101 Blockchains

# Blockchain Basics

101 Blockchains Flashcards

# Learn the fundamentals of Blockchain through Blockchain basics flashcards and lay the foundation of a bright Blockchain career!

## 1. Blockchain

Blockchain is basically a consensus-based digital ledger that includes immutable, digital data, documented in different packages known as blocks. Every block is 'chained' or related to the next block by leveraging a cryptographic signature or hash function. Thus, blockchain serves as a ledger that you can share with anyone. It is open for access to people with the relevant permissions. It is impossible to change the data recorded on blocks in the blockchain.

## 2. Block

Data is documented permanently on the blockchain network with the help of files referred to as blocks. Block is basically a record of some or all the recent transactions on the blockchain network that have not been added to the network. New blocks are added to the blockchain, and they are not vulnerable to any unwanted modifications. Every block includes information about the recent transactions with reference to the previous block in the blockchain.

## 3. Distributed Ledger

The distributed ledger is a type of database or system of record which you can share, replicate, as well as synchronize across different members in a network. The distributed ledger helps in documenting transactions like the exchange of data or assets between network participants. It also helps in eliminating the time and expense associated with the reconciliation of disparate ledgers. Consensus regarding updates to records helps network participants in ensuring governance.

## 4. Consensus

Consensus is the collaborative effort required from members of a blockchain network to verify the validity of transactions. Consensus is essential in blockchain networks for maintaining consistent synchronization of the ledger. Participants have to agree on a specific transaction and verify its validity before it gets permanently documented in the ledger. Network participants can use consensus to establish rules to facilitate the verification of transactions. Consensus mechanisms are crucial for reducing fraudulent transactions.

## 5. Smart Contracts

Just like usual contracts in the real world, smart contracts are helpful for agreements in the blockchain space. Smart contracts are vital tools for the governance of interactions with the ledger. Most importantly, they enable network participants to execute specific parts of transactions without manual interventions. For example, smart contracts could help in stipulating the changes in the cost of shipping according to the arrival time without any underlying complications or setbacks.

## 6. Mining

Mining is a critical aspect in the blockchain space, and it actually implies the addition of transaction records to the blockchain ledger. Mining involves the use of complex hardware for performing mathematical calculations to ensure proper verification of transactions. Miners receive rewards for creating a new hash for each secure block before adding them to the blockchain. The incentives for mining could include Bitcoins. In addition, miners could also collect transaction fees as incentives for confirming transactions.

## 7. Nodes

Nodes are one of the fundamental aspects required for the operations of blockchain technologies, systems, and networks. They are the distributed computers required for the operations of the blockchain network. Every node in the network has a copy of the whole blockchain. The addition of new users in the blockchain network ensures the distribution of copies of blockchain and access to the blockchain. The data on each node is replicable and could be synchronized and shared throughout all nodes.

## 8. Address

Address, also known as a wallet address, is a long string of alphanumeric characters. The address is a significant requirement for sending, receiving, or holding currency. A blockchain user needs two encrypted keys, such as a public key and a private key, to confirm a transaction. The address for a specific blockchain transaction is public, and users need the private key to verify the validity of transactions. Interestingly, the address could also be available as QR codes.

## 9. Proof of Work

Proof of Work is a consensus algorithm and the most common one at that, used primarily for the Bitcoin blockchain. Proof of Work algorithm ensures that the first miner presenting the 'proof of work' for a block gets the opportunity to validate it. Users can generate POWs by repeatedly inserting transaction data and random strings of digits into a formula. Other miners could verify the POW by applying the concerned input in the formulae.

## 10. Hashing

Hashing is a crucial procedure in a blockchain network repeated frequently by miners. The use of hashing on a Proof of Work blockchain constantly can help in finding a suitable signature. A hash is a function capable of taking an input and rendering output in the form of an alphanumeric string you can identify as the hash value. Every block has a hash value responsible for validating the previous transaction and its own hash value.

## 11. Forks

The concept of forking is also an important addition to blockchain fundamentals. It basically emphasizes creating an alternative variant of a blockchain network. Most importantly, forking is generally deployed intentionally for the application of upgrades to a concerned network. The two common types of forks in blockchain include soft forks and hard forks. Soft forks can create two different compatible chains, while hard forks create a new version of the chain that can facilitate improved participation continuity.

## 12. Double Spending

Double spending is one of the critical issues that blockchain resolves with its basic functionalities and design. The incident of double-spending basically involves a specific user in the blockchain network sending a particular transaction to different recipients simultaneously. Blockchain ensures verification of every transaction, thereby minimizing the risk of double-spending. With subsequent confirmations being added for a specific transaction, the possibility for double-spending in the case of a specific blockchain transaction reduces considerably.

## 13. Digital Signature

The term digital signature is a representation of the conventional paper-based signature. In the case of blockchain, digital signatures refer to the private keys which are essential for signing transactions on the blockchain. Every transaction sent across the blockchain has the signature of the private key of the user. Subsequently, broadcasting the signed transaction over the network with the relevant public key ensures accessibility. Miners could use public keys for signature verification.

## 14. Block Explorer

Just like the internet explorer helps in navigating the massive landscape of the web, a block explorer is a tool that helps in navigating the world of blockchain. It is basically an online tool to explore blockchain networks along with real-time impressions and insights into transactions running on the blockchain. Block explorers are crucial for blockchain analysis as they offer critical information, including total coin supply, transaction growth, network hash rate, and other data points.

## 15. Consortium Blockchain

Consortium blockchain refers to a blockchain that has a controlled consensus process. A specific pre-selected set of nodes is responsible for controlling the consensus process. In the case of a consortium blockchain, the right to read the blockchain could either be public or limited to specific participants. Consortium blockchain also offers hybrid routes like the public root hashes of the blocks along with an API that allows the public to make queries and obtain cryptographic proof.

## 16. Permissionless Blockchain

Permissionless blockchain refers to one in which users don't require permission from any other participant on the network to carry out specific actions. The blockchain design also applies to actions such as joining the network. It is quite clear that permissionless blockchains have public availability with better levels of transparency and decentralization. Permissionless blockchains ensure equal distribution of voting power among all network participants. Litecoin and Bitcoin are prominent and popular examples of permissionless blockchains.

## 17. Permissioned Blockchain

Permissioned blockchains, as the name implies, are completely opposite to permissionless blockchains. Certain nodes or network participants in permissioned blockchains have the power of authority over others. Such nodes or participants could establish validators alongside allowing or denying access to the network. Permissioned blockchains rely on centralized authorities with operations in closed and private ecosystems while sacrificing transparency. Permissioned blockchains are generally suitable for internal business operations. Ripple is a renowned example of permissioned blockchain.

## 18. Fungibility

Fungibility is a clear indicator of the fact that a specific product or asset is identical. Fungible and non-fungible tokens are frequent mentions in discussions across the crypto space. Bitcoin is an example of a fungible token as one Bitcoin will always be equal to any other Bitcoin. On the other hand, non-fungible tokens are not identical to one another. For example, digital collectibles such as CryptoKitties is an example of a non-fungible token with distinct properties.

## 19. Confirmation

Confirmation refers to the number of blocks added over the specific block in the blockchain network. Each added block is referred to as confirmation because all nodes on the network are responsible for indirectly verifying the blocks before it's added. So, a block with 5 blocks added on top of it is likely to have 5 confirmations. More confirmations for a block ensure the reduction of probabilities for modifying a block, thereby facilitating transaction safety.

## 20. Cryptography

Cryptography basically points out the method used for secure communication through the use of code. Many blockchain networks use symmetric-key cryptography to ensure the flexible and easier transfer of cryptocurrencies. The blockchain addresses, tailored for individual wallets, are paired with private keys to enable blockchain transactions. The pairing of public and private keys is essential for unlocking blockchain transactions. Asymmetric-key cryptography depends on a secret private key for message encryption and decryption.

## 21. Halving

Many cryptocurrencies, such as Bitcoin, have a specific supply. Therefore, cryptocurrencies are considered highly scarce digital commodities. For example, in the case of Bitcoin, the total amount of Bitcoin that could ever be issued is almost 21 million. The total number of Bitcoin tokens created for every block would be reduced by half at a gap of four years. The process is known as halving, and the final halving would be completed in the year 2140.

## 22. Decentralized Application

A decentralized application or dApp is an open-source application capable of autonomous operations without any entity having control over the majority of its tokens. The application data, alongside records of information, are stored cryptographically in a public, decentralized blockchain, to avoid central points of failure. Decentralized apps use cryptographic tokens to access the application, alongside generating tokens on the basis of a standard cryptographic algorithm, serving as an indicator of the value contributed by nodes to the application.

## 23. Initial Coin Offering

Initial Coin Offering or ICO refers to the specific crowdfunding mechanisms on the blockchain. The basic idea revolves around ICO points financing new projects through pre-selling coins or tokens to investors who might put their money in the project. ICO is generally preceded by a whitepaper with a description of the business model and technical specifications regarding a project. In addition, entrepreneurs can also set a timeline and target budget for the project.

## 24. Lightning Network

A lightning network refers to any decentralized network that uses smart contract functionality to allow instant payments throughout a network of participants. Lightning networks can facilitate instant blockchain transactions without any concerns regarding block confirmation times. It supports the execution of millions of transactions in a matter of seconds, at low costs, even for different blockchains. The lightning network protocol in blockchain applications is a promising solution to the pressing issues of blockchain scalability.

## 25. Mining Difficulty

Mining difficulty is a crucial element in the functioning of blockchains. It points out the extent of difficulty in finding out the next block in a blockchain. Each proof of work consensus algorithm features a specific mining difficulty that could also be adjusted accordingly. The number of miners joining the network has a profound impact on the growth or decline of the difficulty level.

## 26. Token

A token is a digital representation for any entity that could be owned. Traditionally, tokens have been identified as meta-information that you can find encoded in basic blockchain transactions, capitalizing on the immutability in the blockchain. In the case of Bitcoin, tokens worked as outsourced extensions to core protocol at the protocol layer. Modern tokens feature complicated smart contract systems alongside permission systems and associated interaction paths. Tokens are subject to governance through a specific set of rules.

# 101 Blockchains

**101 Blockchains is the world's leading research-based platform built for Enterprise Blockchain Professionals, with a thriving community of over 25,000 professionals.**
**101 Blockchains offers world-class training courses and industry-recognized certification programs that are helping professionals all over the world upgrade their skills and accelerate their career growth.**

**Check out our collection of 101 Blockchains Flashcards. Gain further knowledge about blockchain technology with in-depth guides and blogs. Find world-class professional training courses.**