Blockchain & Lisk Research Document

# Table of Contents

[**Table of Contents**](#_8vtrm02212ti) **2**

[**What is a blockchain and how does it work?**](#_21imj3ny6iks) **3**

[How does Lisk work?](#_tpkk1fftaxd8) 5

[Nodes](#_zgvg5zihr03d) 5

[Delegates](#_5l3wzqjn7n2q) 5

[Sidechains](#_lytepzhf3djs) 5

# What is a blockchain and how does it work?

A blockchain is literally a chain of blocks. These blocks consist of digital information, specifically for cryptocurrency, these blocks store information about transactions.

The information that is stored in a block can, among other things, be the date, time, sender, receiver, and amount of coins transacted. Just like a normal register of a transaction in a blockchain information about the sender and receiver is included in the transaction. Although whereas conventionally real information is used, in a blockchain a digital signature is being used. To distinguish blocks from each other, unique information is stored in them. A nonce (number only used once) is an example of this unique piece of information.

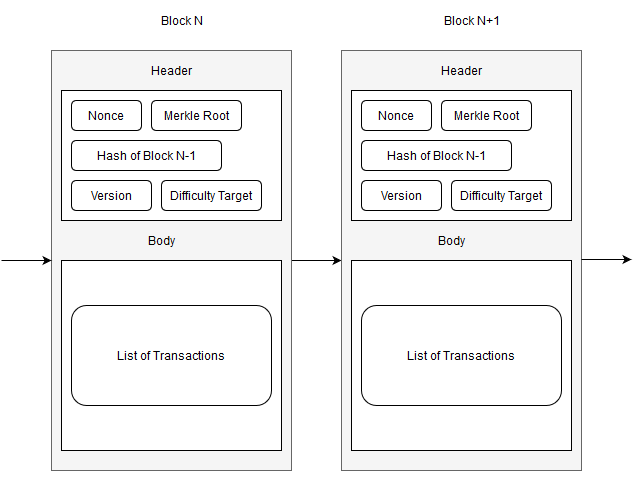
To quickly identify a block a header is used. In the header information is being stored about the block. The block header consists of the following pieces of information:

* Hash of the previous block
* List of transactions in a merkle tree
* Nonce
* Timestamp in unix time
* Version of the block

Every blockchain technology is free to make their own version but you'll find that these pieces of information are generally put in the header.

Along with the header is the body, the body consists of a list of all transactions for that block.

Visual representation of a blockchain:



The way a block is secured is called a consensus model. There are many different ways a ledger can be secured. For Bitcoin for example, Proof of Work is used. The model of consensus decides who is allowed to sign a block and add it to the ledger. The idea behind this is that the who changes regularly and therefore keeps the system decentralized, it also motivates people to contribute to the ledger by rewarding them with a payout when they forge a new block.

## How does Lisk work?

The Lisk network and their currency LSK is a blockchain application platform. It is specially made for applicatie that use blockchain technology.

### Nodes

Nodes are used for multiple things, they forge new blocks, keep track of the ledger and verify blocks added to the blockchain by other nodes. Nodes are implemented to improve trust in a system, they create stability due to the decentralization that they provide. A node also provides a private entrypoint into the network.

A node uses the public key of a delegate to sign a block in the blockchain. Other nodes in the network then add this block to their ledger.

### Delegates

Becoming a delegate means that an account becomes available to sign a block, you are not required to run a node when becoming a delegate.

The reason to become a delegate is mainly to earn LSK. Only the top 101 are able to earn money by signing. Becoming a delegate on the lisk network costs 25 LSK. Because they have invested in the network they have a form of commitment to the network. LSK losing value means that they earn less and also means that their total wallet is worth less.

Voting on delegates costs LSK, for every 33 votes/unvotes a transaction of 1 LSK is required. The 101 delegates with the most votes are used to sign blocks.

### Sidechains

A sidechain is an independant blockchain that is linked to the main chain that it is based off. This is done by a technique called two-way-pegging. This links the side chain to the mainchain. Using this technique provides the possibility to transfer currency from the sidechain to the mainchain, this has an exchange rate. This amount is subsequently locked on the mainchain, this locked amount of currency is released as soon as another transaction from the side chain is transferred to the mainchain.