Blockchain Council™

Blocks, Wallets and Addresses

Blocks

A block is the fundamental unit of a Blockchain.

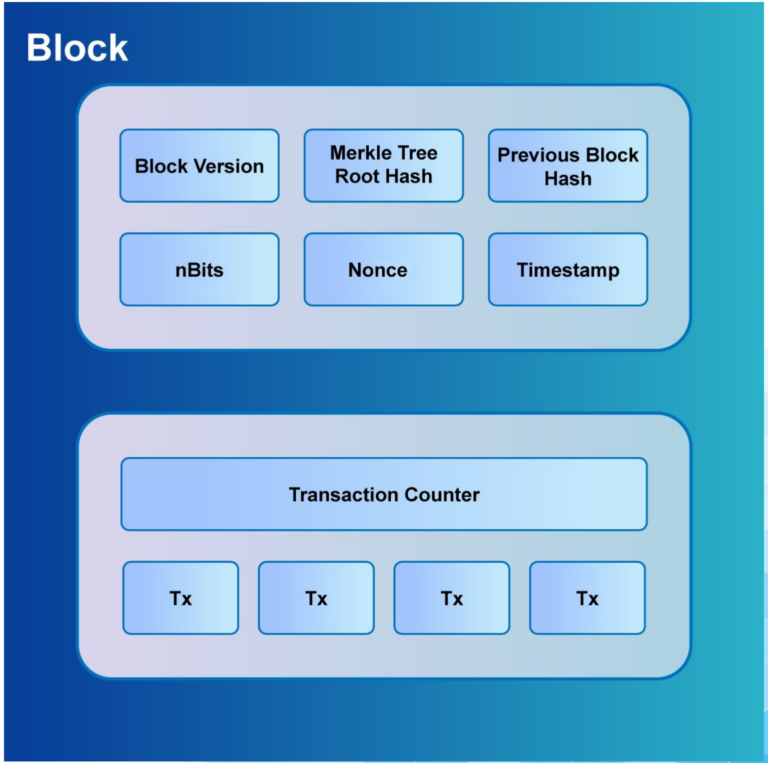
A block is divided into:

- Block header
- Block body

The block header is divided into six components:

- Version number
- Previous block hash
- Merkle tree root hash
- nbits
- Nonce
- Timestamp

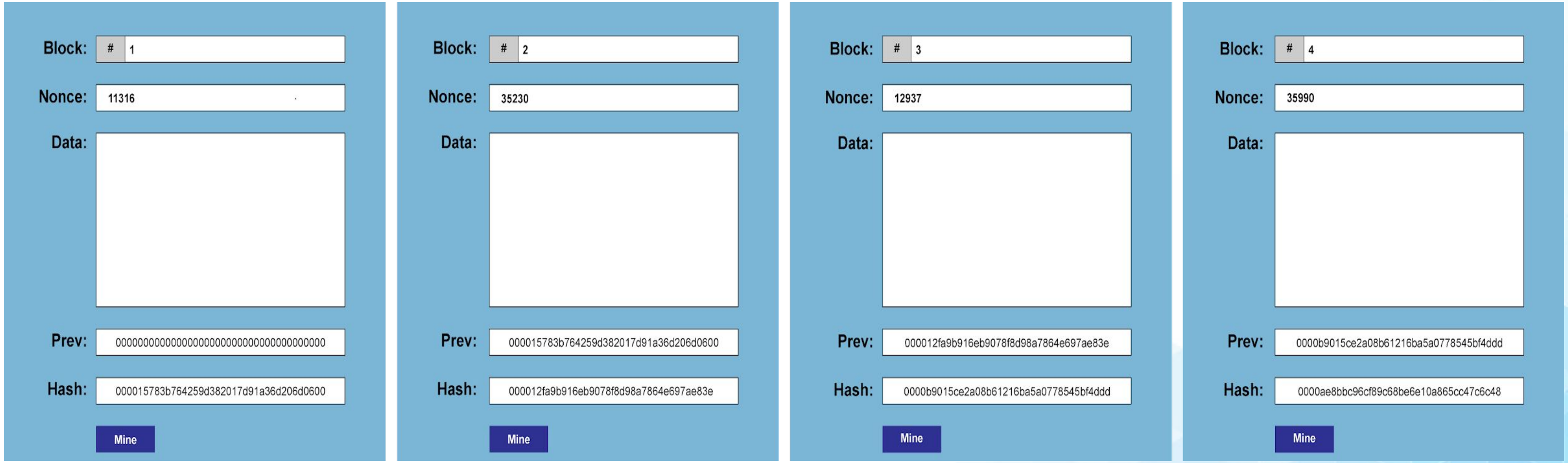
Block body contains all the transactions.



Blocks

Every block contains a hash of all the previous blocks.

Blocks use merkle tree to store the hash of all the transactions to create the hash of block.



Block: # 1
Nonce: 11316
Data:
Prev: 00000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600
Hash: 000012fa9b916eb9078f8d98a7864e697ae83e

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae83e
Hash: 0000b9015ce2a08b61216ba5a0778545bf4ddd

Block: # 4
Nonce: 35990
Data:
Prev: 0000b9015ce2a08b61216ba5a0778545bf4ddd
Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c48

Wallets

- A Blockchain wallet is a software program that enables users to buy, sell, and monitor balance for their digital assets and record the transaction done using the wallet address..
- A wallet stores private and public keys for a user. As the name suggests, public key is shared and works as the address while private key is kept private.
- Public and private keys are used to encrypt and decrypt transaction so only the intended recipient can know the transaction data.
- The wallets can be:
    - Software wallets like Metamask which runs on a machine.
    - Hardware wallets are storage devices on which users can store their keys.
    - Paper wallets are just writing down your public and private key on a paper and keeping it someplace safe.
- A Blockchain wallet offers all the features available for safe and secure transactions and exchanges of funds between various parties.

Blockchain Wallet Features

- **Ease of use -** Blockchain wallets work in a similar way as the wallets that you use for your everyday purchases.
- **High security -** Wallets are secure from most malicious actions as long as the private key is secure.
- **Enables instantaneous transfers across geographies -** With the decentralized nature, blockchain wallet can transfer Cryptocurrency across the globe.
- **Low Transaction Fees -** There is a significantly smaller cost of exchanging funds than the conventional banks.
- **Enable multi-cryptocurrency transfers -** It makes you do basic currency conversions.

Wallet Types

There are two types of wallets used in Blockchain:

Hot Wallet: Hot wallets are online wallets through which it is easy to quickly transfer cryptocurrencies. Private keys in the hot wallet are stored in the cloud for quicker transfer. Hot wallets can be easily accessible 24/7 online and can be accessed from a laptop or mobile computer, but if compromised, there is a chance of unrecoverable theft.
Examples: **Coinbase** and **Blockchain.info**

Cold Wallet: Cold wallets are offline digital wallets where the transfers are digitally signed and then electronically disclosed. Private keys are kept in independent hardware that is not connected to the internet or the cloud, but stored on a paper document. The cold wallet transaction approach helps to shield the wallet from unauthorized entry.
Examples: **Trezor** and **Ledger**

Address

- A Blockchain address is used to identify a user on blockchain network. It is a special sequence of numbers, letters, and functions.
- It applies to a particular network destination where it is possible to transfer the cryptocurrency.
- An address is a placeholder to accept and send blockchain transactions.
- Pay-to-IP had been abandoned in Bitcoin. Pay-to-Public Key Hash became the new standard format for Bitcoin addresses.
- Public keys are generally used to create an address for a user. The steps to create an address include:
  - Hashing of public key using SHA 256
  - Re-hashing using RIPEMD-160
  - Adding “00” prefix
  - Adding checksum bytes at the end
  - Encode the result with base58 encoding

Blockchain Council™

THANK YOU!

Any Questions?

Visit

community.blockchain-council.org

Mail Us

hello@blockchain-council.org