui surveille la valeur d'une crypto-monnaie. En outre, aucune banque n'existe dans ce système qui vérifie les transactions. Ces tâches sont réparties dans le système entre plusieurs utilisateurs.

### Exemples :

#### BITCOIN (BTC) :

Le bitcoin est la crypto-monnaie créée en 2008 et la plus échangée. La monnaie a été créée par Satoshi Nakamoto, dont on pense largement qu'il s'agit du pseudonyme d'une personne ou d'un groupe de personnes dont l'identité exacte reste inconnue.

#### ETHEREUM (ETH) :

Développé en 2015, Ethereum est une plateforme de blockchain avec sa propre crypto-monnaie, appelée Ether (ETH) ou Ethereum. Après le bitcoin, il s'agit de la crypto-monnaie la plus échangée.

#### LITECOIN (LTC) :

Cette monnaie est la plus proche du bitcoin, mais elle a évolué plus rapidement et offre des paiements et des processus plus rapides permettant de réaliser davantage de transactions.

#### RIPPLE (XRP) :

Ripple est un système de *ledger* (livre de compte) distribué créé en 2012. Ripple permet de suivre différents types de transactions, et pas seulement les transactions en devises.

Les crypto-monnaies qui ne sont pas des bitcoins sont appelées « *altcoins* » pour les distinguer de l'original. Il existe aujourd'hui plus de 18 000 cryptomonnaies différentes.

### Où peut-on acheter des cryptomonnaies ?

Tu peux acheter des crypto-monnaies via des bourses numériques sur lesquelles les crypto-monnaies sont négociées. Elles fonctionnent en principe de la même manière que les bourses normales où sont négociées les actions. Les coins peuvent toutefois avoir des prix différents sur différentes bourses. Il convient donc de bien s'informer au préalable pour savoir sur quelle bourse les coins peuvent être achetés au meilleur prix. Coinbase, <https://www.coinbase.com/>, est actuellement la plus grande bourse de crypto-monnaies au monde. Il en existe beaucoup d'autres, par exemple, Bitcoin Suisse, <https://www.bitcoinsuisse.com/>, un fournisseur suisse.

### Où aller avec les coins achetés ?

Si tu achètes des crypto-monnaies sur une bourse, ton avoir est d'abord géré par la bourse. Imagine que c'est comme une banque de dépôt qui détient les titres achetés. Ce dépôt est appelé « *wallet* » (portefeuille). Les coins peuvent être transférés du portefeuille de la bourse vers un « portefeuille » personnel. Il existe différentes possibilités de conserver les coins. Les « *hardware wallets* » (portefeuilles électroniques), qui stockent la clé privée et sécurisent ainsi l'accès, sont une approche très appréciée. Le risque d'un « *hardware wallet* » est de le perdre ou de se le faire voler.