Blockchain

Research document

Table of Contents

[**Structure**](#_gkk42h5ynnxe) **3**

[Blockchain](#_5c4vpnl786o4) 3

[Blocks](#_nptdzuwk03f2) 3

[Side Chain](#_wzel425k1y59) 4

[Decentralization](#_9by21vpcwmg9) 4

[Openness](#_x05zvinldtgu) 4

[**Consensus Mechanism**](#_flw04am7pb6n) **5**

[Proof of Work](#_2vey4qoqsmuq) 5

[Proof of Stake](#_khmngzn9y0t2) 5

[Proof of Authority](#_7a6zeq5w96o9) 5

[Proof of Capacity](#_bxopx9rh957k) 5

[**Mining**](#_be6p87mowd2u) **6**

[Hashing](#_s8srlfre1mh4) 6

[Nonce](#_wjx4rhjum333) 6

[Example](#_e57euy5wffyv) 6

[**Blockchain Explorer**](#_4imcf852a5ho) **8**

[Introduction](#_wu2igj5t0mpd) 8

[Exploration](#_j6uu7g6y0rgo) 8

[Block](#_ajqibi605rro) 9

# Structure

## Blockchain

A blockchain is a distributed ledger, similar to a database, but rather than being controlled by a central authority (Google, Facebook, small company, individual etc.) the ledger is dispersed across multiple computers. It can be run by anyone with an internet connection. The blockchain is a ledger through which data is added and updated in real-time via consensus of the different nodes running the software in the network.

Once data is added to the ledger, it cannot be removed or edited like with a database.

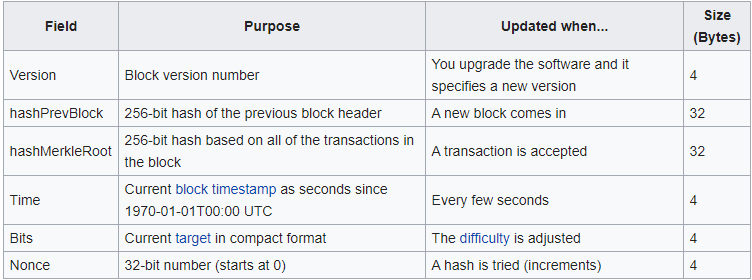
## Blocks

A blockchain consists of multiple blocks that are chained together and contains a cryptographic hash of the previous block, a timestamp and transaction data. Blocks are files where data pertaining to the network are permanently recorded. A block records some or all of the most recent transactions that have not yet entered any prior block. You can see a block as a page of a ledger or record book.

A block contains multiple variables.

The block header contains:

* The block version number
* A timestamp
* The hash from the previous block header
* The hash of the Merkle Root
* The nonce
* The target hash



## Side Chain

Sidechains are cryptographically independent ledgers (blockchains) that link to the main chain...

## Decentralization

## Openness

# 

# Consensus Mechanism

Public blockchains that operate decentralized work on a global scale without any single authority. These blockchains depend on contributions from participants who work on verification, authentication of transactions and mining occurring in the blockchain.

## Proof of Work

Proof of Work (PoW) is a common consensus algorithm used by cryptocurrency networks like BitCoin and Litecoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.

## Proof of Stake

A Proof of Stake (PoS) is a low-cost, low-energy consuming consensus algorithm alternative to PoW.

The block producers are called validators. These validators lock up some of their cryptocurrency as a stake. One of these validators gets chosen based on a selection algorithm that takes their stake (or deposit) into account.

The higher the stake, the more chances the validator has to get selected. Once selected, the validator has the exclusive rights to create a block. The validators that are not chosen do not waste energy doing any computive work.

If the validator misbehaves, it will lose their stake. Therefore, the validator has a good reason to behave honestly.

## Proof of Authority

## Proof of Capacity

# 

# Mining

Adding transactions to a blockchain requires substantial computing processing power. The miners, both individuals and companies, who process blocks are compensated only if they are the first to create a hash that meets a certain set of requirements, called the target hash.

This target hash is a number that a hashed block header must be less than or equal to in order for a new block to be awarded. The target hash is determining the difficulty of the input. The difficulty is adjusted once every x blocks as a function of how much hashing power has been deployed in total by the miners in order to ensure that blocks are processed efficiently..

Successfully mining a block requires the miner to be the first to guess the nonce in the block header. When the hash meets the target hash, the block is added to the blockchain.

## Hashing

A hash is a series of numbers and letters that are deterministic generated, meaning that it will produce the same result each time the same input is used. It also means that the function can generate a hashed input efficiently, it makes determining the input difficult (this is where mining comes into play) and makes small changes to the input result in a very different hash. This complex system creates the privacy net of blockchain.

## Nonce

Nonce (number only used once) is a random string of numbers added to a encrypted or hashed block in a blockchain that, after being rehashed, meets the difficulty level restrictions.

The nonce in blockchain context refers to the first number a blockchain miner needs to discover before solving for a block in the blockchain. Trying to find this solution is also referred to as proof of work. When a miner successfully found the solution, the blockchain miner is offered cryptocurrency in exchange.

A nonce is difficult to find and is considered a way to weed out the less talented crypto miners.

## Miner Reward

A miner reward is awarded to the miner that successfully mines a block in cryptocurrency. It is calculated by the defined reward set by the blockchain owner plus the total fee of transactions.

## Example

* Reward is 2
* Transaction fee is 0.1
* Number of transactions = 499

1. The miner gets 499 transactions from the queue that need to be verified. This will be put into a list of transactions.
2. The miner’s wallet address will be added first in the list of transactions.
3. The miner solves the nonce.
4. This solution for the nonce is accepted by the network of nodes.
5. The miner reward will be calculated. 2 + (499 \* 0.1)
6. The miner will get rewarded with the miner reward.

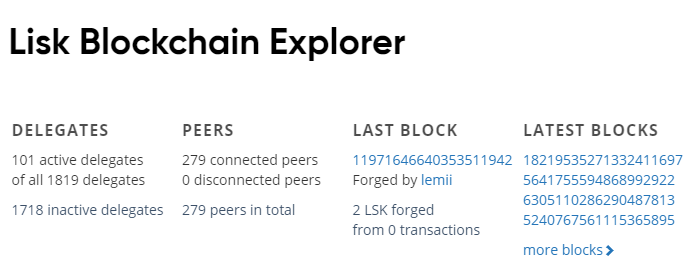
# Blockchain Explorer

## Introduction

A blockchain explorer lets you browse through a blockchain, using an explorer will allow users to “explore” the entire blockchain of the platform you are using. This can only be done for the blockchain structure that the explorer is built for, you cannot for example browse through a litecoin blockchain using a Bitcoin block explorer. The block explorer provides users with all the necessary information of all transactions within the block, for example information about it’s status, sender, recipient and time.

## Exploration

For this example we will use the block explorer from lisk.io, this explorer can be found at : <https://explorer.lisk.io/>. When we access the website we get presented with an overview of the latest mined blocks. We can select a block to get more information about a block.

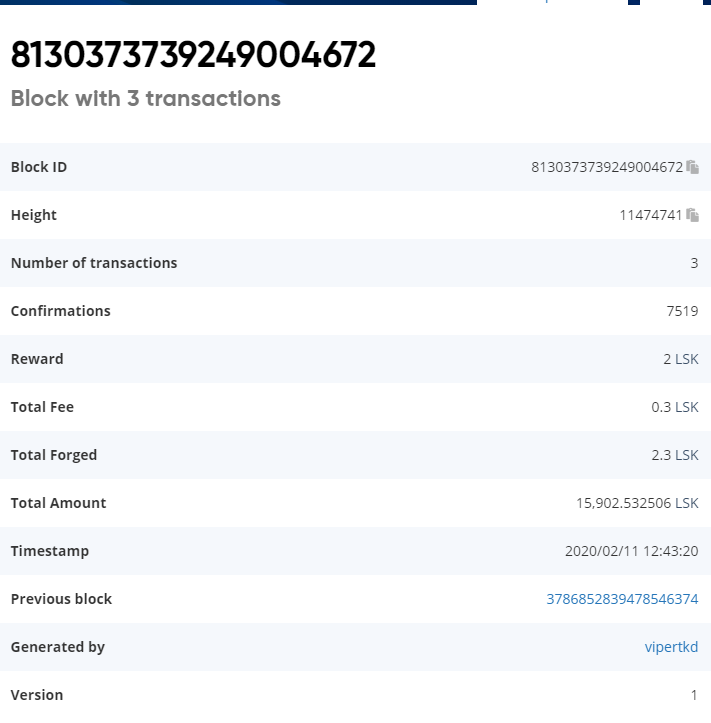


### 

### Block

For this example we will look at the block found at <https://explorer.lisk.io/block/8130373739249004672>.

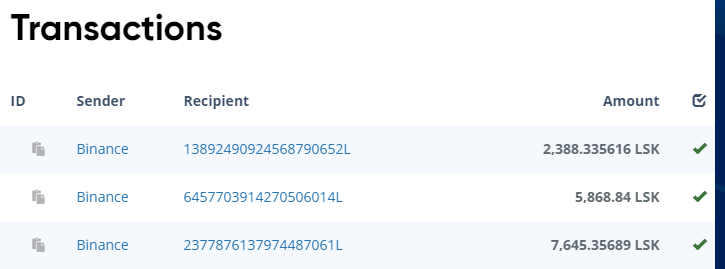
The overview contains information about the block. General information consists of the size of the block, amount of transactions within the block and who has forged the block.



Most of the information found within the block is pretty self explanatory. Features are Height, this indicates the number of blocks between this block and the genesis block. The amount of confirmation indicates how many blocks have “confirmed” this block, in other words how many new blocks have been generated after this block and have confirmed that this block is correct. The reward indicates how much of a specific currency the user who forged the block has received for forging the block, this in combination with the transaction fees for each transaction contained within the block forms the total reward for the user.

Because each block proceeds a previous block leading all the way back to the first one we can use the link to the previous block to go as far back as we please if necessary.

Each block also contains a list of transactions, this can also be empty if there were no transactions available in the transaction queue at the time of creation of the block.



Within each transaction we can find who the sender was and who has received the transaction. We also find the amount of currency that has been sent during the transaction.

Before a transaction is finalised the block has to be confirmed a specific amount of time, in this case we use Lisk which needs 101 confirmation to fully process a transaction.

Our block has been confirmed over 7500 times, so all transactions are processed already.



If we look at a more recently created block containing transactions we can see that this one has been processed but has yet to be confirmed enough times to fully complete the transaction.

