



# What is Blockchain?

# What is Blockchain?

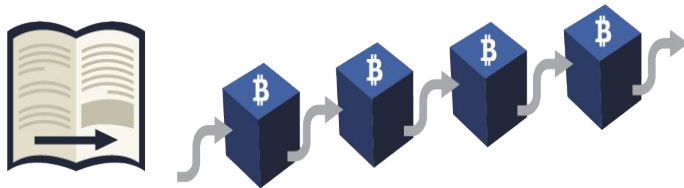
- Blockchain is a transaction record database that is distributed, permission less and maintained around the world by a network of nodes.
- Blockchain has a distributed group of nodes that oversee the network.
- Blockchain uses decentralized technologies to provide **peer-to-peer, permissionless, and immutable network** to store transactions.
- Some real-life examples:
  - Records of sale and purchase of raw material
  - Bank account statements
  - Excel sheets tracking hospital equipment
  - A simple record-keeping book

# Understanding the Book Analogy

Consider Blockchain as a traditional book based ledger, where:

- Each page refers to a block connected to the previous page through a page number.
- Entries of credit and debit on the book is the list of transactions on the blockchain.
- It is easy to detect if a page/block has been altered or deleted.
- Any changes in the book needs the consent of all the involved parties.
- It is impossible to tamper a previous entry in the ledger without someone noticing it, as the pages/blocks are built tightly on top of each other.

**“Book = Blockchain, Page = Block, An entry in page = Blockchain Transaction”**

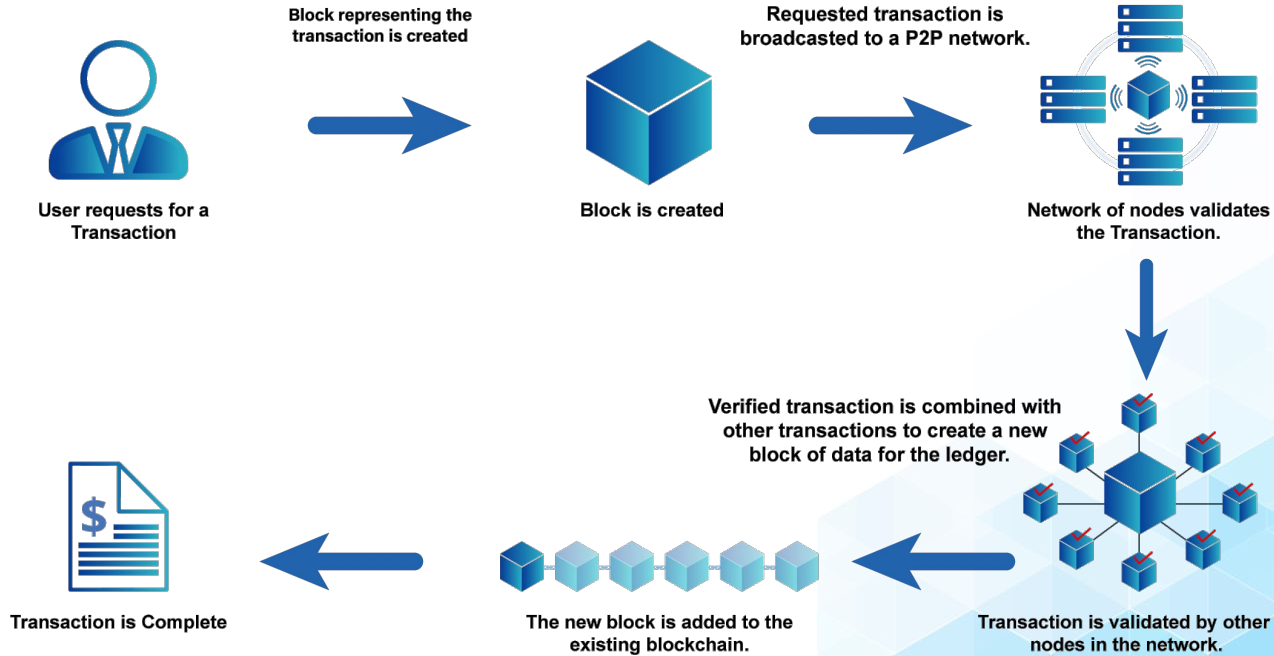


Book	Blockchain
Pages	Blocks
Entries in page	Blockchain Transactions

# History of Blockchain

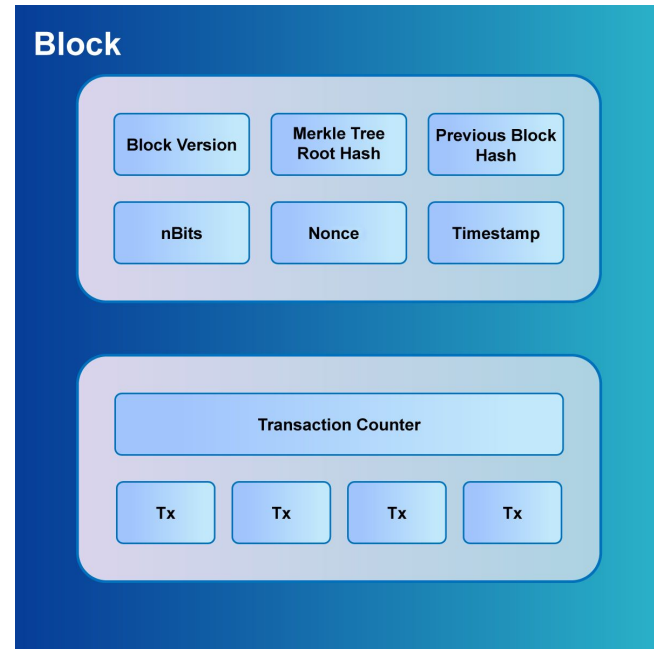
- W. Scott Stornetta and Stuart Haber in 1991, proposed the concept of a secured chain of blocks (set of records).
- In 1998, a Computer scientist Nick Szabo proposed the first digital currency “BitGold”.
- Later in 2008, the blockchain system was conceptualized and introduced by an individual or a community known by the name 'Satoshi Nakamoto.'
- They implemented the idea of using hashing and cryptography create a peer-to-peer system with no third party to store transactions and make them immutable once stored on the blockchain.
- This blockchain architecture is used by the Bitcoin cryptocurrency system as its basic or foundation infrastructure.

# How does Blockchain works?

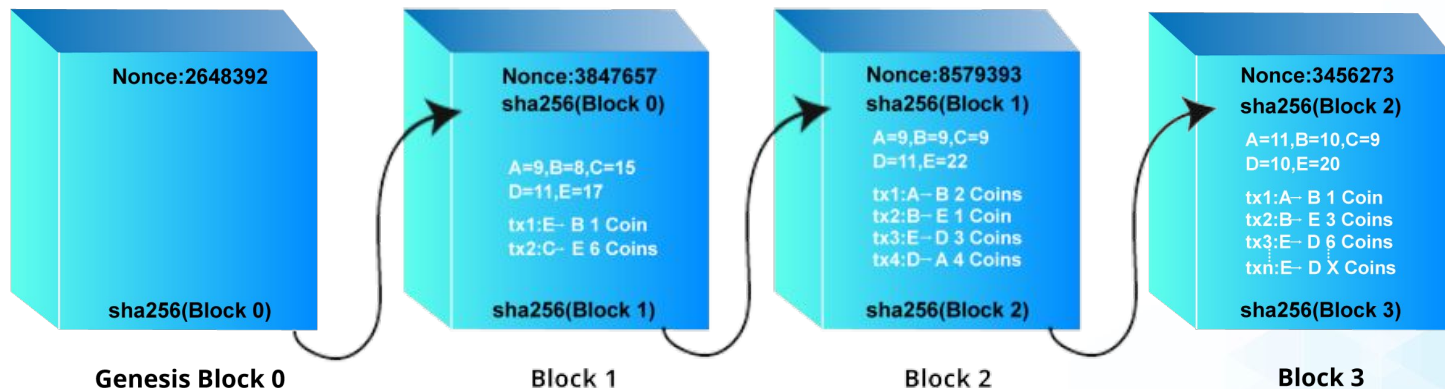


# Block Overview

- Version number signifies the blockchain protocol in the block.
- the hash of the previous block or merkle tree root hash.
- Merkle tree root hash. Each transaction in the block is hashed and stored in a tree-like structure such that each hash is linked to its parent.
- nBits is an encoding of the block target. A block will be valid only if the hash of its header is below the target value.
- Nonce is a variable decided by the miner creating the block changed in order to get a block hash under target value,
- Timestamp value is a source of variation for the block hash.



# How Blockchain looks like?



- Blockchain contains a list of block cryptographically connect to the previous block.
- The blocks are connected such that if there is any change in block(n-1) the connection between the next block will break.
- This makes very hard to change any data in blockchain.
- Each block contains set of transactions data that is linked in the next blocks so that anyone can trace the origin of data

# What makes Blockchain different?





# THANK YOU!

## Any Questions?

Visit

[community.blockchain-council.org](https://community.blockchain-council.org)



Mail Us

[hello@blockchain-council.org](mailto:hello@blockchain-council.org)

