TRANSITION

Text document in support of the presentation:

Introduction to Cryptocurrencies and Bitcoin fundamentals

Created by MSE Institute

Co-funded by the
Erasmus+ Programme
of the European Union

Cryptocurrency and Blockchain Training

Table of Content

Blockchain

A blockchain is a chain of blocks, where each individual block in turn contains transactions. Thus, a blockchain is basically a list of transactions, similar to a journal, from an accounting point of view. The blocks in a blockchain are linked together using a mathematical process. This is called cryptography.

The best-known blockchains are currently Bitcoin and Ethereum.

A blockchain can be operated privately / consortium-based / public or in a mix of those forms.

Bitcoin

The term Bitcoin refers to two things. On the one hand, a currency and, on the other, the associated payment system.

In contrast, the euro, for example, is only a currency. VISA, PayPal or Swift are equally only payment systems. In English, bitcoin in lower case refers to the currency and bitcoin in upper case refers to the payment system.

Bitcoin is based on the white paper by the persona Satoshi Nakamoto, which was published in 2008 under the title Bitcoin: A peer-to-peer electronic cash system and is freely available. (www.bitcoin.org/bitcoin.pdf)

Difference between Bitcoin and Blockchain

Bitcoin is the new digital currency and blockchain is the database behind it. In Bitcoin, the digital token Bitcoin is the essential part of the blockchain of the same name.

Many modern blockchains, such as Ethereum or Ardor, have the respective blockchain with the basic token of the same name. This is needed for the operation of the blockchain, i.e. the transaction fees. However, countless other tokens can be generated by the users on the particular blockchain for different use cases.

Typical features of a Blockchain

A blockchain in the very classical sense is typically:

- Decentralised
- Complete
- Public
- Immutable

Distributed Ledger Vs. Blockchain

Every blockchain can also be seen as a distributed ledger technology (DLT), but not every DLT is a blockchain.

The specific difference is that in a blockchain, the information is bundled in blocks and these blocks are cryptographically linked to each other.

Block

Several transactions are combined into one block. The mechanics vary depending on the blockchain system. For example, a block can be generated after a certain period of time, number of transactions, size of data to be processed or a mixture of all of these.

A block is therefore a container in which the transactions are grouped together. The blocks are linked to each other with unique hash values. Thus, a block contains the hash value of the previous block and passes on its own hash value to the next block. This ensures the non-manipulability of the blocks. By the way, the first block of a blockchain is called a genesis block.

Transactions

A transaction is the transfer of a blockchain-based asset/token from one address to another. In specific cases, it can also mean from one's own address to one's own address, or sending a message instead of an asset/a token. The assets/tokens are accessed via a full node, a web-based node of a blockchain system. Or a wallet that can process the addresses and transactions of multiple blockchain systems.

The recipient's blockchain address/public key must be known, as well as the sender's own secret/private key. The latter is used to start / sign the sending process.

On public blockchains, a fee is charged for this. This fee can usually be calculated automatically. If you set the fees manually, you can ensure that your transaction is integrated in the next block by overpaying. However, underpayment can result in the transaction not being taken into account or only after a long delay.

In a crisis - i.e. a crash - the fees often increase that many people would like to sell the assets on a trading exchange and have to make a transaction from a cold wallet to a trading exchange first.

In banking, it can be compared to transferring Euros from one IBAN to another. On the one hand, you need to know the recipient's public IBAN. While the private key is the access code to the telebanking system or the signature on the payment slip.

Non-Public Transactions

Basically, all transactions are public, in the sense that all hash values of the transactions are stored in a block with the basic information such as sender and recipient and the number of tokens transmitted.

However, encrypted messages can be attached to a transaction, for example.

Some modern blockchain systems also allow these messages to be stored only up to a certain block height, for example.

Non-public transactions can arise, however, if, for example, transactions on a trading exchange are initially only processed locally in the exchange's database and real blockchain entries only take place when sending or withdrawing assets/tokens.

Another possibility for non public transaction is by linking private / consortium-based blockchain systems with public ones. In this case, the transactions on the private blockchain would possibly not be publicly visible.

Wallet

A wallet is usually a smartphone app or a web app with which you can access your blockchain-based assets/tokens. This means that the wallet manages the public address and, ideally, allows you to operate with the actual secret/private key. Why optimal case? If you access your wallet via a trading exchange, the exchange manages the secret/private key and you therefore do not have direct access to your own tokens. With some of these trading exchanges or crypto apps, you don't even see your own public address, but are completely at the mercy of the provider.

With the smartphone apps / web apps described above, you do not operate your own node, which means you have not downloaded a copy of the blockchain, but use the provider's infrastructure.

The safest option is always to use your own full node of the blockchain and the wallet of that node, where possible. Only then is 100% data ownership guaranteed.

There are several types of wallets on which the tokens are accessible, namely:

- Mobile wallets
  Mobile wallets are wallets that run as an app on a smartphone. It is a very convenient way to receive, hold and send coins and tokens. Most mobile wallets try to hide the complexity of the matter via a pleasant user interface. This is done through using QR codes, Storing the private key locally and accessing it via a user/password system, creating a kind of "phone book" of the owners, so that one is not confronted with the long deterrent address every time.

- Desktop wallets
  Desktop wallets are wallets that run as a program on a PC. Due to the possibility of compression by malware, this may not be a very secure way of storing and using coins and tokens.

- Paper Wallets
  All necessary information (public and private key) are printed on a piece of paper and the information is not stored in a digital document. See cold storage below.

- Hardware Wallets
  Hardware wallets are a form of cold storage where there is no ongoing connection to the Internet. The addresses and keys are stored on a stick, similar to a USB data stick. Hardware wallets should only be purchased directly from the respective manufacturer. Well-known brands are Ledger Nano S, Keepkey and Trezor.

- Web Wallets
  Web wallets are a convenient but insecure way to hold coins and tokens. The operator holds the private key for you. There is a saying in the community; “not your key, not your tokens”.

In addition, there are those wallets that are managed for you by a crypto exchange.

Basically, at least from a historical perspective, the rule of thumb is that the more secure a wallet is, the less user-friendly it is.

Cold Storage

Cold storage is a special secure method of storing tokens. Better said the keys to the corresponding addresses. The storage takes place without a connection to the Internet. Paper wallets and hardware wallets are examples of cold storage.

Address

An address is a combination of letters and numbers, such as the following address of the blockchain Litecoin: LhPZaygUVTd53LNtqHu4wHqeRbhn1HuA9h

The address is the public key, comparable to one's own IBAN number of a bank account or home address. The difference to the IBAN, however, is that the transactions are publicly visible, including any associated messages, unless these have been separately encrypted. This is done either via your own full node or via a block explorer. For example, at the above address:

https://blockchair.com/litecoin/address/LhPZaygUVTd53LNtqHu4wHqeRbhn1HuA9h

The address is basically anonymous, unless you publish it yourself, for example on the website of a trader who accepts crypto assets/tokens in the form of cryptocurrencies.

However, to have access to the assets/tokens associated with this wallet address, you need the secret/private key. You can either enter this key directly, then you actually have access to your own assets/tokens. Or you control the entry via user/password at crypto exchanges and they then use the stored key to send the assets/tokens. Caution: In the latter case, you are dependent on the services of others. This will be discussed in the fraud section of the seminar.

Market Capitalization

The market capitalization of a cryptocurrency is calculated, similar to shares, by multiplying the number of issued tokens by their respective last traded price.

However, care must be taken and the market turnover and the number of market participants must be taken into account. Otherwise, it is possible to artificially raise the market capitalization to astronomical heights, even though only a few people exchange tokens with each other.

Secret/Private Key

A secret/private key is similar to the public key, aka the wallet address, also a combination of letters and numbers. For example, it might look like this: 984b0fd5110e4ef790ecd0fe2bb4ffc9.

In recent years, however, it has become common practice to choose a set of words instead. (e.g.: butter tourist soda relief ability juice fantasy glow boss wine cloth farm habit like deny gospel input host). The more words the secret/private key contains, the more secure it is. With the choice of a set of words instead of the classic key, there is no longer a risk of confusion between the private and the public key.

Again, to make a comparison with the bank account: The public key corresponds to the IBAN, the private key to the pin code to access the bank account. And of course, additional security measures such as 2-factor authentication are recommended.

Block Time

The block time is the target for when new blocks are to be appended to the blockchain. The block time determines how quickly transactions are to be carried out. However, the block time can be influenced by other parameters, e.g. that a block is created after 10 minutes, unless there are already 2 MB of data in the block, or a certain number of transactions. This all depends on the design of the respective blockchain system.

Block Height

The block height corresponds to the number of blocks in front of a given block. The Genesis block has a block height of 0. The block height is therefore the counter of a blockchain and you can roughly estimate the time with it. For example, when the community votes on a change to the source code behind a blockchain.

Block Explorer

A block explorer is a kind of search engine that allows you to search and view data in the blockchain. Examples (among many) are Blockchain.info, Etherscan.io or ardor.world. Every blockchain system has one or more providers of such explorers. Caution is advised, however, as you are of course looking at the blockchain "through someone else's eyes", and you in turn have to trust these providers that no erroneous data is being displayed.

Cryptocurrencies

A cryptocurrency is a blockchain-based asset/token whose primary purpose is the transmission of monetary value. The best-known cryptocurrencies are Bitcoin and Litecoin.

However, any blockchain-based asset/token that is speculatively traded can also function as a cryptocurrency. And blockchain systems on which further tokens/assets can be created can also take on this role. The best known of these is Ethereum or from a historical perspective, nxt.

Furthermore, there is also the category of stable coins. These are always tied to a FIAT currency and should be backed 1:1 with reserves in this currency. Audits are extremely important here, as the danger of fraudulent intentions with new stable coins is a definite given.

Alexander Pfeiffer has created a possible categorization/example list of tokens/assets.

Utility Tokens/Assets

Utility tokens are blockchain-based assets/tokens that serve “a higher purpose”. This is the storage, transfer and verification of data beyond the original purpose of blockchain assets/tokens as a direct means of value.

There are countless use cases. For example, keeping a land register, distributing self-produced electricity in the neighbourhood, storing grades and certificates, keeping an account register between banks on different continents, establishing worldwide customer bonus programs, setting up ticket systems at concerts, securing digital assets in games, securing tangible products against counterfeiting and much more.

Alexander Pfeiffer has created a possible categorization/example list of tokens/assets.

Example (Categorization) of Tokens/Assets Types

- Cryptocurrencies: Tokens with the purpose to serve as currency supplement and to transfer monetary values. Traded on dedicated exchanges or over the counter [Like Bitcoin (BTC), Litecoin (LTC)]

- Stable-Coin: Tokens with the purpose to serve as currency supplement and to transfer monetary values, with a nearly fixed conversion rate to a FIAT reserve currency [Like Tether (USDT), USD Coin (USDC), AEUR (AEUR)]

- Tradeable network maintenance utility tokens: Tokens which serve as a reward to maintain the network and which are traded on exchanges. May also have aspects of other token categories, e.g. additionally serve as cryptocurrency [Like Ethereum (ETH), Ethereum Classic (ETC), NXT (NXT), Ardor (Ardr)]

- Non free-tradeable network maintenance utility tokens: Not traded on exchanges, but their distribution can determine the power within a consortium-based (or private) network [tokens that are not traded on exchanges but distributed from a smart contract or centralised authority, mostly with a fixed number of issued tokens from the beginning, like a typical PoS approach; this could be also a token that represents a right to vote for something (and its voting power)]

- Tradeable utility tokens: Tokens that have a specific purpose, e.g. to represent a digital or a real good. The value of this asset is determined by supply and demand on a token trading exchange [like Steem (Steem), Augur (REP), or 'historic' approaches like Amps (AMP), NEXIUM (NXC)]
- Fixed-price (including peer2peer price-negotiable) tradeable utility tokens: Tokens that have a specific purpose, e.g. to represent a digital or a real good. The value of the token is determined by the issuer; a third party that has a contract with the original publisher that allows them to set the prices, as a result of negotiations, or for example at a classic auction (as a restricted bargaining room) [any specific token that represents e.g. a digital art piece, or a real life item of value (indicating its ownership]
- A (tradeable or non-tradable) token representing a share of ownership or a share of contribution to something, leading e.g. a certain reward [Like KuCoin Shares (KCS), Huobi or Binance Coin (BNC)]
- Non-freely tradeable utility tokens: These tokens store data, such as certificates, grades, ownership of a piece; fine art prints (e.g. limited edition prints, each with a unique number), or a last will; they can be a unique (singleton) token per record or a message attached to a specific token when sending. A separate series of tokens is generated for each different use case. Each series has its own asset ID on the respective Blockchain. (the name of the series does not have to be unique, only the asset ID). This means: The moment a message is added to one of the tokens (from a series) and this token is sent, the connection of the token with the message and the rule that the token cannot be forwarded without the knowledge of the original sender becomes a unique process, which is identified by the unique transaction ID. Messages can be attached unencrypted or encrypted. This data is usually linked to a person or a property and is not (or only under specific circumstances) tradable. It is also linked to a specific wallet (e.g. of the recipient). The Singleton/Unique Token form of this category is similar to the concept of non-fungible tokens (NFTs).

Smart Contracts

Smart contracts go back to the ideas of computer scientist and lawyer Nick Szabo. He published an article on the subject in 2002 (A Formal Language for Analyzing Contracts) (https://bit.ly/2i2IRpB). They are computer programs, mostly simple if-then instructions, which are stored on a blockchain basis and therefore cannot be manipulated. Smart contracts can digitally implement any type of contract we can imagine, but above all, they can also automate digital action processes. It is often important to include digital identities in the process of creating the smart contracts and to excessively check the functionality before they are published. Use cases that are frequently mentioned can be found in logistics, in the area of energy supply or in the area of a digital land register.

Types of blockchains (private / consortium / public)

Blockchain systems can basically be operated in three different ways:

Private blockchain: is basically a closed system and is operated exclusively within organisations, companies or government structures. No information is passed on to the outside world unless there is evidence that a transaction has taken place.

Blockchain operated by a consortium: serves connected parties who have a common goal. Consortium partners may join the Blockchain on the basis of joint agreements.

Public blockchain: has no restrictions on joining and/or leaving the Blockchain. All information is public, although it is possible to store some information in encrypted form.

Private and consortium blockchains can also store information on a public blockchain, for example the hash value of all transactions within – for example 24 hours. This keeps the data content itself private but ensures that no data manipulation takes place retroactively. Not block by block, but still, as in the example above, for all data older than 24 hours.

Airdrops

Airdrops are tokens that you receive because you are in possession of another cryptocurrency or asset. Many new projects on Ethereum, NXT, or other blockchain systems where additional tokens can be generated use airdrops to promote their ICO or provide more decentralized distribution. From a tax perspective, airdrops are constantly discussed and also how to deal with unwanted airdrops from a recipient perspective.

SegWit (and the Bitcoin forks)

On July 21, 2017, bitcoin miners locked-in Bitcoin Improvement Proposal (BIP) 91, enabling Segregated Witness at block 477,120. SegWit helps with scaling in two ways:

SegWit should eliminate transaction malleability, allowing the Lightning Network, an overlay network of micropayment channels, to scale by allowing nearly infinite numbers of immediate, low-fee transactions "off chain“.

On August 8, all bitcoin mining pools indicated support for SegWit, albeit it would not be completely active until August 21st, when miners would start rejecting blocks that did not support SegWit. In the beginning, most bitcoin transactions were not upgraded. Segregated Witness began on August 24, 2017. The week after SegWit was enabled, bitcoin's price climbed over 50%. Bitcoin traded at $2,748, up 52% from $1,835. In the first week of October, the proportion of network transactions employing SegWit increased from 7% to 10%. Unhappy with the proposed SegWit improvements, a small group of largely Chinese bitcoin miners provided an alternative plan for a split, resulting in Bitcoin Cash. Which lead to a fork into Bitcoin and Bitcoin Cash and the resulted into two rival groups within the Bitcoin community.

However, it turned out quite quickly that Bitcoin Cash became the altcoin with much lower trading volume than the continuation of the original Bitcoin blockchain with the Segwit upgrade.

This led to another dispute within the Bitcoin Cash community and a fork of this alternative variant to Bitcoin. On November 15, 2018, Bitcoin Cash hard forked into Bitcoin Cash and Bitcoin SV. The split resulted from a "civil war" between two bitcoin cash camps. Bitcoin ABC (Adjustable Blocksize Cap) was pushed by entrepreneur Roger Ver and Bitmain's Jihan Wu, keeping the block size at 32 MB. In contrast, the "Bitcoin Satoshi Vision" party led by Craig Steven Wright and millionaire Calvin Ayre proposed increasing the block size limit to 128 MB.

Until August 24, 2017, all 3 variants share the same transaction history. Thus, if you purchased a Bitcoin before that, you own all 3 iterations of Bitcoin.

Forks

A hard fork is a fundamental change to a blockchain protocol that is incompatible with all previous blocks. Hard forks are often the product of ideological or technological disputes within the crypto community.

After a hard fork, nodes still running the old software are invalid. In order to continue on the new version created by the fork, all nodes must follow the new rules.

Hard forks can be implemented for a variety of reasons. One of the most famous Bitcoin hard forks took place when the developers decided to change the size of the blocks on the Bitcoin blockchain. The developers thought this would make mining blocks faster and help increase the user base. The result was Bitcoin Cash, a new cryptocurrency that is incompatible with the original Bitcoin despite its shared heritage.

But hard forks are not always born out of disagreement. Sometimes serious security risks are found in old versions of software, and sometimes developers decide that new features should be added. These developments are often agreed upon by consensus and are not always the result of division within the crypto community. Here, users need to upgrade to the latest version of the node in order to generate valid transactions and not be on an invalid fork.

Bitcoin: A Peer-to-Peer Electronic Cash System Whitepaper

In October 2008, someone under the pseudonym Satoshi Nakamoto presented his concept of the electronic money system in a cryptography forum on the internet. This is now accessible at www.bitcoin.org/bitcoin.pdf. This paper describes the theoretical foundations of this new cryptocurrency and is considered as the founding document of the entire crypto and blockchain movement.

We don't know who Nakamoto is. The last contact was in April 2011, when he/she gave the bitcoin.org domain and the Bitcoin source code to several prominent members of the community.

Forerunner projects

Of course, even before Nakamoto's white paper, there were various attempts to redesign electronic money systems.

- ecash by David Chaum
- Hashcash by David Back
- Bit Gold by Nick Szabo
- b-money by Wei Dai

to name but a few.

Nakomato knew these projects and ideas, their strengths and weaknesses, and incorporated them into his/her consideration.

When did Bitcoin become more popular?

There were several spikes whenever the Bitcoin price reached a new milestone on the exchanges. A big media wave, also in the mainstream, was in December 2017. This was particularly noticeable in the Google search queries.

The number of queries decreased continuously in 2021, but this can also be explained by the fact that more people now know, at least on a superficial level, what a Bitcoin is.

The first documented purchase between Bitcoin and classic means of payment was in 2010. A person bought 2 pizzas for 10 000 Bitcoin.

The first exchange of Bitcoins within the community began in 2011. Here, Bitcoin reached the rate of 1 euro as a peak.

A breakthrough was in June 2011, when Wikileaks accepted donations in Bitcoin, when the US government had banned classic electronic means of payment for donations to this platform.

From a negative perspective, Bitcoin achieved notoriety in 2013 and 2014. In 2013 as a means of payment on the Dark Net, on the illegal trading place Silk Road. And in 2014 when the trading exchange Mt. Gox closed, with 850 000 customers Bitcoin disappeared. At the time, over 70 per cent of global trade went through this platform.

Main difference between Cryptocurrencies and Fiat / conventional money

Conventional money - also often called FIAT from the Latin "let it be" - is issued by a central bank. Bitcoins and other cryptocurrencies are created or managed by the network, depending on the consensus algorithm.

In the meantime, however, there are approaches to using blockchain technology to manage the monetary assets issued by central banks.

With conventional money, the determination of the money supply is based on political decisions. With blockchain-based assets, on the other hand, an algorithm is the determinant. However, changes to the algorithm can be made through the votes of people, such as the current asset holders or those who provide mining power (depending on the rules of the specific blockchain).

Blockchain transactions do not require intermediaries. Provided the sending party controls its private/secret key, it can send assets directly from the owners wallet to another address. However, there is of course also the variant where a web trading exchange or bank is involved, as with the classic bank transfer, and in future there will even be monetary values and crypto values stored in the same account.

The creation of a wallet address via a node or a wallet software can also be done by yourself, you do not need anyone to open an account for you.

However, when assets are traded, bought and sold, a very strict KYC has been established in Europe, America and Asian countries. Of course, a peer2peer exchange of crypto assets is still possible. However, registration with full name, address, passport copy, etc. is necessary if you want to connect the blockchain world with the world of traditional bank accounts.

The situation is similar with foreign transactions. Basically, the blockchain has no borders and you can send assets from one wallet to another. It is nation independent as you just distribute the assets on the network to another address. The owner of the wallet has access from anywhere in the world with their own private / secret key.

How can blockchain-based assets / cryptocurrencies like Bitcoin be acquired?

There are various methods here, the most common being:

- ➢ Buying directly from another person, for example at a real meeting where the blockchain asset is exchanged for cash.
- ➢ Purchase from a cryptocurrency vending machine. These vending machines, often simply called Bitcoin vending machines, are booming worldwide.

- Buying through a crypto selling platform such as Coinbase or Bitpanda.
- Buy from a crypto trading platform such as Kraken, Binance or Bittrex.
- Buying Bitcoin / Crypto vouchers or symbolic coins in which the key is engraved, for example.
- Original purchase through mining / forging. So as someone who is proactive part of the network.

How can Crypto Assets or Bitcoin be lost?

There are various methods here, the most common being:

Access to blockchain assets can also be lost. In the worst case, forever. In the case of Bitcoin, it is estimated that the keys to access around 4 million Bitcoins have been lost.

The reasons for this are manifold:

- Death of the owner and no "dead man switch" installed, which transfers the keys to the heir via a smart contract.
- Broken hard drive, USB sticks or simply lost or yellowed paper slips on which the keys were stored.
- Forgotten passwords to the trading exchanges or password safes.
- Trading exchanges that go bankrupt or where the owners have fraudulently misused the keys.

In any case, it pays to store the keys in different secure ways, for example on a dedicated USB stick and additionally printed on hard paper, foiled in a safe.

What is a consensus Algorithm?

The following must be prevented:

- sending tokens/assets that do not belong to you.
- the same token/asset being sent several times
- that all entries on the blockchain are always checked and that all nodes have the exact same copy of the blockchain after a block has been formed.

For the first problem, the already known digital key the private / secret key, is used. The digital signature of the account holder.

The second and third problems are solved with a decentralised database, which is always synchronous and where data truth always prevails.

There is a consensus mechanism in the source code to achieve this, but it varies depending on the blockchain used. The most common are Proof of Work and Proof of Stake. There are also hybrid forms and alternative experiments.

Proof of Work

How does “Proof of Work (PoW)” work on a Blockchain?

In the context of blockchains, performing a proof-of-work mechanism or calculating the results is called "mining". In the process, the miners try to find a result with certain properties by performing billions of arithmetic operations. Once they have found such a result, they are remunerated with the so-called block subsidy.

The process of a transaction being pushed into the network looks like this until it is confirmed:

- Transactions are combined into a block
- The miners check whether these transactions are legitimate by hashing the block header of the candidate block
- The first miner to find the solution receives the block subsidy as well as the transaction fees
- The validated transactions are appended to the blockchain in the form of the block

How exactly do the proof-of-work calculations work?

The miners use hash functions, meaning mathematical functions that generate a fixed-length string from a string of characters of any length. The difficulty lies in finding a result with certain properties that result from the hash function. Bitcoin, for example, uses the SHA-256 hash function for mining.

From the miner's point of view, the question must be solved:

"What input do I need to put into the mathematical function to get the given output?"

Since an important property of the hash function used is its non-existent invertibility, one cannot simply calculate for an output what the corresponding input was.

Instead, one has to "guess" what the input was that can be used to obtain that exact output. Therefore, the miners perform the calculations billions of times per second and try out many input values until one has finally found an input that gives the desired output.

If the block is then mined correctly, it is appended to the blockchain. Since all participants in the network know the algorithm, they can check that the solution is correct and that they have a valid blockchain. The key is that it is easy to check whether the calculations are correct, while the calculation itself is complex on the part of the miner. The proof is difficult to provide, but easy to verify.

Proof of Work – Mining difficulty

What is the difficulty?

The difficulty results from the difficulty of finding the desired output of the hash function. In the case of Bitcoin, for example, it is specified how many zeros the output at the beginning of the string (nonce) must have. The more zeros are required, the more difficult it is to find the output. This can easily be illustrated with a lottery game. Hitting two correct numbers is much easier than hitting six of the given numbers.

The difficulty in Bitcoin is always set so that a new block should be found every ten minutes on average. This benchmark is checked every fortnight. If it turns out that the benchmark of 2,016 blocks was exceeded in a fortnight, in other words that more blocks were found than intended, the difficulty is too low and is corrected upwards - and vice versa.

Proof of Stake (PoS)

Proof-of-stake is an alternative consensus mechanism for public blockchains. Instead of the hash rate, the stake of a user is decisive in the proof-of-stake mechanism. The stake is a certain number of tokens that is assigned to the user's own validator node. The larger the stake, the more likely it is that this user will be selected to validate the next block. Simply said, whoever owns a larger share of the company normally receives more voting rights that entitle them to make decisions.

An important difference, however, is that the proof-of-stake mechanism uses a random algorithm to build consensus on a blockchain network. This draws a participant who then has the right to mine the block. In simple terms, each token is then a winning ticket - consequently, users with a higher stake (= more tickets) also have a higher probability of being selected. In contrast to proof of work, the new tokens are not released gradually, but the number of tokens in circulation is fixed from the start.

One of the first pure proof of stake networks was Nxt, which has been running without any problems since 2013. However it does not play a role anymore in regard to "coinmarketcap".

Proof of Stake has the enormous advantage of being very eco-friendly.

Others Approaches / Consensus Algorithms

There are many different other variants. Many of them are experimental or research prototypes. Often they are hybrids of the two already mentioned. Or variants where the community chooses which nodes are allowed to validate the blockchain. These nodes are often called delegates, hence the name delegated proof of stake is common for the iteration.

Mempool

When a transaction is commissioned, one of the usually tens of thousands of nodes first checks whether there is double spending and whether the correct private key is used. If both are correct, the transaction is passed on to potentially be processed in the next or one of the next blocks. This stage is the mempool. The speed of processing often depends on the amount of transaction fees paid.

Mining

Using Bitcoin as an example, each miner prepares a block that can potentially be used in the blockchain, the so-called candidate block. In this block comes the hash of the previous block, then selected (usually lucrative for the miner) transactions from the mempool and finally a count value (the nonce value).

In order for one of these prepared blocks to actually become the next block in the blockchain, the miner must solve a mathematical problem through trial and error. This is very computationally intensive, depending on the current mining difficulty. The more computing power a miner, or a mining pool, i.e. an association of miners, has, the greater the chance of winning and being the first to solve the puzzle. And thus collect the reward. The mining difficulty varies depending on the total computing power in the network and the algorithm of the blockchain can almost perfectly adept to new situations.

A hash is created from the candidate block. The guess attempt is successfully completed when the hash created from the candidate block has a certain value.

In a kind of cryptographic lottery, all miners now try to solve the puzzle; who wins ultimately depends on chance. But the more computing power you have in the race, the higher the chance of winning, of course. Once a miner has solved the puzzle, it is verified by the other participants. This process is very fast. The candidate block of the successful miner becomes the actual next block of the blockchain. The candidate blocks of the unsuccessful miners are discarded in this process.

This puts the block of the successful miner into the blockchain. All initially unconfirmed transactions contained in the block become confirmed transactions. Thanks to the consensus, a new block is thus created.

Shortly after that the block is accepted in the network. The blockchain is thus extended by one block. The transactions contained in the last block are deleted from the mempool.

At this moment, all miners discard their unfinished candidate blocks and the game starts over.

ICOs / IPOs

Initial Coin offerings (ICO) are a way to raise capital in apparent imitation of IPOs (Initial Public offerings). In most cases, a group of individuals or a company sells blockchain-based tokens either for a share in the company or for a future service.

Mostly, however, it is not so much the latter, i.e. utility tokens, but shares and thus the speculative side around blockchain tokens.

A starting price of the tokens is set and you can buy them. Mostly in exchange for an established cryptocurrency.

ICOs have fallen into disrepute in recent years, because in addition to the legitimate and in part also very successful previous approaches, there is an extraordinary amount of fraud around this topic.

Advantages of accepting Cryptocurrencies

Payment with cryptocurrencies is advantageous from the point of view of a merchant/the seller, because:

- The purchase price is received more quickly than with credit card payment
- Lower fees should be incurred than with credit card payment
    - However, there may be exceptions to this, for example if there is a kind of fee war in the event of a crashing price as to which transaction should go into the next block.
- No cash has to be checked, held, stored and taken to the bank.
- Optimally, a separate receiving address is generated for each purchase so that the customer does not have a window into the finances of the seller. Therefore, it is often very clumsy, as you can still see, if a fixed address is written directly on the homepage of the buyer, or a printout, which serves for all transactions.

Disadvantages of accepting Cryptocurrencies

Disadvantages, on the other hand, from the point of view of the merchant/seller are:

- Often, it is necessary to again establish a service provider between the buyer and the seller, which manages the Bitcoin / Cryptocurrency payments. This is a sensible step for sellers for reasons of convenience, especially with regard to legal processing, etc.
- The often rapidly changing exchange rate to classic currencies
    - This can be offset by automatically exchanging a predetermined percentage of the crypto transaction into traditional currency.
- The waiting time for the transaction to be confirmed by the blockchain, which varies depending on the blockchain system. From a few seconds with Ardor/Ignis up to 10 minutes with Bitcoin.

- Here, too, there are already solutions such as the Lightning network, where transactions are also confirmed via Bitcoin in a fraction of a second. Here, a second layer is built on top of the blockchain.

Advantages of paying with Cryptocurrencies

Payment with cryptocurrencies is advantageous from the point of view of a buyer, because:

- The merchant is not given any sensitive credit card data. Nevertheless, care should also be taken with one's own wallet address and solutions should be used where a separate outgoing address is generated for the respective payment. Otherwise, the seller has full insight into the buyer's liquidity. Lower fees should be incurred than with credit card payment.

- The buyer can also make purchases anonymously, unless strict Know You Customer rules are implemented.

Disadvantages of paying with Cryptocurrencies

Payment with cryptocurrencies is advantageous from the point of view of a buyer, because:

There are no obvious disadvantages. Except for the points already discussed:

- Depending on the blockchain and the seller's T&C, there could be a delay period during the transaction

- Depending on the seller's T&Cs or the regulation of the country where the purchase is made, various know-your-customer measures could be in place.

- If no own outgoing address is generated for sales, then one gives the seller insight into the own financial strength, at least of the respective address used.

Payment process

Mostly, a QR code and the address of the buyer's wallet is shown. Either as a printout at the checkout, on a tablet PC or visible on the website when buying online.

When paying from a mobile wallet, the easiest process is to scan the QR code. Otherwise, the seller's wallet address can be copied and pasted.

Then everything should be checked again well, it is recommended to always check the first and last letters as a minimum. Since there is already virus software that detects that a wallet address is copied to the cache, and then another address is inserted when pasting.

Risks

- A rather negative perception of bitcoin and blockchain among the general public.

- A high energy consumption of PoW blockchains, such as Bitcoin.

- Manipulation of the exchange rate by Whales (Holders of large numbers of a cryptocurrency or tradable token).

- The lack of scalability of Bitcoin's mainnet, or the possible lack of trust in 2nd layer solutions like Lightning.

- Lack of acceptance of cryptocurrencies in daily life.

- Double spending due to possible 51% attack.

- The legal uncertainty.

- The need to trust the source code of an unknown programmer.

- Fraud “around” the topic of blockchain.

- Ongoing warnings from governments and regulators.

- While blockchain is an immutable database, there is no way to prevent the information stored on it from being incorrect. This makes digital identities and other procedures for verifying registered information all the more important.

Positive expectations

- More secure and faster processes for private, business and political procedures and use cases.

- Faster and more secure payment transactions across borders.

- Faster and more secure recognition of certificates, less paperwork.

- If traditional intermediaries such as notaries are not afraid of the technology, it can be used by them to the benefit to all parties involved.

- The possibility of data ownership by citizens.

- Use of the technology in all apps and use cases we know, to secure highly sensitive data streams.

- Cryptocurrency (involving 2nd layer solutions like the lightning network) is said to play an important role in the future of “space economy”.

September/October 2021 “things to know”

- “London” Hard Fork of Ethereum and its resulting positive updates on the one hand and network-issues on the other hand.

- Craziness of NFT selling and buying, and its possible use for money-laundering.

- New regulations planned in regard to KYC, especially by the European Union.

- Meetings and decisions from the SEC (USA) in regard to Blockchain and Cryptocurrencies.

- The China Mining-Ban and its possible impact on mining difficulty.

- Repeating declaration about Bitcoin by People’s bank of China

- Issues with Solana Blockchain (halted for several hours)

- Several major blockchains like btc, ltc have a nearby record in hashrate, transaction volume and new addresses, besides the “Fear/Uncertainty and Doubt” (FUD) coming from the recent China news.

Fraud

Market Manipulation:

- Through a pretense of transfer volume and market capitalization.

- Through tweets and the announcement of news or rumours.

- By buying and selling tokens by whales (people and companies that hold large shares of tokens).

Speculation Frauds:

- Deliberate sale of tokens with no value, for example through ICOs.
- Building supposed financial products around the topic of blockchain, which only aim to scam.
- False promises from trading exchanges.
- Setup of Fake Trading Exchanges.

Technical Fraud:

- Due to the possible installation of fake nodes and wallets.
- Through scam emails and website where you are supposed to enter the private key.
- By intentionally or unintentionally incorrectly programmed smart contracts.