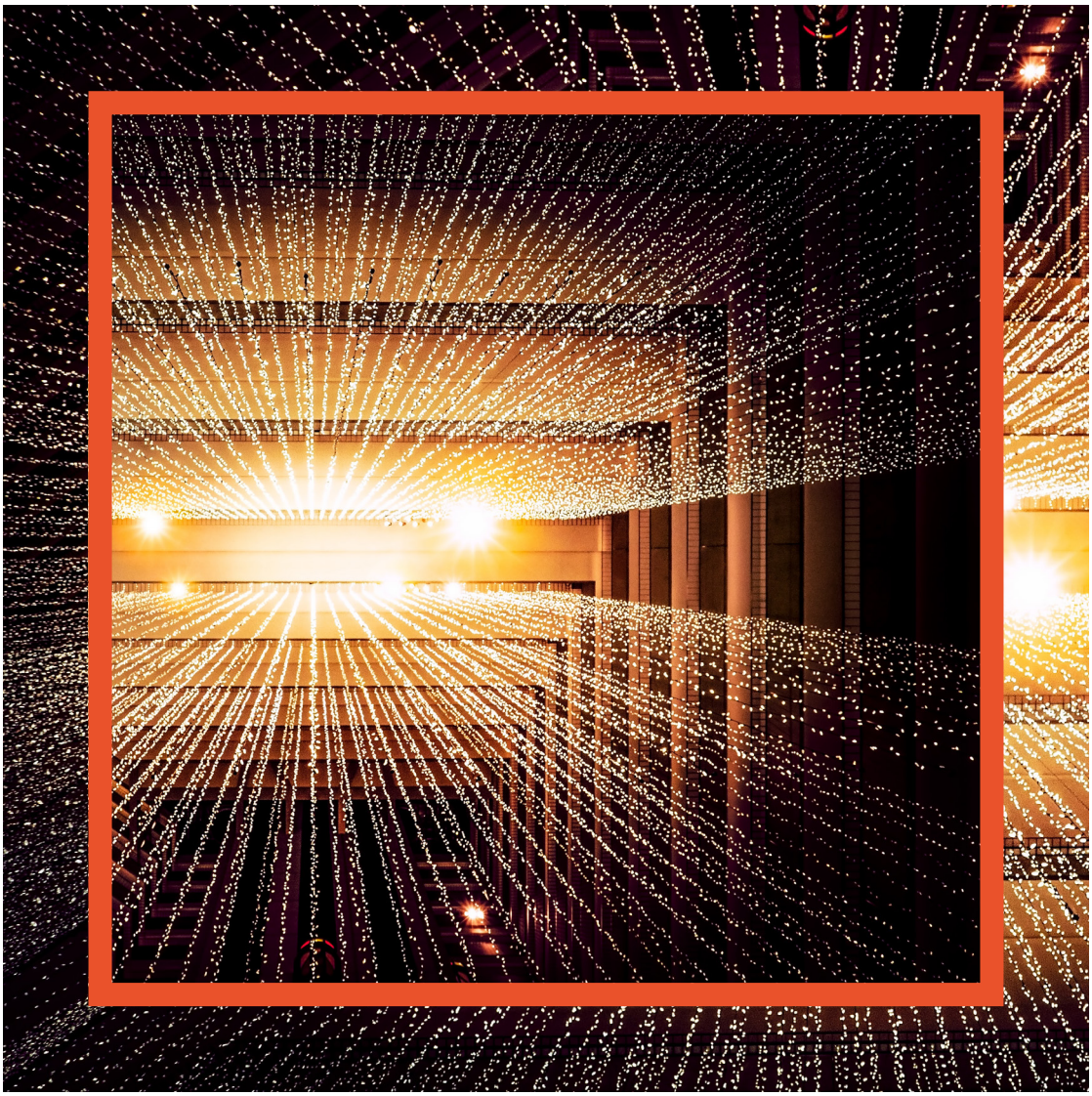
CRYPTOCURRENCIES:
from Bitcoin to Ether



Swissquote

Content

BITCOIN (XBT)

The first cryptocurrency

Bitcoin is the first digital currency ever created. It was designed in 2009 a month after the Lehman Brothers' collapse, by Japanese developer Satoshi Nakamoto. It can be represented by two symbols: XBT and BTC.

The primary ambition was to build an anonymous, transparent, decentralized and easy to set up electronic payment system.

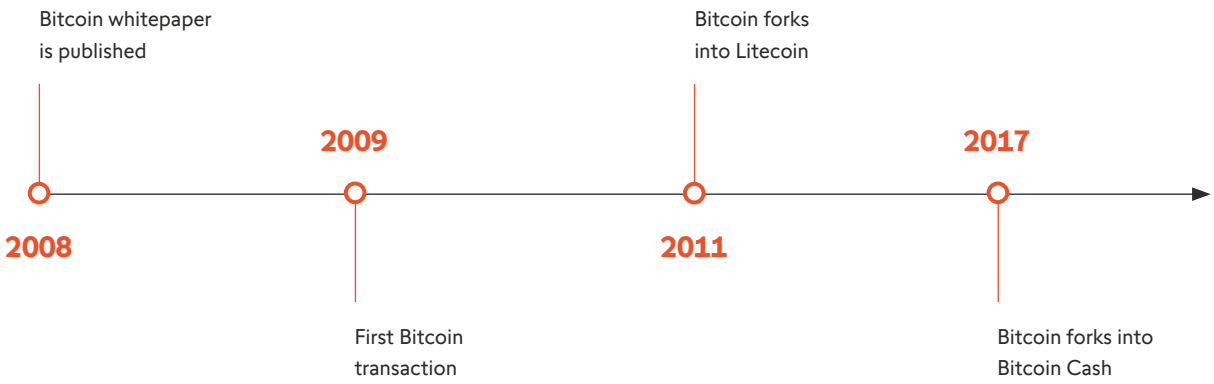
KEY FIGURES (AS OF MARCH 25TH, 2020)

Crypto	Rank	Market Cap	Current Price
XBT	#1	EUR 113Bn	EUR 6'148

Price chart

Source: CoinMarketCap

General aspects



CRYPTOCURRENCY: Bitcoin is a native coin referring to a digital representation of a financial value that can be transferred. It relies on powerful computation and mathematical encryption in order to secure information and transactions.

DECENTRALIZED: Bitcoin is decentralized, implying that it does not require any central administrator or middlemen. Bitcoin units or fractions of it can be sent from user to user on the Bitcoin blockchain network.

TECHNOLOGY: Blockchain is a chain of blocks that are linked together and distributed among users, in order to act as an immutable ledger of data.

LIMITED SUPPLY: Just like many cryptocurrencies, Bitcoin is characterized by limited supply. In practice, this means that no more Bitcoin will be generated once the maximum supply of 21 million units is reached.

OPEN SOURCE: The Bitcoin protocol is open source, and everyone can access, review and contribute to the development of the code.

Other applications of blockchain

CHARITY
Optimization of the transparency of the use of received funds.

HEALTHCARE
Enhancement of the security of digital health records and of the tracking of drug supply.

The blockchain

What is the blockchain?

Blockchain is the underlying technology supporting Bitcoin and many other cryptocurrencies.

A blockchain is a database that operates as a decentralized digital ledger. The data records are organized into blocks, which are cryptographically associated to one another.

The main advantages are its permanent availability due to the absence of a single point of failure, and its stability as data cannot be altered once it has been registered on the blockchain. Blockchain technology also eliminates the dependency on intermediaries and the need to trust a single organization.

What makes blockchain secure?

In the case of bitcoin and many other virtual currencies, blockchain technology guarantees that no bitcoin is destroyed nor duplicated. This is made possible thanks to two main blockchain properties:

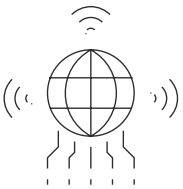
Immutability

- Once a transaction or the record of any type of data has been confirmed to be valid, **it cannot be altered anymore and its integrity is guaranteed.**

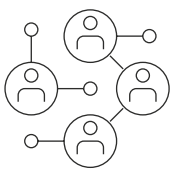
Consensus

- **Capability to ensure a one-and-only true state of the blockchain network**, and thereby the validity of every transaction recorded on it.

Other applications of blockchain



INTERNET OF THINGS
Blockchain allows for the securing of the data collection capabilities offered by IoT.



SUPPLY CHAIN
Improvement of the management of products' distribution and transparency of payments.

How does Bitcoin blockchain work?

As previously said, once a Bitcoin transaction is validated, it cannot be modified or deleted from the blockchain. Indeed, data is added by blocks. that are chained to one another.
The chain of blocks and transactions are auditable, as they can be seen by everyone. Blockchain can be described as a directory where each new entry is linked to the last one. For instance, if we look at the block ranked 452nd, we will be able to verify that it came after the block ranked 451st. Moreover, even the latest block to date would be different if the first block ever created (»the genesis block») was different too.

How do Blockchain blocks link together?

Simply put, the mathematical encryption powering Bitcoin blockchain allows for the generation of a unique output by each block, from the data contained in the latter. This output is then passed on the following block offering a permanent linkage between the two, and thereby denying by design any attempt of subsequent alteration of previous transactions.

WHAT IS HASHING?

Hashing designates the operation whereby various inputs of different sizes generate various outputs of constant sizes. Hashing algorithms will also always generate the same output for a same input.

BLOCKCHAIN ANALOGY

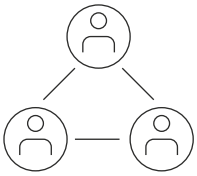
Block rank	Block		Hash analogy
1	hsgAO	→	EM
2	lzoEM	→	OF
3	pmzOF	→	LN

How are blockchain blocks created?

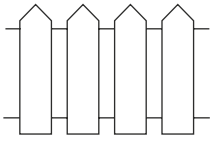
The production of new blocks is the direct result of a process known as «mining». As previously said, blocks are connected together thanks to cryptography. The production of new blocks necessitates the engagement of network participants, that put their computational power at use in order to allow for the mathematic encryption of transaction data.

Thereby, miners are responsible of the verification of all transactions. Furthermore, the reward they receive for their mining activity is in the form of newly created Bitcoins that are thus injected in the network.

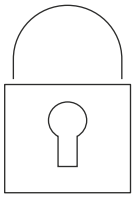
What does Bitcoin blockchain offer?



ELIMINATES COUNTERPARTIES
All Bitcoin payments are operated without the need for a counterparty, which allows for lower transaction fees and a reduction of the risks usually associated with the participation of middle-men.



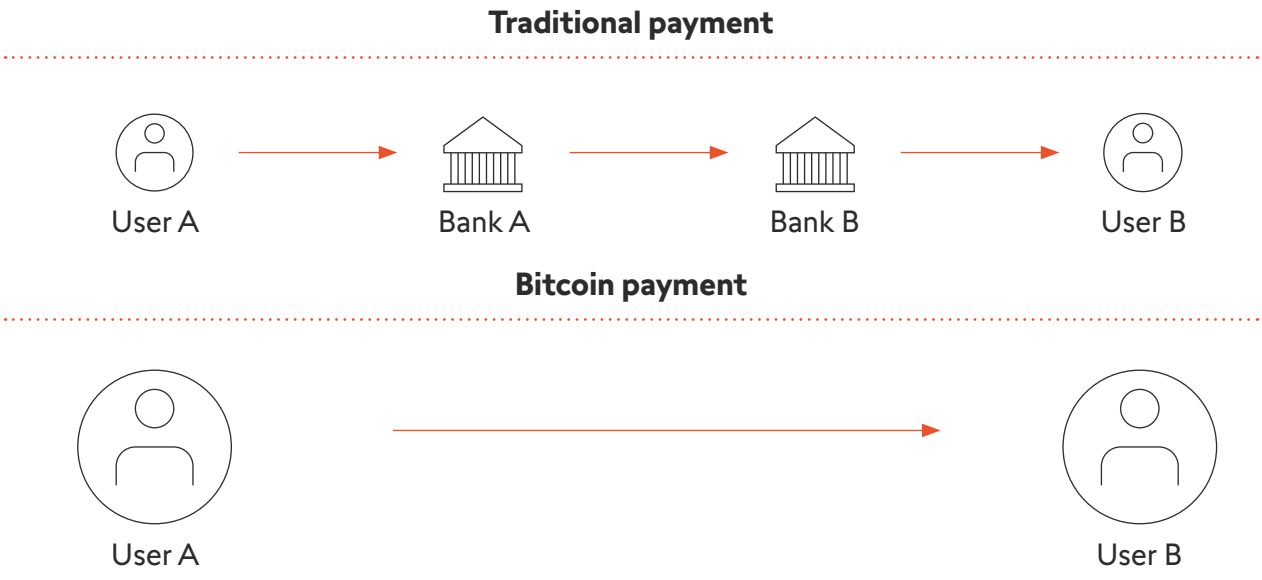
LOW ENTRY BARRIERS
The blockchain is permissionless, which means that there is no permission required to participate and contribute to the blockchain network. As such, a user only needs a connection the internet to be able to effectively engage in bitcoin transactions.



ENHANCED SECURITY
By being decentralized, blockchain does not offer a single central server that could be subject to malicious action. The blockchain functions thanks to a network of scattered nodes, and hacker has to target a very high number of nodes at once in order to compromise the network.

Bitcoin payments

Comparison with traditional payment methods



What are Bitcoin's non-custodial storage options?

Given the absence of a third party, questions often arise about the different available possibilities when it comes to non-custodial Bitcoin storage. There are two main options: hot wallets and cold wallets.

Hot wallets are online software that allow their users to store and send / receive bitcoins in a very simple way. Cryptocurrency holders' accounts can be considered as a type of hot wallet. On the other hand, cold wallets are stored offline – usually on a physical medium – and offer a higher level of security. Ledger is arguably the most renowned provider of cold wallets. Other options also include Trezor, KeepKey, and CoolWallet S.

Bitcoin nodes

What are Bitcoin nodes?

Bitcoin nodes can be defined as certain types of programs that interact with the Bitcoin blockchain. By being in constant communication with each other, these nodes are what allows Bitcoin to run as a fully decentralized cryptocurrency, by ensuring that all the defined rules are followed.

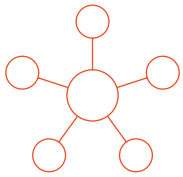
Full nodes, light nodes and mining nodes are the three major types of nodes in the Bitcoin network.

FULL NODES

These nodes are the heart of Bitcoin's decentralization feature. Full nodes upload and verify transactions and blocks thereof.

LIGHT NODES

Light nodes have reduced capabilities in comparison with full nodes, but also require less resources. They allow users to locate their transaction in a specific block.



MINING NODES

Mining nodes can be described as full nodes with the added capability of mining, and thereby block production. These nodes validate transactions before relaying them to other nodes.

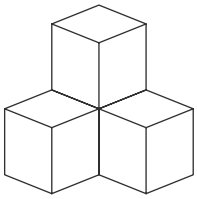
Bitcoin halving

What is Bitcoin halving?

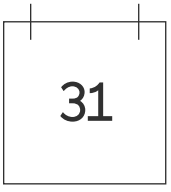
Bitcoin halving means that the usual reward miners get for verifying bitcoin transactions is divided by two. This event occurs every time 210'000 bitcoins have been mined, which usually happens every four years.

		Block reward for miners after halving
January 2009	Bitcoin launch	50 BTC
November 2012	1st Bitcoin halving	25 BTC
July 2016	2nd Bitcoin halving	12.5 BTC
May 2020	3rd Bitcoin halving	6.25 BTC
2024	4th Bitcoin halving	3.125 BTC
2028	5th Bitcoin halving	1.5625 BTC

Occurs approximately every 4 years



A major event regulating the supply of bitcoin



The next halving will happen around May 18th, 2020

Why do Bitcoin halvings occur?

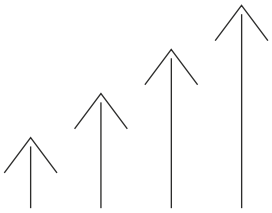
Bitcoin halving is embedded in the blockchain software and has direct implications for miners. Miners play a key role, as their activity allows for the verification of every bitcoin transaction.

Transactions are verified by blocks. Once a block of transactions has been verified, a miner receives a reward that consists of a number of new bitcoins. Today and until the next halving, a miner receives 12.5 BTC per verified block. After the next halving, this reward will be halved.

Bitcoin halvings will continue until the maximum supply of 21 million bitcoins is reached, which is expected to happen around 2140. After that, miners will still receive transaction fees in order to remain incentivized to verify bitcoin transactions.

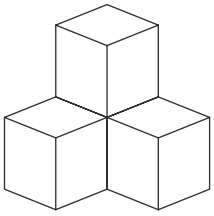
Halvings and Bitcoin price evolution

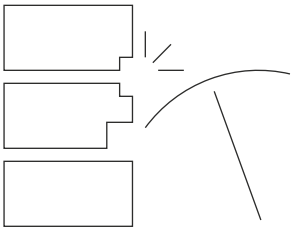
What are the consequences of Bitcoin halving?



Historically, bitcoin prices surge a month before halving and during the period after halving. To date, Bitcoin prices have never dropped below their value prior to the latest halving. This can be explained by many factors, amongst which increased attention around bitcoin and the automatic decrease in the supply of new bitcoins.

Halving is an immutable predefined planned reduction of the created bitcoin that occurs approximately every 4 years until the maximum amount of Bitcoin units have been mined. This is the way Bitcoin's inflation is controlled.





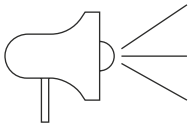
It is predictable that a certain number of miners might stop their activity as result of the 50% decrease of the block reward, that will not be able to cover their computing and energy costs. However, this should not have any effect on the speed at which transactions are verified, as the difficulty of verifying transactions is seamlessly adjusted by the software.

Bitcoin transactions

How does a Bitcoin transaction practically work?

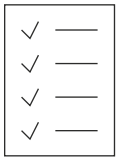
Example: Vanessa wants to send 10 BTC to Chad

1



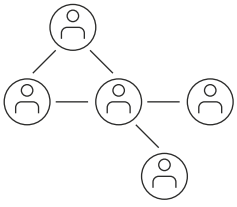
Vanessa informs the network of miners that she wants to send 10 BTC to Chad. She provides them with Bob's address, and her personal signature and public key to enable the miners to confirm her identity.

2



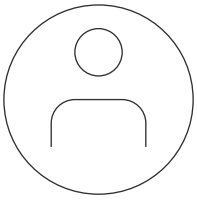
The miners check that verifying the transaction will prove profitable for them. They then make sure that the 10 BTC belong to Vanessa and that the transaction is valid - before placing it into a block.

3



The miner relays the information to the entire network of miners, so that they can verify its validity, and all add it to their copy of their blockchain.

4



Chad effectively receives the 10 BTC Vanessa sent him.

Automated verification of identity

No dependence on a central counterpart

Enhanced and permanent traceability

Forks

What are Bitcoin forks?

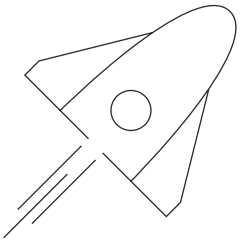
Forks are to the Bitcoin protocol what updates are to the different computer software we use in everyday life. Indeed, Bitcoin forks allow for the fixing of the various issues of the protocol and the further enhancement of its possibilities and performance.

The Bitcoin protocol is what defines the rules governing the functioning of the cryptocurrencies' protocol, that all the nodes of the network must follow (e.g. the size of a block). Thus, each fork can have important consequences on how Bitcoin works.

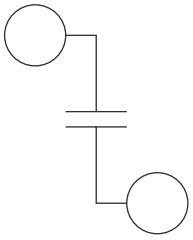
What is a soft fork?

There are two types of forks: soft works and hard forks. A soft Bitcoin fork is basically a modification of the Bitcoin protocol that stays compatible with the previous versions of the latter.

In practice, this means that older nodes (i.e. nodes that existed before the fork and that were not updated) are still able to process transactions as long as they do not violate the new rules established by the fork. On a side note, even in the case of soft forks, older nodes usually chose to be updated as that typically allows them to be more efficient in their operations.



More convenient for users, as there is no need for an upgrade



Lower probability of a chain split

What is a hard fork?

A hard fork is also a modification of the Bitcoin protocol, with the exception that older nodes that do not update to its latest version of the protocol will not be able to continue their activity at all.

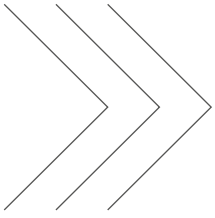
The two main types of hard forks

Planned hard forks

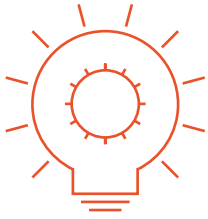
The vast majority the nodes upgrade to the latest version on a voluntary basis, thereby effectively abandoning the older version (i.e. the old chain) and leaving it with a small number of participants.

Controversial hard forks

This usually happens when the community disagrees on the upgrade, and usually results in the formation of two separate blockchains (i.e. a chain split), and thereby in thereby two independent cryptocurrencies.



Hard forks allow for much more latitude as compatibility with the rules of the previous versions does not need to be granted



The Bitcoin – Bitcoin Cash hard fork

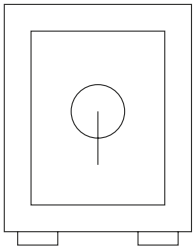
is hard fork happened in August 2017, as the community was divided on how Bitcoin's scalability issues should be addressed. With a fork always being based on the original blockchain, all Bitcoin holders received the same mount of Bitcoin Cash units at the time of the fork.

Proof-of-work algorithms

Blockchain consensus

As previously mentioned, consensus is one of the two main features of blockchain. Blockchain can typically achieve consensus through 2 types of algorithms: Proof of Stake (PoS) and Proof of Work (PoW). Bitcoin's blockchain uses the latter.

The original goal of PoW algorithms was to be able to defend against DoS («Denial of Service») attacks. DoS attacks typically disrupt individuals' access to networks, by overcharging them or making them crash with other harmful operations.



Thanks to the use of Proof-of-Work algorithms, a successful attack on the Bitcoin blockchain would require enormous computational capabilities and would prove to be very time consuming. Moreover, the high associated cost plays an important dissuasive role.

How do Proof of Work algorithms work?

In order for a block to be added on the Bitcoin blockchain, miners compete between themselves to solve complex mathematical problems (i.e. produce a hash) thanks to their computing power. Miners then broadcast their solution to other nodes (miners) of the network in order for them to check if the solution is correct.

Each of these blocks carry a block hash, which effectively represents the work done by miners – i.e. the proof of work. In order for an external malicious actor to hack Bitcoin's blockchain, it would have to produce a longer ledger than the one in place (with all the blocks since inception) – which would require almost unachievable computing power.

Summary

The most popular cryptocurrency

Designed in 2009, Bitcoin is the most-well known cryptocurrency to date. Its ambition was to create a «peer-to-peer electronic cash for the Internet» that would be «fully decentralized, with no central bank and no trusted third parties required to operate».

Bitcoin is supported by blockchain

The cryptocurrency is supported by blockchain, which provides it with many features, such as immutability or enhanced security and traceability.

Bitcoin is constantly improving

As its protocol is open-source, Bitcoin has an important community that is largely contributing to its development.

The future of Bitcoin

Due to its finite supply (21 million Bitcoin units), Bitcoin is often referred to as the «digital gold». Around 90% of Bitcoins have been mined so far. However, due to the Bitcoin halvings, it should take another 100 years before all Bitcoins are mined. Thus, due to its scarcity and difficulty to produce and the high liquidity associated with Bitcoin, many independent observers view the cryptocurrency as a safe heaven and an asset which value will appreciate over time.

ETHEREUM (ETH)

Current trading

Released in 2015 and often referred to as the «MS Windows» of cryptocurrencies, Ethereum is used to develop decentralized applications. Its associated cryptocurrency, Ether, is the second largest cryptocurrency in the market.
The inventor of Ethereum Vitalik Buterin developed the concept of «smart-contracts» which are programs executed on the blockchain.

KEY FIGURES (AS OF MARCH 25TH, 2020)

Crypto	Rank	Market Cap	Current Price
ETH	#2	EUR 14Bn	EUR 123.16

Price chart

Source: CoinMarketCap

General aspects

What is Ethereum?

Ether and Bitcoin are both well-known cryptocurrencies. The main difference between the two of them is the fact that Ethereum allows for **smart contracts** and the building of **decentralized applications (Dapps).**

Decentralized applications

While Bitcoin is mainly a money-transfer system powered by blockchain, Ethereum's ambition is different as its main goal is to **enable developers to build and publish decentralized applications (called Dapps) on its blockchain.** Many other cryptocurrencies available on Swissquote such as Eos, Chainlink or Tezos, also offer the possibility of developing and using Dapps.

Smart contracts are also expected to resolve several complexities that players are facing in securities trading, clearing and settlement, insurance claim management or even supply chain document management.

Ether – the cryptocurrency

Ethereum can be defined as a decentralized software platform, and Ether as its associated cryptocurrency. **As such, Ether is not only a tradeable cryptocurrency, but is also used by developers to pay for various services provided on the Ethereum network – such as running or monetizing applications**.

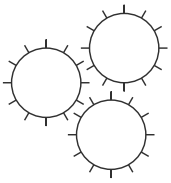
Ether can be obtained through both trading on exchanges and mining. Unlike Bitcoin, mining Ether does not require industrial capabilities as it encourages decentralized mining by individuals, with proof-of-work algorithms (complex mathematical problems needed to be solved in order to confirm the formation of a block).

Smart contracts

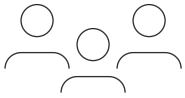
What is a smart contract?

Simply put, smart contracts could be described as self executing digital contracts. More precisely, these are computer code whose aim is to facilitate the transfer of value, content or property. **The main characteristic of smart contracts is that they allow this transfer of ownership or any other operation they are supporting only if certain previously defined conditions are met.** This allows for secure operations to take place between unknown third parties and an unmatched speed of execution.

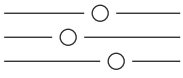
Publicly available on the ledger



Automatic execution of specific operations and transfers



Does not require the intervention of a middlemen



Entirely customizable

BENEFITS

- Provides superior security to traditionally enforced contracts
- Reduces transaction costs
- Ensures complete security even with unknown third parties

Ethereum Virtual Machine (EVM)

The EVM is often cited as the core innovation of Ethereum. It is a software that enables the development and execution of blockchain powered applications in the most efficient possible manner and safeguards them against all interferences with other programs on the blockchain.

LITECOIN (LTC)

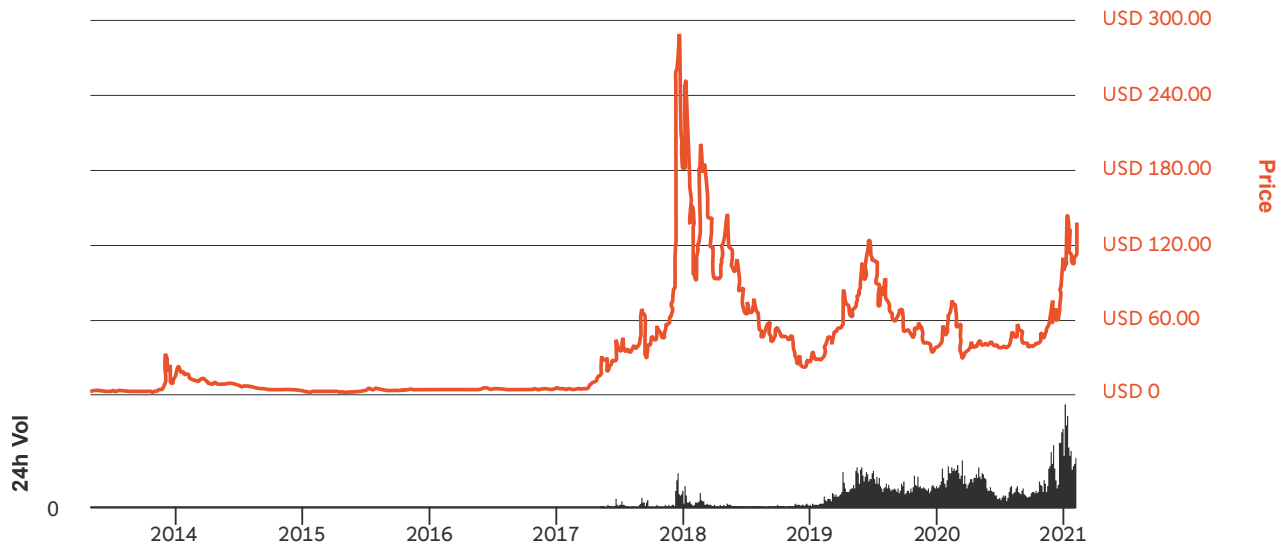
Current trading

Founded in 2011 by Charlie Lee, a former Google engineer, Litecoin is one of the first cryptocurrencies to be launched. The main ambition behind its creation was to establish a digital currency that would be more suitable for everyday use than Bitcoin.
Litecoin is based on the same open source code foundation as Bitcoin. Its main advantage is that its code enables a block to be generated every 2.5 minutes, compared to 10 minutes for Bitcoin.

KEY FIGURES (AS OF MARCH 25TH, 2020)

Crypto	Rank	Market Cap	Current Price
LTC	#7	EUR 2.3Bn	EUR 35.78

Price chart



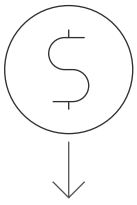
Source: CoinMarketCap

General aspects

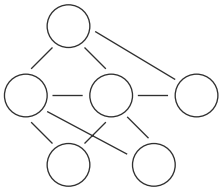
How is Litecoin different from Bitcoin?

Litecoin is a cryptocurrency that is the result of a fork of the Bitcoin core client. Practically, this means that Litecoin is based on Bitcoin's initial open source codebase, to which its developers have added new features. As such, Litecoin is also based on blockchain technology and relies on a fully decentralized system. However, new features were designed in order to serve Litecoin's ambition of solving issues that Bitcoin was not designed to address.

4x times faster transaction speed



Cheaper transactions



Different mining algorithm

Fast and near-zero cost transactions

While both Bitcoin and Litecoin rely on the proof-of-work algorithm, Litecoin uses Skrypt, which appears as a more democratic method of mining compared to Bitcoin's SHA-256 algorithm. Indeed, it is less processor intensive than SHA-256, because it does not create a rise in mining difficulty that would only make mining accessible to miners with heavy computing power. **Skrypt algorithm is what allows Litecoin to drastically reduce transaction costs.**

Similarities with Bitcoin

Alike Bitcoin, there is a limited supply of Litecoin, thereby protecting the cryptocurrency from inflation and helping it preserve its value. Litecoin transactions are verified like Bitcoin transactions – thanks to miners that are rewarded for each confirmed block of transaction. And like for Bitcoin, the reward for miners is divided by two after each halving (the next being expected to happen in 2023).

RIPPLE (XRP)

Current trading

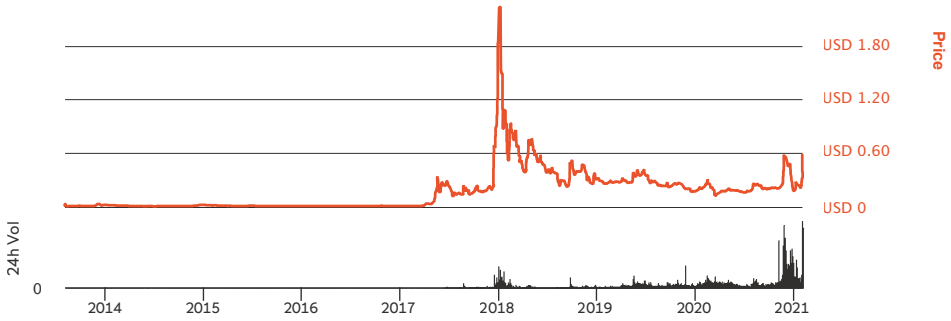
Ripple allows for ultra-fast transactions (circa 4 seconds) and offers particularly low transaction fees, combined with a scalable network. The Ripple real-time settlement centralized system can handle around 1'500 transactions/second.

The main feature of XRP is the network that supports it, which can be considered as an exchange facilitating payments between banks and other financial institutions.

KEY FIGURES (AS OF MARCH 25TH, 2020)

Crypto	Rank	Market Cap	Current Price
XRP	#3	EUR 7.0Bn	EUR 0.16

Price chart



Source: CoinMarketCap

Brief history

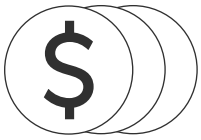
2004 — First prototype of Ripple as a decentralized digital monetary system (RipplePay)

2012 — Inception of OpenCoin, tech company focused on payment solutions for financial institutions

2015 — Official rebranding of Ripple Labs (ex-OpenCoin) to Ripple

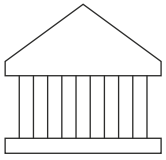
General aspects

The main features of Ripple



Convertible to all currencies

Transactions cleared in less than 4 seconds



Designed for financial institutions

The XRP ledger

The XRP ledger (XRPL)

→ **Open-source distributed system which allows for instantaneous financial transactions,** storage of accounting details and currency exchange services.

→ **Consensus is reached through Ripple's proprietary consensus algorithm,** that is enforced through a network of validating independent nodes.

→ **Ripple clients have access to a list of trusted nodes (the UNL), which all have to agree on the current state of the ledger.** Therefore, verifying ripple transactions does not rely on mining.

A cryptocurrency for financial institutions

Ripple is the first cryptocurrency which is targeted to banks and financial institutions. **Its ambition is to solve the issues that the latter face, in terms of liquidity constraints linked to possible FX rate fluctuations, speed of settlement (4 seconds compared to 2-3 days for traditional payment systems), while offering the level of security associated with the use of blockchain.**

BITCOIN CASH (BCH)

Current trading

Bitcoin cash was created through the August 2017 Bitcoin Fork. Alike Bitcoin, it is a «peer-to-peer electronic cash for the Internet. It is fully decentralized, with no central bank and requires no trusted third parties to operate».
The idea behind its creation was to offer fast, near-instant transactions and reduce the high cost of transactions associated with Bitcoin. This allows Bitcoin Cash to be used by individuals in everyday small transactions, which is not the case for Bitcoin.

KEY FIGURES (AS OF MARCH 25TH, 2020)

Crypto	Rank	Market Cap	Current Price
BCH	#5	EUR 3.8Bn	EUR 204.55

Price chart

Source: CoinMarketCap

The origins of Bitcoin Cash

Bitcoin Cash was created through a hard fork with Bitcoin in 2017. Bitcoin Cash's blockchain was altered in order to increase the size of a block of transactions from Bitcoin's 1MB to 8 to 32MB.

General aspects

Increased scalability and lower fees

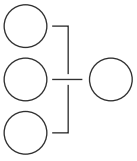
Transaction processing capabilities

By substantially increasing the size of a block, the ambition of Bitcoin Cash's new blockchain version is to solve the issues associated with higher transactions fees some Bitcoin users were facing.

Bitcoin Cash's blockchain reduces the time transactions need to find their way into a block, without the need to incentivise miners by setting a higher transaction fee. Thereby, Bitcoin cash appear more practical for micropayments and allows the network to prevent congestion even in periods of higher activity.

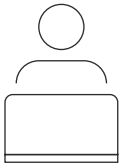
Thanks to its increased block size, Bitcoin Cash can also offer higher rewards to miners for mining a block, as the latter will be composed of more transactions.

Shared features with Bitcoin

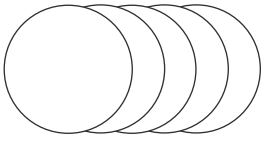


Blockchain based

Open source code



Proof-of-Work algorithm



Limited Supply (21 million coins)

NEXT STEPS – START TRADING WITH SWISSQUOTE

1

Go to **swissquote.com/trading**

2

Open a demo account.

3

You can practice trading
with CHF 10'000 virtual money.
No risk & no obligation.

Try a demo now!

Why trade with Swissquote?

- 20 years of online trading expertise
- Access to 3 million products on major international stock exchanges
- Most comprehensive trading platform on the market
- Multilingual customer support
- Training and education with online webinars
- High-performance mobile applications
- International Group listed on the SIX Swiss Exchange (SIX:SQN)

Swissquote is regularly quoted and consulted by global financial media.

Bloomberg

CNBC

FINANZ und WIRTSCHAFT

LE TEMPS

Investing.com

Neue Zürcher Zeitung

swissquote.com/crypto-assets/education