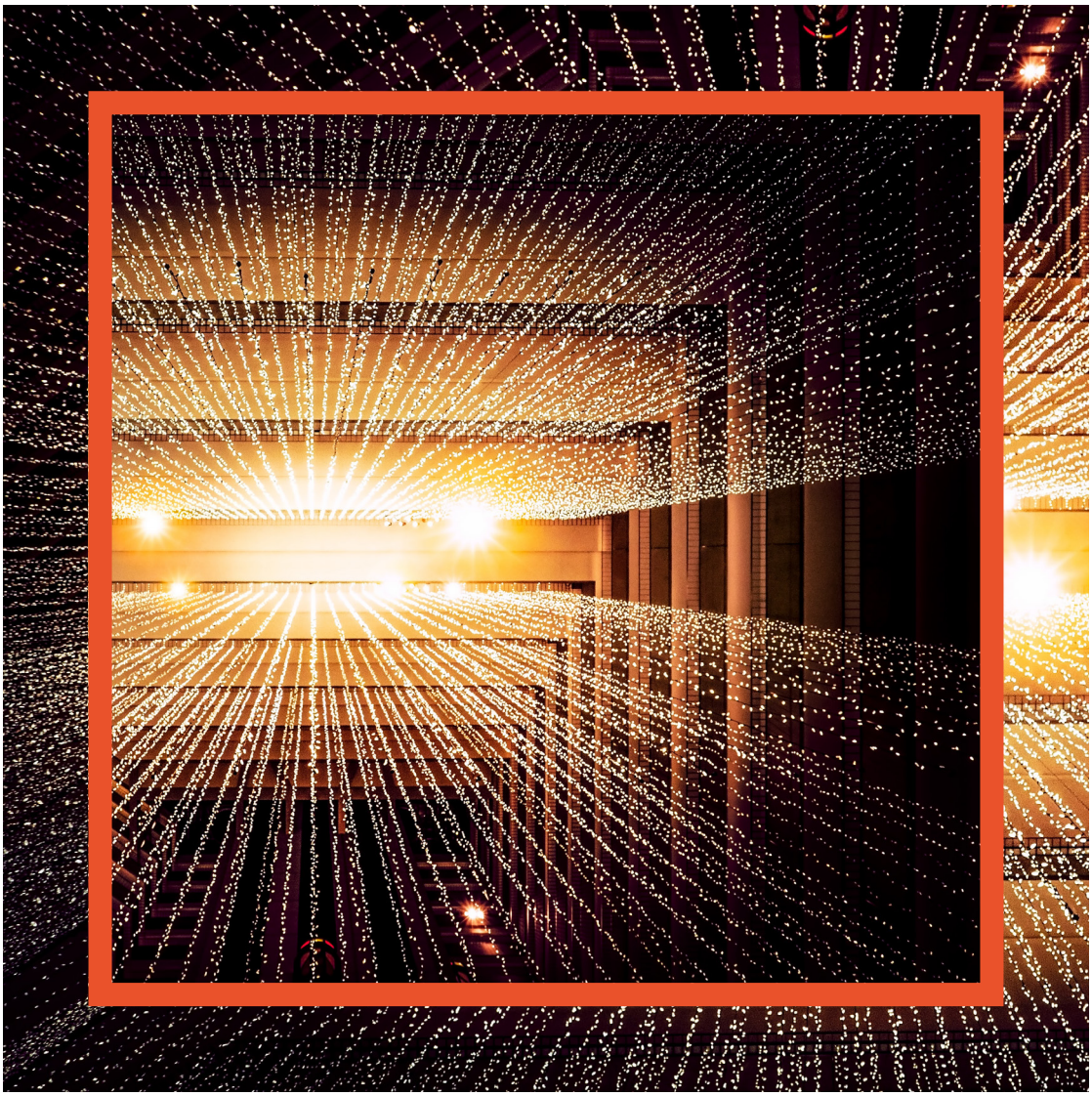
CRYPTO-MONNAIES:
du Bitcoin à l'Ether



Swissquote

Sommaire

Bitcoin (XBT) 4

Ethereum (ETH) 19

Litecoin (LTC) 22

Ripple (XRP) 24

Bitcoin Cash (BCH) 26

Étapes suivantes: commencez à trader avec Swissquote 28

BITCOIN (XBT)

La première crypto-monnaie

Le Bitcoin est la toute première monnaie numérique jamais créée. Il a été inventé en 2009, un mois après la chute de Lehman Brothers, par le programmeur japonais Satoshi Nakamoto. On peut le représenter avec deux symboles: XBT et BTC.

Son ambition première était de construire un système de paiement électronique anonyme, transparent, décentralisé et simple à mettre en place.

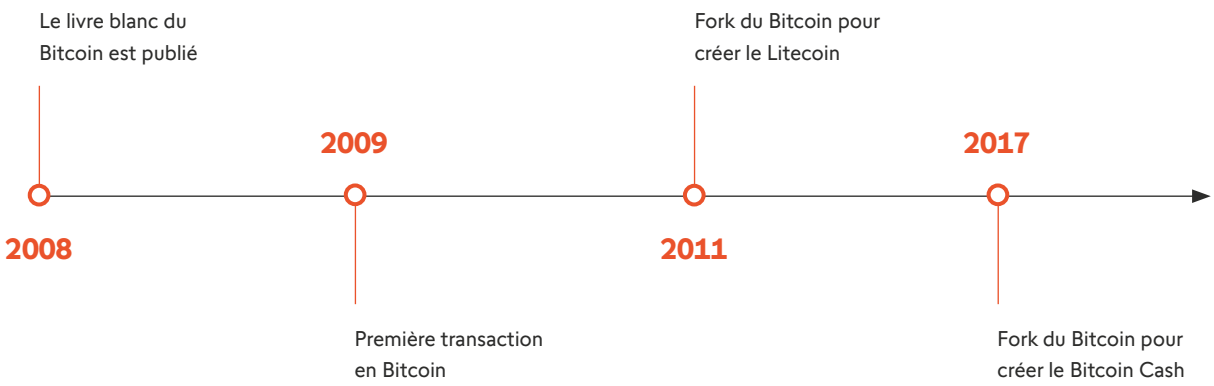
CHIFFRES CLÉS (AU 25 MARS 2020)

Crypto	Rang	Cap. boursière	Cours actuel
XBT	1er	EUR 113 md	EUR 6'148

Graphique du cours

Source: CoinMarketCap

Généralités



CRYPTO-MONNAIE: Le Bitcoin est une monnaie originale qui désigne une représentation numérique d'une valeur financière susceptible d'être transférée. Il s'appuie sur des calculs puissants et un chiffrement mathématique pour sécuriser les informations et les transactions.

DÉCENTRALISÉ: Le Bitcoin est décentralisé, ce qui implique qu'il n'a pas besoin d'administrateur central ou d'intermédiaires. Des unités ou des fractions de Bitcoin peuvent être envoyées d'un utilisateur à un autre sur le réseau blockchain du Bitcoin.

TECHNOLOGIE: La blockchain est une chaîne de blocs reliés entre eux et répartis entre les utilisateurs afin de fonctionner comme un registre de données immuable.

OFFRE LIMITÉE: Comme de nombreuses autres crypto-monnaies, le Bitcoin se caractérise par une offre limitée. Dans la pratique, cela signifie que plus aucun Bitcoin ne pourra être créé lorsque le maximum de 21 millions d'unités aura été atteint.

OPEN SOURCE: Le protocole du Bitcoin est open source. Tout le monde peut donc accéder au code pour l'examiner et contribuer à son développement.

Autres applications de la blockchain

ORGANISATIONS CARITATIVES
Optimisation de la transparence de l'utilisation des fonds reçus.

SANTÉ
Amélioration de la sécurité des dossiers médicaux numériques et du suivi de l'approvisionnement en médicaments.

La blockchain

La blockchain, qu'est-ce que c'est?

La blockchain est la technologie à l'origine du Bitcoin et de bien d'autres crypto-monnaies.

Une blockchain est une base de données qui fonctionne comme un registre numérique décentralisé. Les données sont organisées en blocs, qui sont crytpographiquement reliés les uns aux autres.

Ses principaux avantages sont la disponibilité permanente grâce à l'absence d'une source d'erreur unique et la stabilité, étant donné qu'une fois enregistrées dans la blockchain, les données ne peuvent plus être modifiées. La technologie de la blockchain supprime également la dépendance vis-à-vis des intermédiaires et la nécessité de faire confiance à une organisation unique.

Qu'est-ce qui rend la blockchain si sûre?

Dans le cas du Bitcoin et de nombreuses autres monnaies virtuelles, la technologie de la blockchain garantit qu'aucun Bitcoin n'est jamais détruit ou dupliqué. Ce sont deux propriétés de la blockchain qui permettent cela:

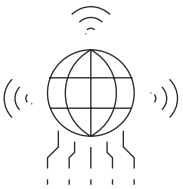
L'immuabilité

- Une fois que la validité d'une transaction ou de l'enregistrement de tout type de donnée est confirmée, **il n'est plus possible de les modifier et leur intégrité est garantie.**

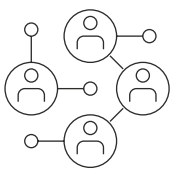
Le consensus

- **La capacité à garantir un état unique du réseau blockchain,** et donc la validité de chaque transaction qui y est enregistrée.

Altre applicazioni della blockchain



INTERNET DES OBJETS
La blockchain permet de sécuriser les capacités de collecte de données offertes par l'IoT.



CHAÎNE D'APPROVISIONNEMENT
Amélioration de la gestion de la distribution des produits et transparence des paiements.

Comment fonctionne la blockchain du Bitcoin?

Comme expliqué précédemment, une fois qu'une transaction en Bitcoin est validée, elle ne peut plus être modifiée ou supprimée de la blockchain. En effet, les données y sont ajoutées sous forme de blocs, qui sont enchaînés les uns aux autres.

La chaîne de blocs et les transactions peuvent être auditées, puisqu'elles sont visibles de tous. On peut décrire la blockchain comme un répertoire où toute nouvelle entrée est reliée à la précédente. Par exemple, si l'on cherche le bloc classé 452e, il sera possible de vérifier qu'il arrive après le bloc classé 451e. En outre, le dernier bloc en date serait lui-même différent si le tout premier bloc (le «bloc de genèse») était différent lui aussi.

Comment les blocs d'une blockchain sont-ils reliés entre eux?

En un mot, le chiffrement mathématique qui alimente la blockchain du Bitcoin permet à chaque bloc de générer un identificateur unique à partir des données qu'il contient. Cet identificateur est ensuite transmis au bloc suivant, ce qui crée un lien permanent entre les deux et empêche, par nature, toute tentative de modification ultérieure des transactions précédentes.

QU'EST-CE QUE LE HACHAGE?

Le hachage désigne l'opération par laquelle des données entrantes de tailles différentes génèrent des données sortantes de taille constante. Les algorithmes de hachage génèrent en outre toujours le même résultat à partir des mêmes données entrantes.

ANALOGIE DE BLOCKCHAIN

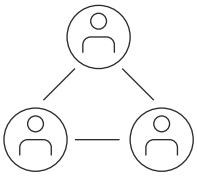
Rang du bloc	Bloc		Analogie de hachage
1	hsgAO	→	EM
2	IzoEM	→	OF
3	pmzOF	→	LN

Comment les blocs d'une blockchain sont-ils créés?

La production de nouveaux blocs est le résultat direct d'un processus appelé «minage». Comme expliqué précédemment, les blocs sont reliés entre eux grâce à la cryptographie. La production de nouveaux blocs impose aux participants du réseau de s'engager à mettre à profit leur puissance de calcul pour permettre le chiffrement mathématique des données de transaction.

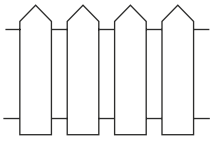
Les mineurs sont donc responsables de la vérification de toutes les transactions. Par ailleurs, en récompense de leur activité de minage, ils reçoivent les Bitcoins nouvellement créés, qui sont donc injectés dans le réseau.

Que permet la blockchain du Bitcoin?



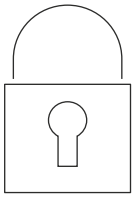
ÉLIMINER LES CONTREPARTIES

Tous les paiements en Bitcoin sont réalisés sans l'intervention d'aucune contrepartie, ce qui permet de réduire les frais de transaction et de limiter les risques généralement liés à la participation d'intermédiaires.



FAIBLES BARRIÈRES À L'ENTRÉE

La blockchain ne nécessite aucune autorisation, ce qui signifie qu'il n'y a pas à demander de permission pour participer et contribuer au réseau blockchain. Ainsi, un utilisateur a simplement besoin d'une connexion à Internet pour pouvoir effectivement réaliser des transactions en Bitcoins.

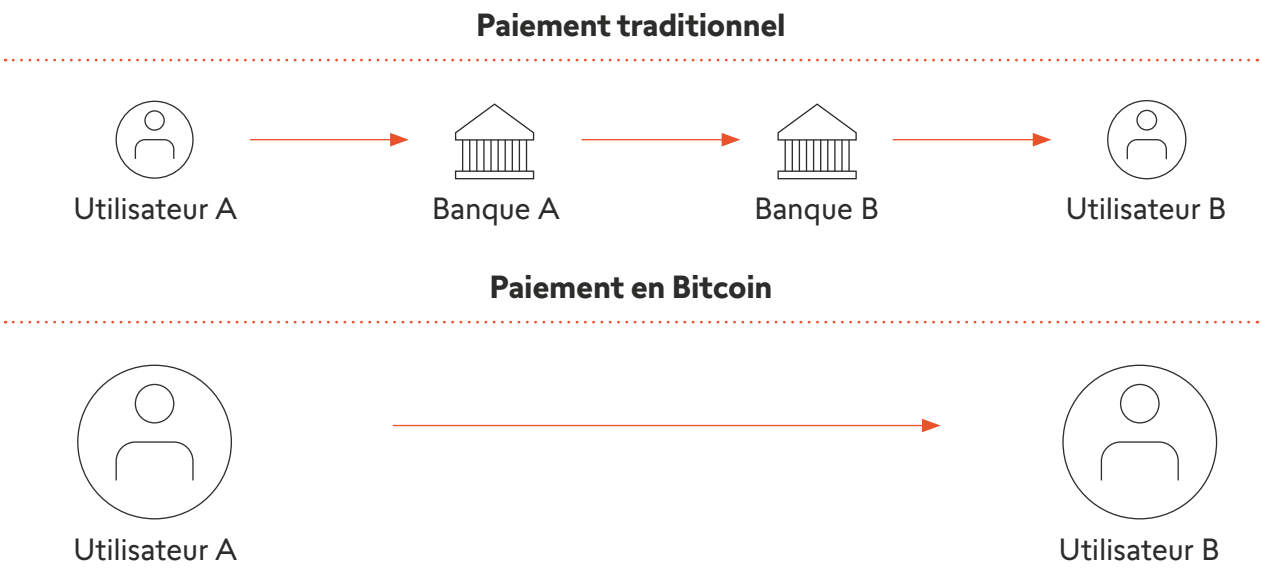


SÉCURITÉ RENFORCÉE

Comme elle est décentralisée, une blockchain ne s'appuie sur aucun serveur central exposé à une action malveillante. La blockchain fonctionne grâce à un réseau de nœuds dispersés et un pirate devrait cibler simultanément un grand nombre de nœuds pour compromettre le réseau.

Paiements en Bitcoin

Comparaison avec les méthodes de paiement traditionnelles



Quelles sont les options de stockage sans surveillance du Bitcoin?

Étant donnée l'absence de tiers, on se pose souvent la question des différentes possibilités en matière de stockage sans surveillance (dit «non-custodial») des Bitcoins. Il existe deux options principales: le portefeuille chaud et le portefeuille froid.

Un portefeuille chaud est un logiciel en ligne qui permet à ses utilisateurs de stocker et d'envoyer/recevoir simplement des Bitcoins. Les comptes des détenteurs de crypto-monnaie peuvent être considérés comme un type de portefeuille chaud.

De son côté, le portefeuille froid est un stockage hors ligne, le plus souvent sur un support physique, qui offre un niveau de sécurité plus élevé. Ledger est sans nul doute le fournisseur de portefeuille froid le plus connu. Trezor, KeepKey et CoolWallet S figurent parmi les autres options.

Nœuds Bitcoin

Que sont les nœuds Bitcoin?

Les nœuds Bitcoin peuvent être définis comme des types de programmes spécifiques qui interagissent avec la blockchain du Bitcoin. Comme ils communiquent constamment les uns avec les autres, ces nœuds sont ce qui permet au Bitcoin de fonctionner comme une crypto-monnaie totalement décentralisée. Ils garantissent en effet que toutes les règles sont respectées.

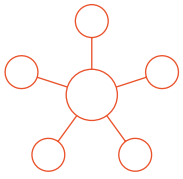
Les nœuds complets, les nœuds légers et les nœuds de minage sont les trois principaux types de nœuds du réseau Bitcoin.

NŒUDS COMPLETS

Ces nœuds sont à la base des caractéristiques de décentralisation du Bitcoin. Les nœuds complets téléchargent et vérifient les transactions et les blocs qui les comprennent.

NŒUDS LÉGERS

Les capacités des nœuds légers sont moins élevées que celles des nœuds complets, mais ils réclament également moins de ressources. Ils permettent aux utilisateurs de localiser leur transaction dans un bloc spécifique.



NŒUDS DE MINAGE

Les nœuds de minage peuvent être décrits comme des nœuds complets ayant la capacité supplémentaire de miner et donc de produire des blocs. Ces nœuds valident les transactions avant de les relayer vers d'autres nœuds.

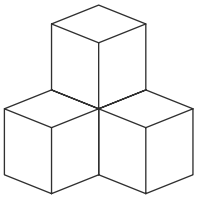
Bitcoin Halving

De quoi s'agit-il?

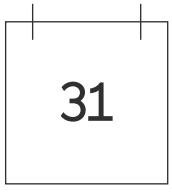
Le Bitcoin halving signifie que la prime que reçoivent habituellement les mineurs pour la vérification des transactions en Bitcoins est divisée par deux. Cet événement se produit chaque fois que 210'000 Bitcoins supplémentaires sont minés, soit généralement tous les quatre ans.

		Prime de minage par bloc
Janvier 2009	Lancement du Bitcoin	après le halving
Novembre 2012	1er Bitcoin halving	25 BTC
Juillet 2016	2e Bitcoin halving	12.5 BTC
Mai 2020	3e Bitcoin halving	6.25 BTC
2024	4e Bitcoin halving	3.125 BTC
2028	5e Bitcoin halving	1.5625 BTC

Se produit environ tous les 4 ans



Un événement majeur qui régule l'approvisionnement en Bitcoins



Le prochain halving aura lieu aux alentours du 18 mai 2020

Pourquoi les Bitcoin halvings ont-ils lieu?

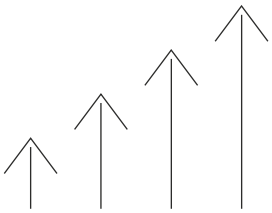
Le halving est intégré au logiciel de la blockchain et il a des implications directes pour les mineurs. Les mineurs jouent un rôle fondamental, car leur activité permet de vérifier chaque transaction en Bitcoin.

Les transactions sont vérifiées par bloc. Dès qu'un bloc de transactions est vérifié, un mineur reçoit une prime qui consiste en un certain nombre de nouveaux Bitcoins. Aujourd'hui, et jusqu'au prochain halving, un mineur reçoit 12,5 BTC par bloc vérifié. Après le prochain halving, cette prime sera divisée par deux.

Les Bitcoin halvings continueront jusqu'à ce que le nombre maximum de 21 millions de Bitcoins soit atteint, ce qui devrait se produire autour de l'année 2140. Après cela, les mineurs continueront à percevoir des commissions de transaction afin de les inciter à poursuivre a vérification des transactions en Bitcoins.

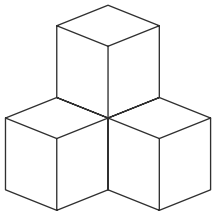
Halvings et évolution du cours du Bitcoin

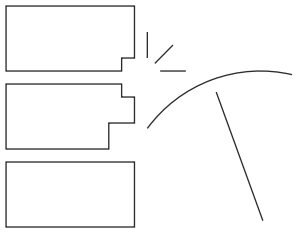
Quelles sont les conséquences des Bitcoin halvings?



On a observé par le passé que le cours du Bitcoin commençait à augmenter un mois avant le halving et que cette hausse se poursuivait après l'événement. À ce jour, les cours du Bitcoin ne sont jamais descendus en deçà de la valeur qu'ils affichaient avant le halving précédent. Cela s'explique par de nombreux facteurs, comme l'attention accrue portée au Bitcoin et la réduction automatique de l'offre de nouveaux Bitcoins.

Le halving est une réduction planifiée prédéfinie et immuable des Bitcoins créés, qui se produit environ tous les quatre ans jusqu'à ce que le nombre maximum d'unités de Bitcoin soit miné. C'est de cette façon que l'inflation du Bitcoin est contrôlée.





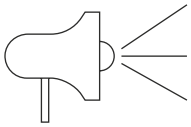
On peut prévoir qu'un certain nombre de mineurs stopperont leur activité en raison de la baisse de 50 % de la prime par bloc, puisqu'elle ne compensera plus leurs coûts de calcul et d'électricité. Cependant, cela ne devrait pas avoir d'effet sur la rapidité des vérifications des transactions, étant donné que le niveau de difficulté pour vérifier les transactions est ajusté de façon fluide par le logiciel.

Transactions en Bitcoins

Dans la pratique, comment fonctionne une transaction en Bitcoins?

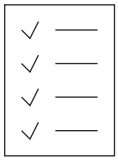
Exemple: Vanessa souhaite envoyer 10 BTC à Chad

1



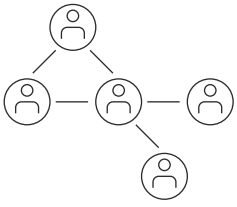
Vanessa informe le réseau de mineurs qu'elle souhaite envoyer 10 BTC à Chad. Elle leur fournit l'adresse de Bob et sa signature personnelle ainsi que sa clé publique pour permettre aux mineurs de confirmer son identité.

2



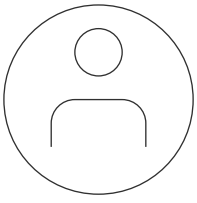
Les mineurs vérifient que la transaction sera rentable pour eux. Ils s'assurent ensuite que les 10 BTC appartiennent à Vanessa et que la transaction est valide, avant de l'ajouter à un bloc.

3



Le mineur relaie l'information à l'ensemble du réseau de mineurs afin qu'ils puissent en vérifier la validité et l'ajouter à leur copie de la blockchain.

4



Chad reçoit les 10 BTC envoyés par Vanessa.

Vérification automatique d'identité

Pas de dépendance envers une contrepartie centrale

Traçabilité renforcée et permanente

Forks

En quoi consistent les forks du Bitcoin?

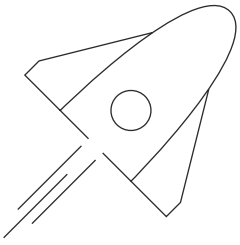
Les forks sont pour le Bitcoin ce que les mises à jour sont pour les différents logiciels que nous utilisons au quotidien. En effet, les forks du Bitcoin permettent de résoudre les différents problèmes du protocole et d'améliorer encore ses possibilités et performances.

Le protocole Bitcoin est ce qui définit les règles qui régissent le fonctionnement des crypto-monnaies. Tous les nœuds du réseau doivent le suivre (par ex., la taille des blocs). Chaque fork peut donc avoir des conséquences importantes sur le fonctionnement du Bitcoin.

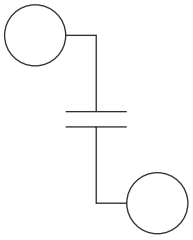
Qu'est-ce qu'un fork mou?

Il existe deux types de forks: les forks mous et les forks durs. Un fork mou du Bitcoin est essentiellement une modification du protocole Bitcoin qui reste compatible avec les précédentes versions.

Dans la pratique, cela signifie que les nœuds plus anciens (c'est-à-dire les nœuds qui existaient avant le fork et qui n'ont pas été mis à jour) restent en mesure de traiter des transactions dès lors qu'ils n'enfreignent pas les nouvelles règles établies par le fork. Notons par ailleurs que même en cas de fork mou, les nœuds anciens optent généralement pour la mise à jour car elle leur permet le plus souvent de fonctionner plus efficacement.



Plus pratiques pour les utilisateurs, car la mise à niveau n'est pas nécessaire



Moindre probabilité de scission de chaîne

Qu'est-ce qu'un fork dur?

Un fork dur est également une modification du protocole Bitcoin, mais les nœuds plus anciens qui ne sont pas mis à jour vers cette dernière version du protocole ne pourront plus du tout poursuivre leur activité.

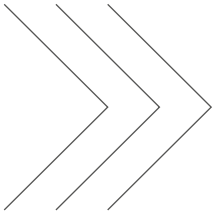
Les deux principaux types de fork dur

Forks durs planifiés

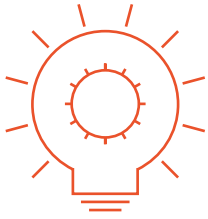
La grande majorité des nœuds appliquent la dernière version de façon volontaire, et abandonnent donc effectivement la version précédente (c'est-à-dire l'ancienne chaîne) qui ne conserve plus qu'un petit nombre de participants.

Forks durs controversés

Ils se produisent généralement lorsque la communauté ne s'accorde pas sur la mise à niveau, ce qui entraîne généralement la formation de deux blockchains séparées (ou une scission de chaîne) et donc de deux crypto-monnaies indépendantes.



Les forks durs offrent beaucoup plus de latitude, car la compatibilité avec les règles des versions précédentes n'est pas nécessaire



Le fork Bitcoin – Bitcoin Cash

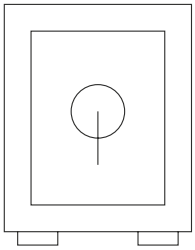
Ce fork dur est survenu en août 2017 alors que la communauté était partagée sur la façon de résoudre des problèmes d'évolutivité. Étant donné qu'un fork s'appuie toujours sur la blockchain d'origine, tous les détenteurs de Bitcoin ont reçu le même montant en unités de Bitcoin Cash au moment du fork.

Algorithmes de preuve de travail

Consensus blockchain

Comme indiqué précédemment, le consensus est l'une des deux principales caractéristiques de la blockchain. Généralement, deux types d'algorithmes permettent à une blockchain de parvenir au consensus: la preuve d'enjeu (proof of stake, PoS) et la preuve de travail (proof of work, PoW). Le Bitcoin utilise le second.

L'objectif original des algorithmes PoW était la défense contre les attaques de déni de service. Ces attaques perturbent généralement l'accès au réseau des individus en les surchargeant ou en provoquant un plantage à l'aide d'autres opérations malveillantes.



Grâce aux algorithmes de preuve de travail, pour qu'une attaque contre la blockchain du Bitcoin réussisse, elle aurait besoin de capacités de calcul phénoménales et prendrait énormément de temps. En outre, le coût élevé associé joue un rôle dissuasif important.

Comment fonctionnent les algorithmes de preuve de travail?

Pour qu'un bloc soit ajouté à la blockchain du Bitcoin, les mineurs sont en concurrence pour résoudre des problèmes mathématiques complexes (par ex., produire un hachage) grâce à leur puissance de calcul. Les mineurs diffusent ensuite leur solution aux autres nœuds (mineurs) du réseau pour qu'ils s'assurent qu'elle est correcte.

Chacun de ces blocs comporte un hachage de bloc, qui représente effectivement le travail réalisé par les mineurs, c'est-à-dire la preuve de travail. Pour qu'un acteur externe malveillant puisse pirater la blockchain du Bitcoin, il lui faudrait produire un registre plus long que l'existant (avec tous les blocs depuis le lancement), ce qui imposerait une puissance de calcul impossible à atteindre.

Résumé

La crypto-monnaie la plus populaire

Conçu en 2009, le Bitcoin est la crypto-monnaie la plus connue à ce jour. Son ambition était de créer une «monnaie liquide électronique de pair à pair pour Internet» qui serait «entièrement décentralisée, sans banque centrale et sans la nécessité de tiers de confiance pour fonctionner».

Le Bitcoin s'appuie sur la blockchain

La crypto-monnaie dépend de la blockchain, qui lui apporte de nombreuses fonctionnalités, comme l'immuabilité, la sécurité renforcée et la traçabilité.

Le Bitcoin s'améliore constamment

Comme son protocole est open source, le Bitcoin compte une importante communauté qui contribue largement à son développement.

L'avenir du Bitcoin

En raison de son nombre fini (21 millions d'unités de Bitcoin), le Bitcoin est souvent désigné comme «l'or numérique». Environ 90% des Bitcoins ont déjà été minés. Cependant, en raison des Bitcoin halvings, il faudra environ 100 années supplémentaires avant que l'intégralité des Bitcoins ait été minée. Ainsi, à cause de sa rareté et de sa difficulté à produire ainsi que de la liquidité élevée qui lui est associée, de nombreux observateurs indépendants considèrent cette crypto-monnaie comme une valeur refuge et un actif dont la valeur ne pourra que s'apprécier dans le temps.

ETHEREUM (ETH)

Trading actuel

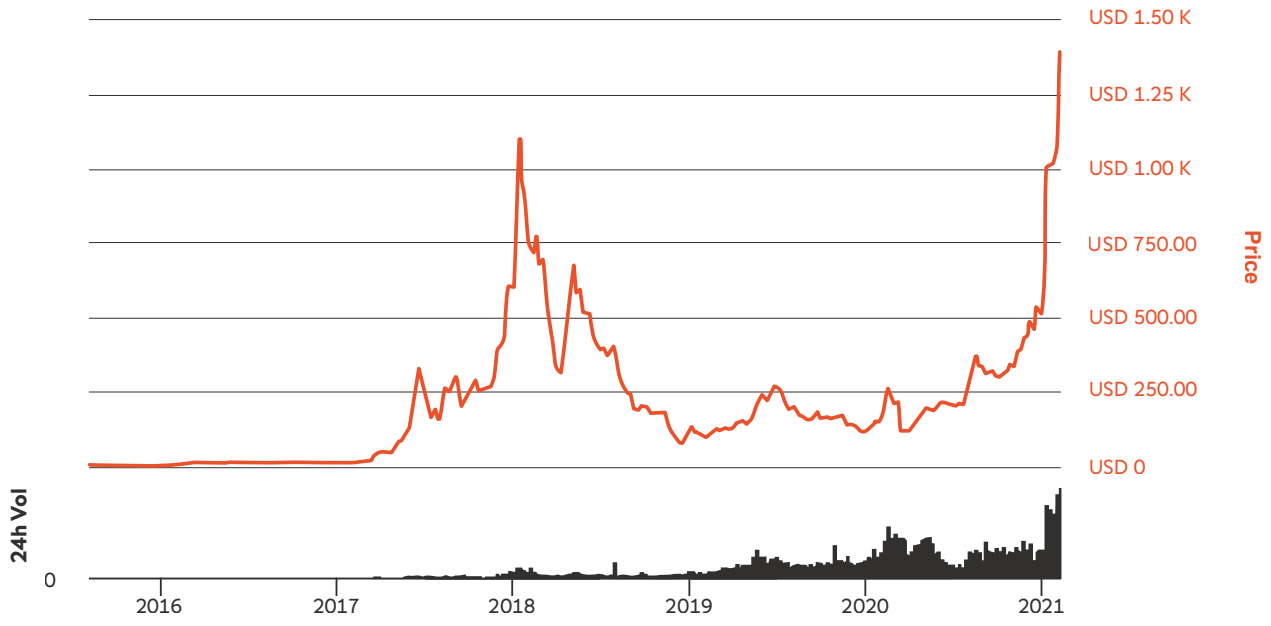
Lancé en 2015 et souvent désigné comme le «Microsoft Windows» des crypto-monnaies, Ethereum est utilisé pour la mise au point d'applications décentralisées. Sa crypto-monnaie associée, l'Ether, est la deuxième du marché par la taille.

Le créateur d'Ethereum, Vitalik Buterin, a inventé le concept des «smart contracts», qui sont des programmes exécutés sur la blockchain.

CHIFFRES CLÉS (AU 25 MARS 2020)

Crypto	Rang	Cap. boursière	Cours actuel
ETH	2e	EUR 14 md	EUR 123.16

Graphique du cours



Source: CoinMarketCap

Généralités

Ethereum, qu'est-ce que c'est?

L'Ether et le Bitcoin sont deux crypto-monnaies bien connues. La principale différence entre elles réside dans le fait qu'Ethereum permet la création de **smart contracts** et la construction d'**applications décentralisées (Dapps).**

Applications décentralisées

Alors que le Bitcoin est avant tout un système de transfert monétaire fondé sur la blockchain, l'ambition d'Ethereum est différente. Son objectif principal est de **permettre aux développeurs de construire et publier des applications décentralisées (appelées Dapps) sur sa blockchain.** Beaucoup d'autres crypto-monnaies disponibles sur Swissquote, comme Eos, Chainlink ou Tezos, offrent également la possibilité de développer et d'utiliser des Dapps.

Les smart contracts devraient également résoudre plusieurs difficultés auxquelles sont confrontés les acteurs en matière de trading de titres, de compensation et de règlement, de gestion des déclarations de sinistre d'assurance, voire de gestion des documents de la chaîne d'approvisionnement.

Ether – la crypto-monnaie

Ethereum peut être défini comme une plateforme logicielle décentralisée et l'Ether est sa crypto-monnaie associée. **Ainsi, l'Ether n'est pas seulement une crypto-monnaie négociable, il est également utilisé par les développeurs pour payer différents services fournis sur le réseau Ethereum, comme le fonctionnement ou la monétisation d'applications.**

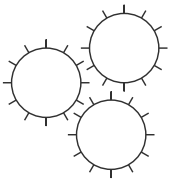
On obtient des Ethers par trading sur des bourses ou par minage. À la différence du Bitcoin, le minage de l'Ether ne nécessite pas de capacité industrielle, car il encourage le minage décentralisé par des personnes, avec des algorithmes de preuve de travail (des problèmes mathématiques complexes à résoudre pour confirmer la formation d'un bloc).

Smart contracts

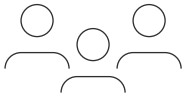
Un smart contract, qu'est-ce que c'est ?

Pour résumer, on pourrait décrire les smart contracts comme des contrats numériques qui s'exécutent automatiquement. Il s'agit plus précisément de code informatique dont l'objectif est de faciliter le transfert d'une valeur, d'un contenu ou d'un bien. **La principale caractéristique des smart contracts est qu'ils permettent ce transfert de propriété et toute autre opération à laquelle ils sont destinés, uniquement si certaines conditions prédéfinies sont remplies.** Ciò consente di intraprendere operazioni sicure tra terze parti sconosciute e una velocità di esecuzione senza pari.

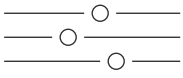
Disponible publiquement sur le registre



Exécution automatique d'opérations et de transferts spécifiques



Ne nécessite pas l'intervention d'un intermédiaire



Entièrement personnalisable

AVANTAGES

- Offre une sécurité supplémentaire par rapport aux contrats appliqués de façon traditionnelle
- Réduit les frais de transaction
- Garantit une sécurité totale, même avec des tiers inconnus

Ethereum Virtual Machine (EVM)

L'EVM est souvent citée comme l'innovation fondamentale d'Ethereum. Il s'agit d'un logiciel qui permet le développement et l'exécution d'applications alimentées par la blockchain de la façon la plus efficace possible et qui les protège de toute interférence avec d'autres programmes de la blockchain.

LITECOIN (LTC)

Trading actuel

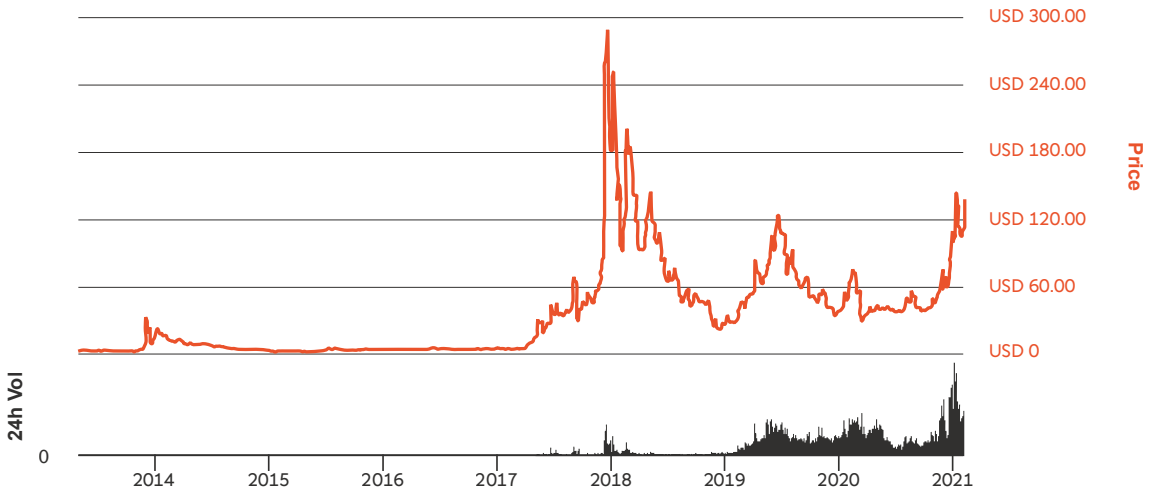
Fondé en 2011 par Charlie Lee, un ancien ingénieur de Google, le Litecoin est l'une des premières crypto-monnaies à avoir été lancées. La principale ambition à l'origine de sa création était de proposer une monnaie numérique plus adaptée à une utilisation quotidienne que le Bitcoin.

Le Litecoin repose sur le même code source ouvert que le Bitcoin. Son principal avantage est que son code permet la génération d'un bloc toutes les 2,5 minutes, contre 10 minutes pour le Bitcoin.

CHIFFRES CLÉS (AU 25 MARS 2020)

Crypto	Rang	Cap. boursière	Cours actuel
LTC	7e	EUR 2.3 md	EUR 35.78

Graphique du cours



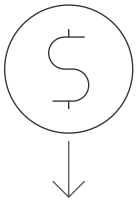
Source: CoinMarket Cap

Généralités

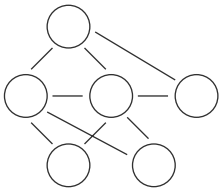
En quoi le Litecoin est-il différent du Bitcoin?

Le Litecoin est une crypto-monnaie née d'un fork du client de base du Bitcoin. Dans la pratique, cela signifie que le Litecoin s'appuie sur la base du code open source original du Bitcoin, à laquelle ses développeurs ont ajouté de nouvelles fonctionnalités. Ainsi, le Litecoin repose aussi sur la technologie de la blockchain et sur un système entièrement décentralisé. Cependant, de nouvelles fonctionnalités ont été imaginées pour servir l'ambition du Litecoin de résoudre des problèmes pour lesquels le Bitcoin n'avait pas été conçu.

Vitesse de transaction 4x plus rapide



Transactions meilleur marché



Algorithme de minage différent

Transactions rapides et au coût quasi nul

Si le Bitcoin et le Litecoin s'appuient sur l'algorithme de preuve de travail, le Litecoin utilise Skrypt, qui semble constituer une méthode de minage plus démocratique que l'algorithme SHA-256 du Bitcoin. En effet, il réclame moins de ressources de calcul que le SHA-256, car il ne génère pas d'augmentation de la difficulté de minage qui rendrait le minage uniquement accessible à ceux qui disposent d'une puissance de calcul importante. **L'algorithme Skrypt est ce qui permet au Litecoin de réduire drastiquement les frais de transaction.**

Points communs avec le Bitcoin

Tout comme le Bitcoin, l'offre de Litecoin est limitée, ce qui protège la crypto-monnaie de l'inflation et l'aide à conserver sa valeur. Les transactions en Litecoin sont vérifiées comme les transactions en Bitcoins, grâce à des mineurs qui sont récompensés pour chaque bloc de transaction confirmé. Et tout comme le Bitcoin, la prime de minage est divisée par deux après chaque halving (le prochain est attendu en 2023).

RIPPLE (XRP)

Trading actuel

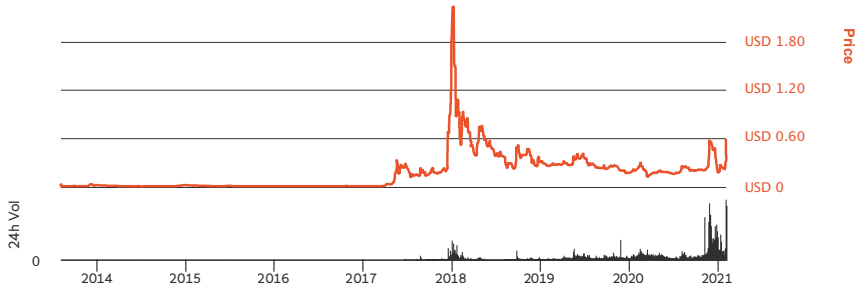
Ripple permet des transactions ultrarapides (env. 4 secondes) et s'accompagne de frais de transaction particulièrement faibles, le tout associé à un réseau évolutif. Le système de règlement centralisé en temps réel de Ripple peut gérer environ 1'500 transactions/seconde.

La principale caractéristique du XRP est le réseau qui le soutient. Il peut être comparé à une bourse qui facilite les paiements entre des banques et d'autres établissements financiers.

CHIFFRES CLÉS (AU 25 MARS 2020)

Crypto	Rang	Cap. boursière	Cours actuel
XRP	3e	EUR 7 md	EUR 0.16

Graphique du cours



Source: CoinMarketCap

Rapide historique

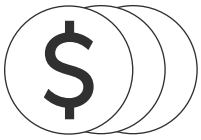
2004 — Premier prototype de Ripple comme système monétaire décentralisé (RipplePay)

2012 — Lancement d'OpenCoin, une société technologique centrée sur les solutions de paiement pour les établissements

2015 — Changement du nom de Ripple Labs (ex-OpenCoin) pour Ripple

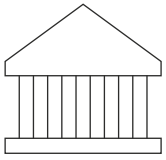
Généralités

Les principales caractéristiques de Ripple



Convertible dans toutes les monnaies

Transactions réglées en moins de 4 secondes



Conçu pour les établissements financiers

Le registre XRP

The XRP ledger (XRPL)

→ **Système distribué open source qui permet des transactions financières instantanées,** le stockage des informations comptables et des services de change.

→ **Le consensus est atteint grâce à l'algorithme de consensus exclusif de Ripple,** qui est appliqué au travers d'un réseau de nœuds de validation indépendants.

→ **Les clients de Ripple ont accès à une liste de nœuds de confiance (les UNL), qui doivent tous être d'accord sur l'état actuel du registre.** La vérification des transactions en Ripple ne dépend donc pas du minage.

Une crypto-monnaie pour les établissements financiers

Le Ripple est la première crypto-monnaie qui cible les banques et les établissements financiers. **Son ambition est de résoudre les difficultés que ces derniers rencontrent en matière de contraintes sur la liquidité par rapport aux fluctuations possibles du taux de change et de vitesse de compensation (4 secondes contre 2-3 jours pour les systèmes de paiement traditionnels), tout en offrant le niveau de sécurité associé à l'utilisation de la blockchain.**

BITCOIN CASH (BCH)

Trading actuel

Le Bitcoin Cash a été créé par le fork du Bitcoin d'août 2017. Tout comme le Bitcoin, il s'agit «d'une monnaie liquide électronique de pair à pair pour Internet. Il est entièrement décentralisé, sans banque centrale et sans la nécessité de tiers de confiance pour fonctionner.»

L'idée à l'origine de sa création était de proposer des transactions rapides, quasi instantanées et de réduire le coût de transaction élevé associé au Bitcoin. Le Bitcoin Cash peut ainsi être utilisé par des particuliers pour les petites transactions du quotidien, ce qui n'est pas le cas du Bitcoin.

CHIFFRES CLÉS (AU 25 MARS 2020)

Crypto	Classifica	Cap. boursière	Cours actuel
BCH	5e	EUR 3.8 md	EUR 204.55

Graphique du cours

Source: CoinMarketCap

Les origines du Bitcoin Cash

Le Bitcoin Cash a été créé par un fork dur du Bitcoin en 2017. La blockchain du Bitcoin Cash a été modifiée pour augmenter la taille d'un bloc de transactions. Elle est passée de 1 Mo pour le Bitcoin à 8 à 32 Mo.

Généralités

Évolutivité supérieure et frais inférieurs

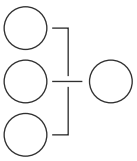
Capacité de traitement des transactions

L'objectif de la nouvelle version de la blockchain du Bitcoin Cash est d'augmenter fortement la taille des blocs pour résoudre les problèmes associés aux frais de transaction supérieurs encourus par certains utilisateurs du Bitcoin.

La blockchain du Bitcoin Cash réduit le temps nécessaire à l'intégration des transactions dans un bloc, sans qu'il soit nécessaire de motiver les mineurs en fixant des frais de transaction plus élevés. Le Bitcoin Cash semble donc plus pratique pour les micropaiements et permet au réseau d'éviter l'encombrement, même lors des périodes de forte activité.

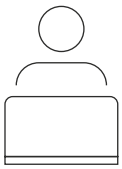
Grâce à l'augmentation de la taille des blocs, le Bitcoin Cash permet également aux mineurs de percevoir des primes plus élevées pour le minage d'un bloc, étant donné qu'il contient plus de transactions.

Caractéristiques communes avec le Bitcoin

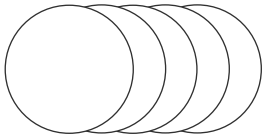


Fondé sur la blockchain

Code open source



Algorithme de preuve de travail



Approvisionnement limité (21 millions d'unités)

ÉTAPES SUIVANTES: COMMENCEZ À TRADER AVEC SWISSQUOTE

1

Allez sur **swissquote.com/trading**

2

Ouvrez un compte démo.

3

Vous pouvez vous entraîner au trading avec un compte virtuel de CHF 10'000 Sans risque ni obligation.

Essayer la démo dès maintenant!

Pourquoi trader avec Swissquote?

- 20 ans d'expertise dans le trading en ligne
- Accès à 3 millions de produits sur les grands marchés boursiers internationaux
- La plateforme de trading la plus complète du marché
- Service client multilingue
- Des webinaires pour apprendre et vous former
- Des applications mobiles hautement performantes
- Groupe international coté sur la SIX Swiss Exchange (SIX:SQN)

Swissquote est régulièrement citée et consultée par les médias financiers internationaux.

Bloomberg

CNBC

FINANZ und WIRTSCHAFT

LE TEMPS

Investing.com

Neue Zürcher Zeitung

swissquote.com/crypto-assets/education