Accounts, Blocks, Transactions and Merkle Trees

Blockchain Accounts - Private Key

- In general once you create an account on Blockchain, you will get a Private Key and a public address.
- Private Key is used to generate a signature for each transaction over the blockchain.
- The generated signature is used to confirm that the transaction has come from a specific user, and also prevents the transaction from being altered by any malign entity.
- In simple words - “Private Keys are used to sign the cryptocurrencies you send to others.”
- Example: **L34EXrFCuxQCorfE66sxQe8Tyh71SyU8cc9z7HnbEWwW8YsgbvTw**

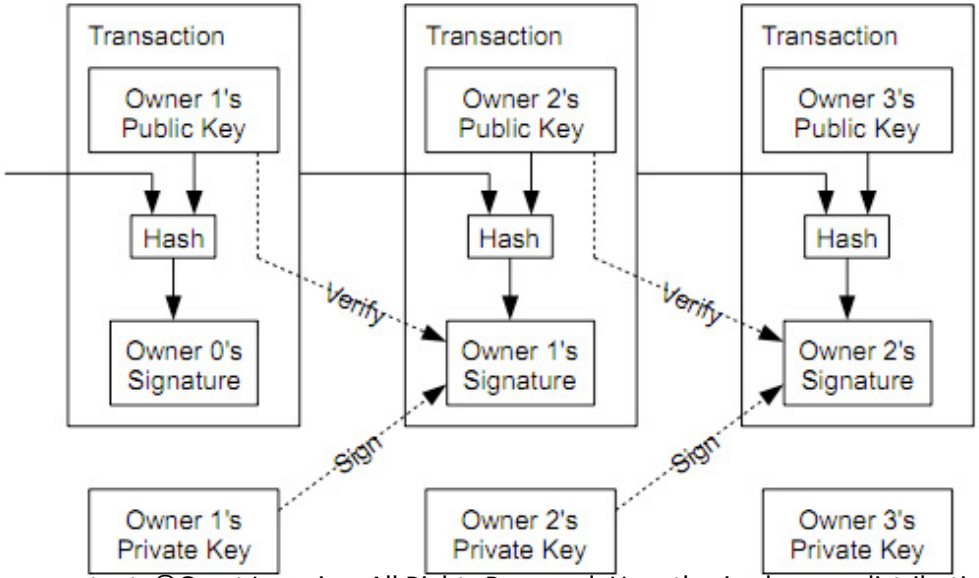
Blockchain Accounts - Addresses

- A cryptocurrency address in a core is a representation of the public key.
- One-way cryptographic hash functions are used to derive address from the public key.
- For example in Bitcoin, the algorithms that are being used to generate a bitcoin address from the public key are the Secure Hash Algorithm 256 (SHA-256) and the RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160)
- The address appears typically in a transaction between two parties, with the address signifying the recipient of the funds.
- Example: **1JPgMJuAvYJU6mxxbJdmf1XBd7bBPdPV3a**

Transactions

- Transactions are records of data in chronological order
- Transactions are stored in a Merkle tree inside the Block.
- The transactions, when submitted, are picked up by the blockchain network and is inserted into a ‘pool of unconfirmed transactions.’ The transaction pool is a collection of all the transactions on that network that have not been confirmed yet.
- Miners on the network select transactions from this pool and add them to their ‘block.’
- Transactions also contain metadata information which can be utilized to store data over the Blockchain.

Transactions



Source: https://bitcoin.org/bitcoin.pdf

Blocks

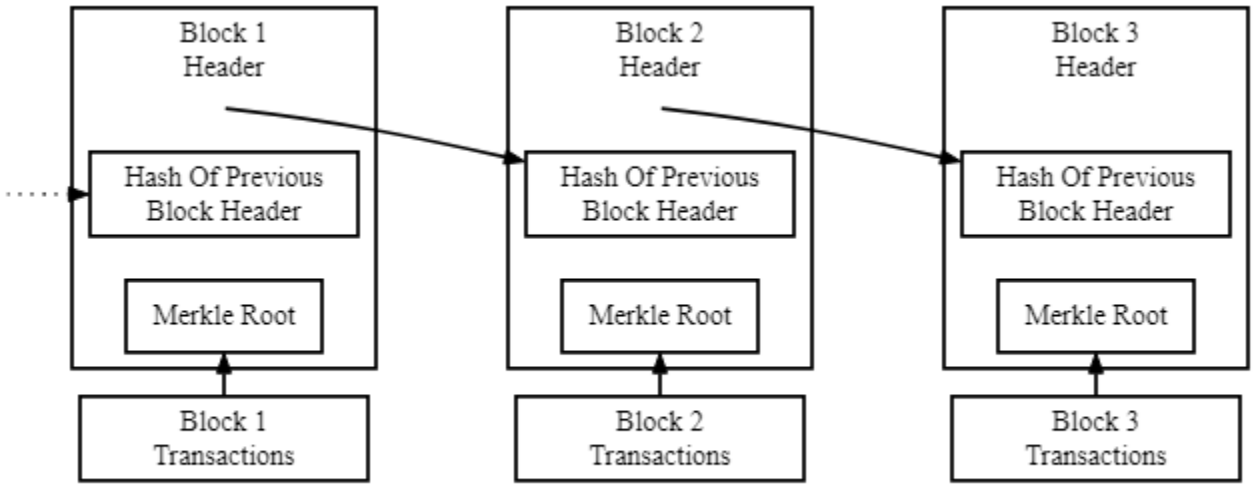
- A Block is a container data structure which contains a set of confirmed transactions.
- A block could contain different information, and a chain of these blocks evolves into a blockchain as long as it links one and the other.
- The blocks are stored on the hard drives of many miners spread across the globe on a peer to peer network.
- In the Bitcoin algorithm, a block is created every 10 minutes. All the transactions happening over the network within 10 minutes interval are crunched into that block and added to the chain.

Structure of Blocks

All blocks in the Blockchain are composed of a header, identifiers and a long list of transactions. The structure of a block is as follows:

- Block Header
- Block identifiers
- Merkle Trees

Blocks



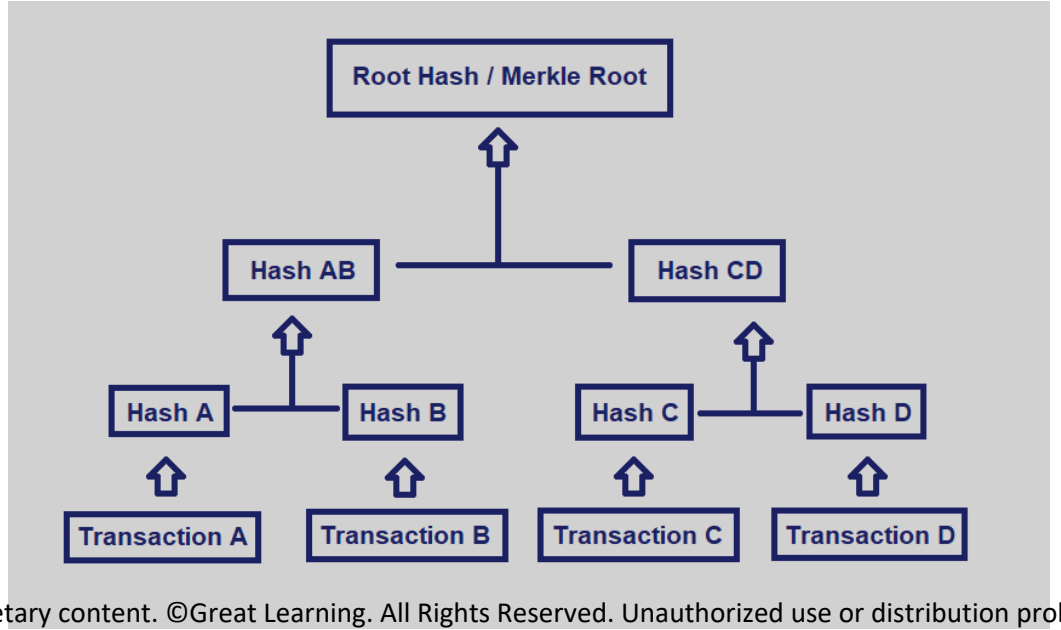
Simplified Bitcoin Block Chain

Source: https://bitcoin.org/en/blockchain-guide

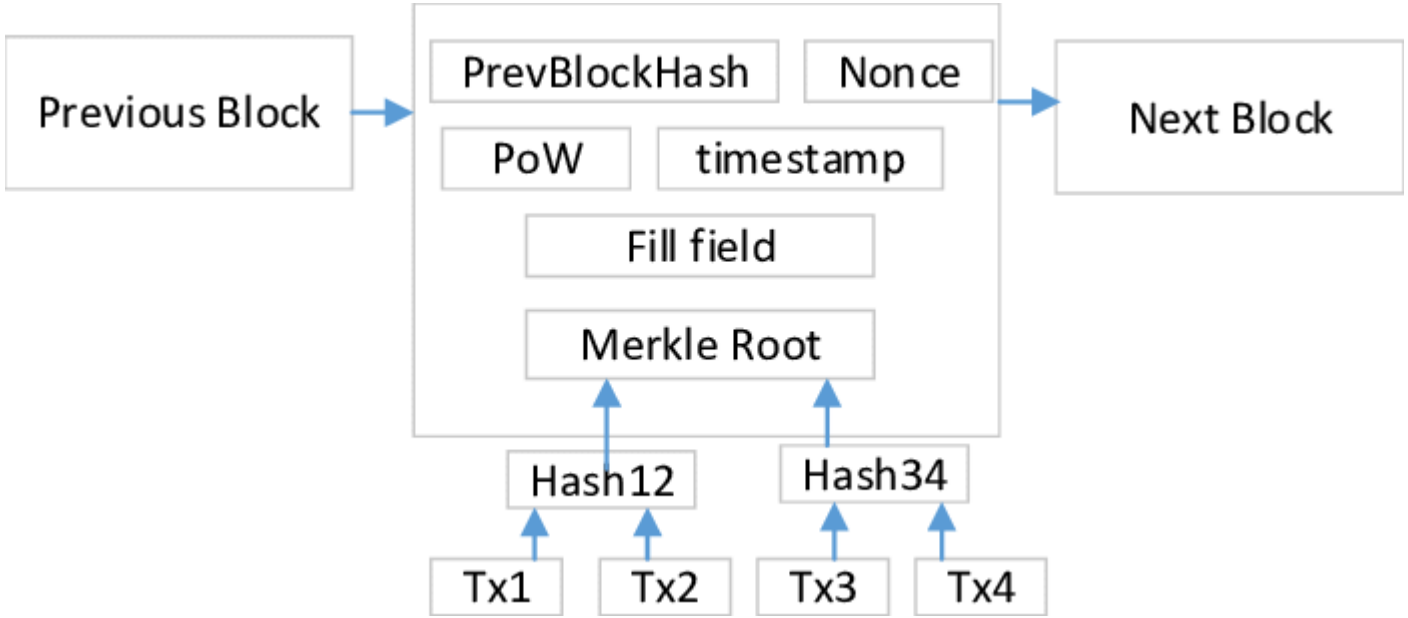
Example of Bitcoin Block

Field	Description	Size
Magic No	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction Counter	positive integer VI = VarInt	1 - 9 bytes
Transactions	The (non empty) list of transactions	Transaction counter-many transactions

Merkle Tree



Merkle Tree with a Block



greatlearning
Learning for Life

Thank You