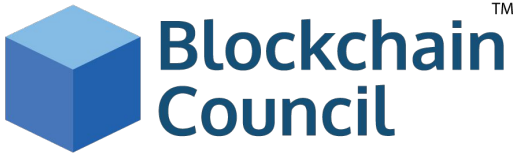


Certified Hyperledger Expert

What is Blockchain?

What is Blockchain?

- Blockchain is a distributed database existing on various computers at the same time.
- A decentralized ledger tracking digital assets on P2P network.
- Some analogies for Blockchain.

Any real life example?

- ❖ Records of your sales & purchases of raw material
- ❖ Or may be simply your bank account statement
- ❖ An excel sheets tracking all hospital equipments
- ❖ Simply a large size book

Book Analogy

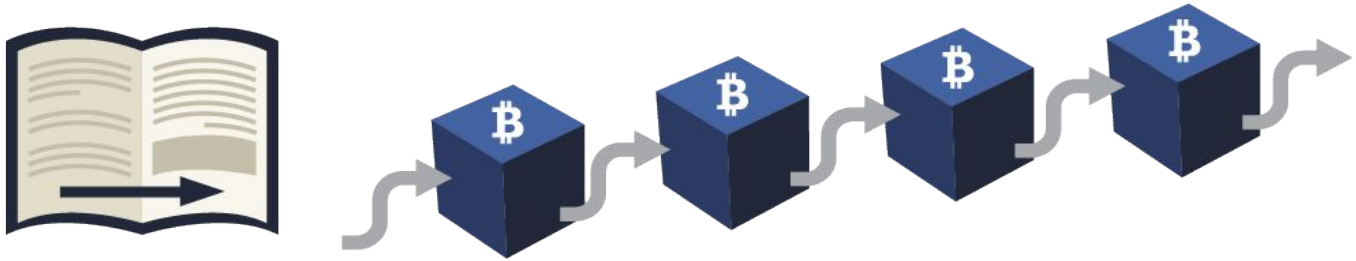
Imagine it as a old time book based ledger where each page reference to the previous page through a page

Book = Blockchain, Page = Block, an entry in page = blockchain transaction

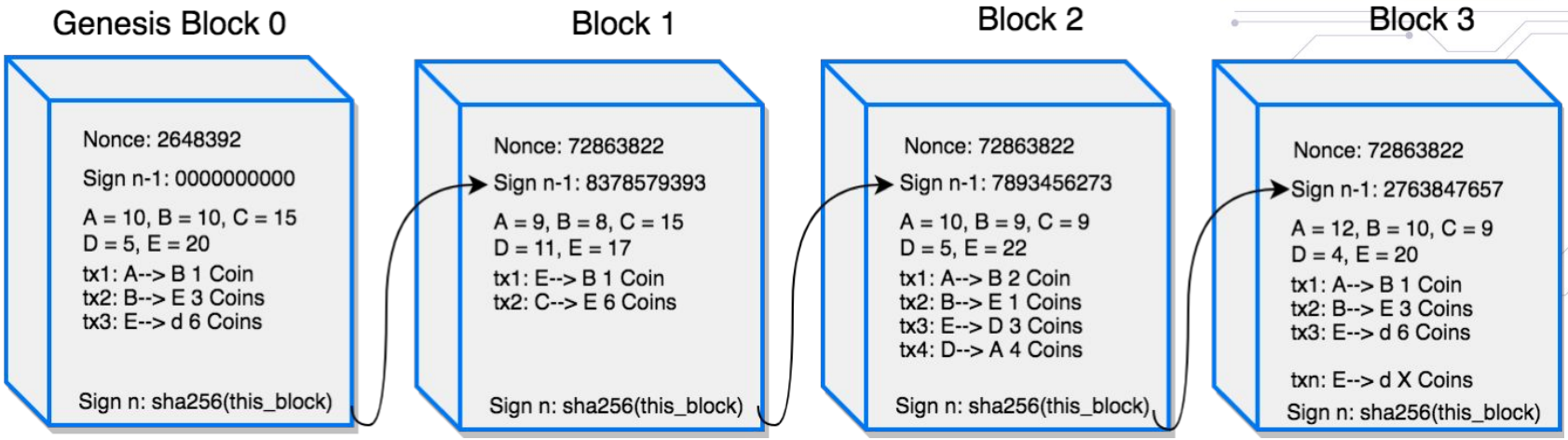
Easy to detect if a page/block has been removed or deleted

Easy to arrange the pages/blocks & identify suspicious activity. That's why page numbers are important in ledger.

Since the pages/blocks are built tightly on top of each other it is impossible to temper a previous entry in the ledger without someone noticing it.



Peek Inside Blockchain



More on Blockchain

- In case of real Blockchain, each block is built on top of the new block and use its previous block's content/signature + Nonce (random string).
- Building a block & adding it in the Blockchain is the task of the miner nodes (optional).
- In public Blockchain, it is made computationally difficult to add a block to prevent attacks.
- Miners try to guess a number (nonce) in such a way that if it gets crunched with the most recent block's fingerprint, then it will create a new fingerprint which will be less than the last/most recent block in the Blockchain.
- It takes time & computational power to add a Block in the Blockchain. Hence there is a reward (12.5 BTC in case of Bitcoin Blockchain, 5 ETH in Ethereum)
- Private Blockchain can choose other methods to add a block as they can trust the miners using a contract etc.

Make you own Definition for Blockchain

Let's build our definition

- It’s a decentralised database which stores information in the form of transactions
- It can be public or private
- Stored data is Immutable
- Highly secure
- Data gets recorded via consensus-based algorithms
- Uses cryptography
- Generally, exist over a peer-to-peer network

So here is our definition:

“Blockchain is a consensus-based secure decentralised public/private database which stores information immutably over the peer-to-peer network”.

Summary

- It is a decentralised distributed ledger (data structure) where data is being stored inside blocks in the form of transactions.
- Removes the dependency on the trusted third party for recording the data in Blocks.
- In public Blockchains, more complex algorithms are required to avoid malicious activities.
- Since each block is built on top of the previous Block, the immutability has been achieved.
- Here immutability means, very difficult to fake/alter a block & very very easy to detect the tampering.
- This all exists in the memory of the computers and runs as a computer process.
- Every participant of the Blockchain contains an almost same copy of the Blockchain ledger.

THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org