Blocks, Wallets and Addresses

Blocks

A Block is the the smallest unit of a blockchain.

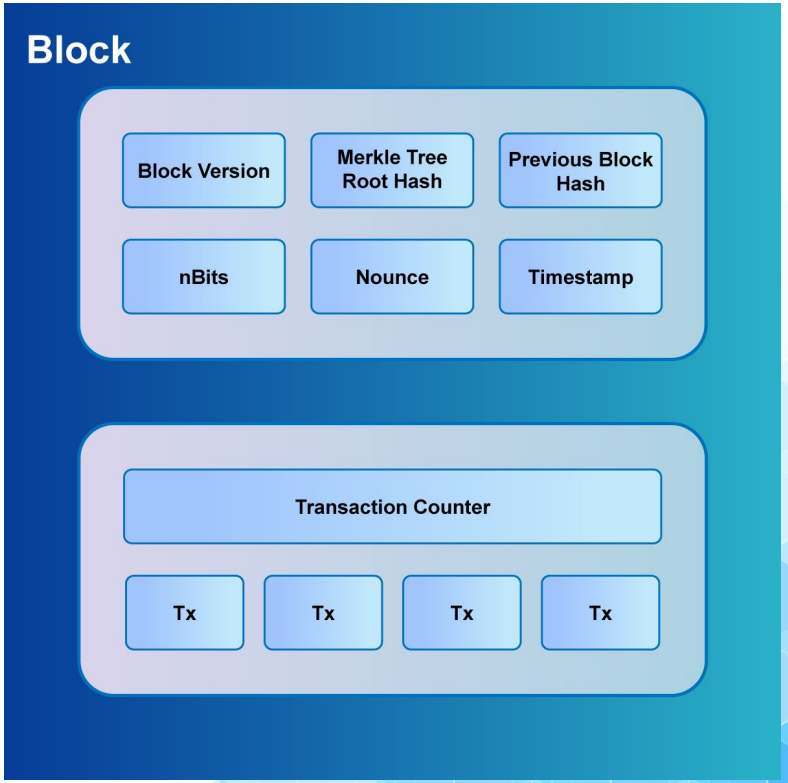
Block is differentiated into:

- Block Header
- Block Body

Block header is divided into six components:

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

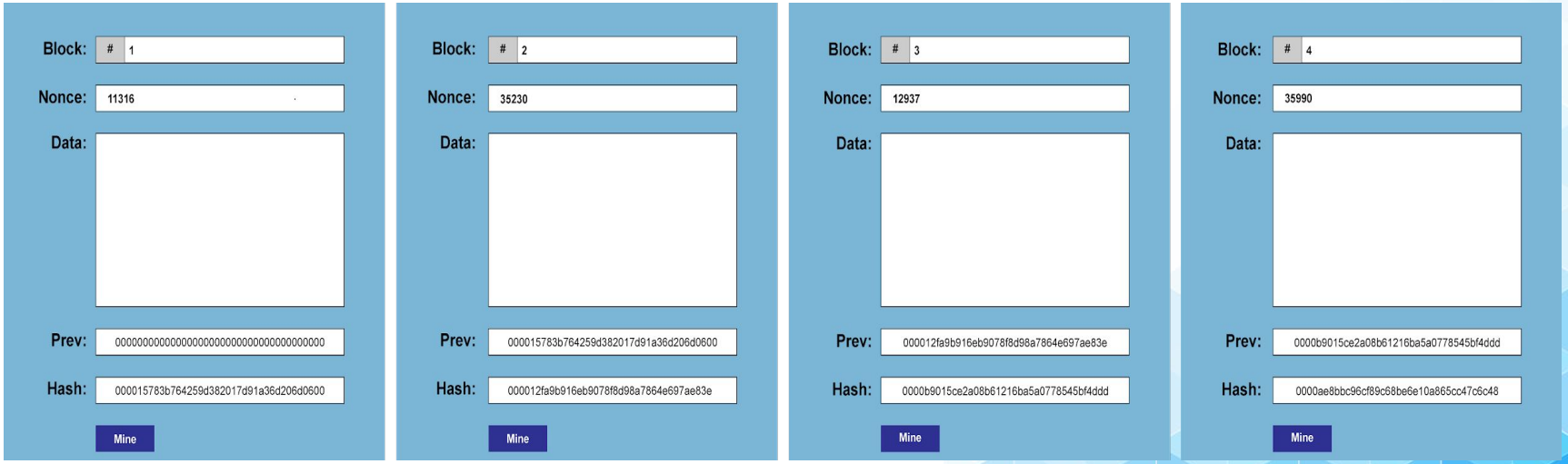
Block Body contains all the transactions.



Blocks

Every block contains a hash of the all the previous block.

This has the effect of generating a series of blocks from the genesis block to the present block.



Wallets

A blockchain wallet is a software program that enables users to buy, sell, and monitor balance for their digital currency or assets.

A wallet stores private and public keys for a user.

A blockchain wallet allows anyone to quickly share assets. Transactions, as they are signed cryptographically, are safe.

The wallet can be accessed from web browsers, even from the mobile phones, and the user's privacy and identities are protected.

A blockchain wallet offers all the features available for safe and secure transactions and exchanges of funds between various parties.

Blockchain Wallet Features

Simple to use - It's almost like the other app or a wallet that you use for your everyday purchases.

Completely secure - Wallet is said to be secure as it keeps your private key secure.

Enables instantaneous transfers across geographies - Transfer of funds do not have any geographical barrier.

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 wallet 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 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 pretty much like an email address which is a special sequence of numbers and letters and functions.

It applies to a particular network destination where it is possible to transfer the cryptocurrency. The idea is to send a person a unique address every time he or she receives crypto.

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.

A standard P2PKH address has something like 34 signs and starts with a “one”.

If you paste an address in your bitcoin wallet, it scans the prefix and calculates the checksum. It refuses the address if it doesn't fit. It is difficult to transfer funds to an incorrect address because of a typing mistake.