Lyncoin (LCN)

A Peer-to-Peer Electronic Cash System Based on Cryptography

Revison: 3, Date: February 12, 2024

Website: Lyncoin.com

Twitter: @lyncoin1

Abstract

Chain Type: AuxPoW

Proof-of-Work Algorithm: SHA2-256D (Bitcoin)

Block Time: 1 Minute

Halving: Not Halving, reduced by 1% every 43200 blocks (approx. 30 days)

Start Date: December 31, 2022

Block time was initially 10 minutes with a block reward of 21000 LCN; after block height 71700, the block time was reduced to 1 minute and the block reward was divided by 10. For the current block reward and the amount of supply in circulation, please check the Explorer.

Introduction

Lyncoin is a digital currency that operates without intermediaries or central authorities. Transactions are recorded on a public ledger called the blockchain, which is enforced with cryptography. Lyncoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. Transactions are broadcast to the network and usually begin to be confirmed within 1 minute, through a process called mining. Mining is a distributed consensus system that is used to confirm pending transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks.

Transactions

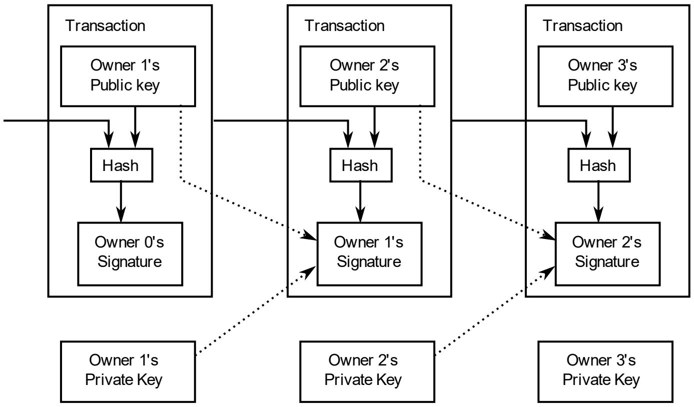
Lyncoin transactions are messages that indicate the transfer of lyncoins from one user to another. These transactions are secured using cryptography and are broadcasted to the entire Lyncoin network for verification. The transaction information is publicly available on the blockchain, which is a digital ledger. The history of each Lyncoin transaction can be traced back to the point where the lyncoins were first produced or mined.

Each transaction has a unique digital signature that verifies the authenticity of the transaction and ensures that the lyncoins being transferred belong to the sender.

The transaction is then verified by other nodes in the Lyncoin network. Once the transaction is verified, it is added to the blockchain, which is a public ledger of all Lyncoin transactions.

Miners process Lyncoin transactions and are rewarded with newly created lyncoins for their work. Miners compete to solve complex mathematical problems in order to validate transactions and add them to the blockchain. This process is known as mining, and it is what makes the Lyncoin network secure and decentralized.

The diagram provides an uncomplicated explanation of how transactions operate within Lyncoin's network.



Coinbase Transaction

A coinbase transaction is a unique kind of transaction that creates new coins and pays miners for validating the blockchain. It does not have any inputs, but it has one or more outputs that specify the addresses that will receive the block reward. A coinbase transaction is typically the first transaction in a new block.

Keys

Lyncoin uses a cryptographic system called public-key cryptography, which involves two kinds of keys: public keys and private keys. Public keys are known to everyone and used for identification, while private keys are secret and used for encryption and authentication.

Private keys are used to generate public keys with a mathematical function named the Elliptic Curve Digital Signature Algorithm (ECDSA). Private keys are 256-bit numbers that are randomly created and can be used to sign transactions, showing that they are from the wallet's owner.s

The signature also makes sure that the transaction cannot be changed by anyone after it is sent. Public keys are then used with a hash function to make the public address that Lyncoin users use to transfer and receive money. A hash function is a function that takes an input and gives a fixed-length output that is difficult to invert.

The public address is a shorter and easier version of the public key that can be given to others. The key system in Lyncoin makes sure that only the owner of the private key can use the lyncoins linked to the public address, and that the transactions are checked by the network using the public key. The key system also allows the creation of many addresses for each user, improving privacy and security.

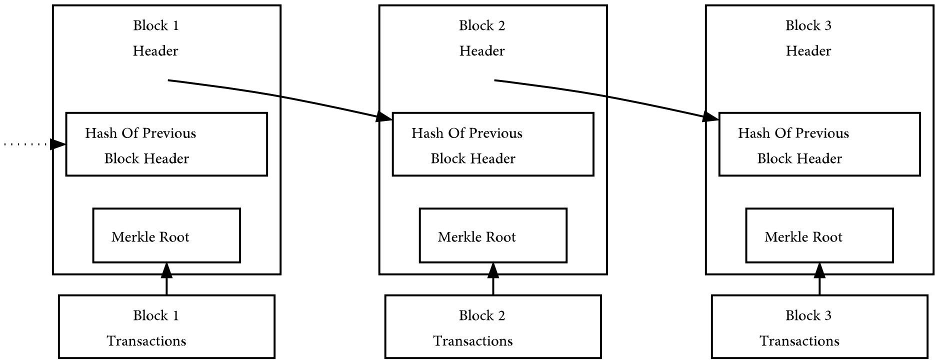
Mining

Lyncoin mining is the way of confirming transactions on the blockchain and generating new lyncoins. Miners use powerful devices and programs to crack hard math problems that approve blocks of transactions. The miner who solves the problem first gets a prize in Lyncoin. Mining also makes the Lyncoin network safe and distributed.

Auxpow, which stands for auxiliary proof of work, is a method of mining several cryptocurrencies simultaneously, using the same computing power. It lets a miner send the same work to different blockchains, and get rewards from all of them. The blockchain that does the real mining is the parent blockchain, while the ones that take its work are the auxiliary blockchains. Auxpow helps smaller blockchains boost their security by using the computing power of bigger ones.

Block

A block is a way of storing data about the transactions that happen on the Lyncoin network. It has two parts: a header and a list of transactions. The header has a code that links it to the previous block, a time stamp, a difficulty level, and a random number. The network nodes check the transactions and add them to the block. A miner creates a new block by solving a math problem using the header and shares it with the network. The blockchain is a chain of blocks that acts as a record of all Lyncoin transactions.

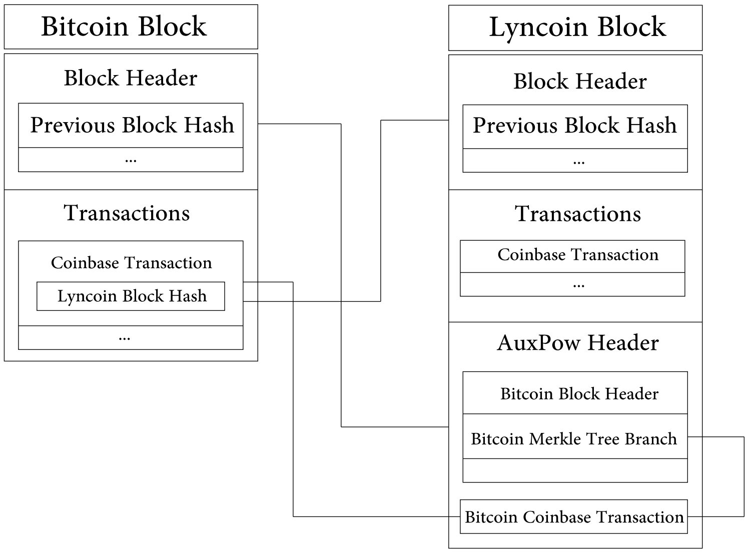


Simplified Proof of Work Block Chain

Merged mining is a technique that lets you mine more than one cryptocurrency at once without losing efficiency. Auxpow blocks are special blocks that enable this technique. They use the work done on a main blockchain (the parent blockchain) as valid proof of work for another blockchain (the auxiliary blockchain). This way, miners can protect multiple chains with the same computing power and get rewards from both.

For instance, Lyncoin is an auxiliary blockchain that takes auxpow blocks from Bitcoin, the main blockchain. This means that Bitcoin miners can produce both Bitcoin and Lyncoin blocks at the same time, and Lyncoin nodes can confirm the blocks by looking at the Bitcoin proof of work.

An auxpow block looks like a normal block, but it has some extra data between the nonce and txn_count parts.This data has the coinbase transaction and the merkle branches that connect the auxpow block to the main block and the other auxiliary chains.



Peer-to-Peer Network

When a new core wallet starts, it lacks knowledge of active full node IP addresses. To find these addresses, the node queries hardcoded DNS seeds maintained by the team. DNS seeds respond with IP addresses of full nodes willing to accept new connections. Once connected, peers exchange addr (address) messages, sharing IP addresses and port numbers. This decentralized process facilitates peer discovery. Lyncoin Core maintains a record of known peers in an on-disk database. Peers can send addr messages to propagate IP addresses of other peers. This fully decentralized approach ensures that nodes discover each other independently, reducing reliance on DNS seeds. Lyncoin is using the default port 5054 for the main network.

Smart contracts

A Lyncoin smart contract is a software code stored and executed across all nodes in the Lyncoin blockchain network. The smart contract creator defines the rules and negotiates them with the involved parties. Once saved on the blockchain, the contract remains there permanently, and its code remains unchanged. The Lyncoin ledger ensures security and immutability by replicating and storing the agreement. Beyond defining agreement rules, blockchain smart contracts allow for automatic execution of those rules or other obligations. No central authority or intermediaries are necessary for seamless software functioning. Lyncoin smart contracts offer transparency and can scale efficiently. They avoid expensive intermediaries. Execution occurs swiftly due to automation. The blockchain ensures tamper-proof execution. Once recorded, the contract remains unchanged. Lyncoin Smart contracts follow predefined rules without errors.

Team

While our website does provide information about our team, we maintain a deliberate veil of anonymity. Our team members prefer to operate behind the scenes, allowing their work to speak for itself. This approach grants us flexibility and strategic advantages, while still ensuring that our project remains transparent and accessible to our users. Anonymity allows developers to make project decisions without worrying about reputational risks or public scrutiny. They can focus on creating a great project without external pressure.

Chat Links

Telegram: https://t.me/lyncoingroup

Discord: https://discord.com/invite/UNJFYkz2a2