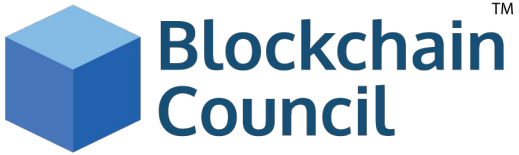


Certified Blockchain Architect

Technical Components of Blockchain Architecture

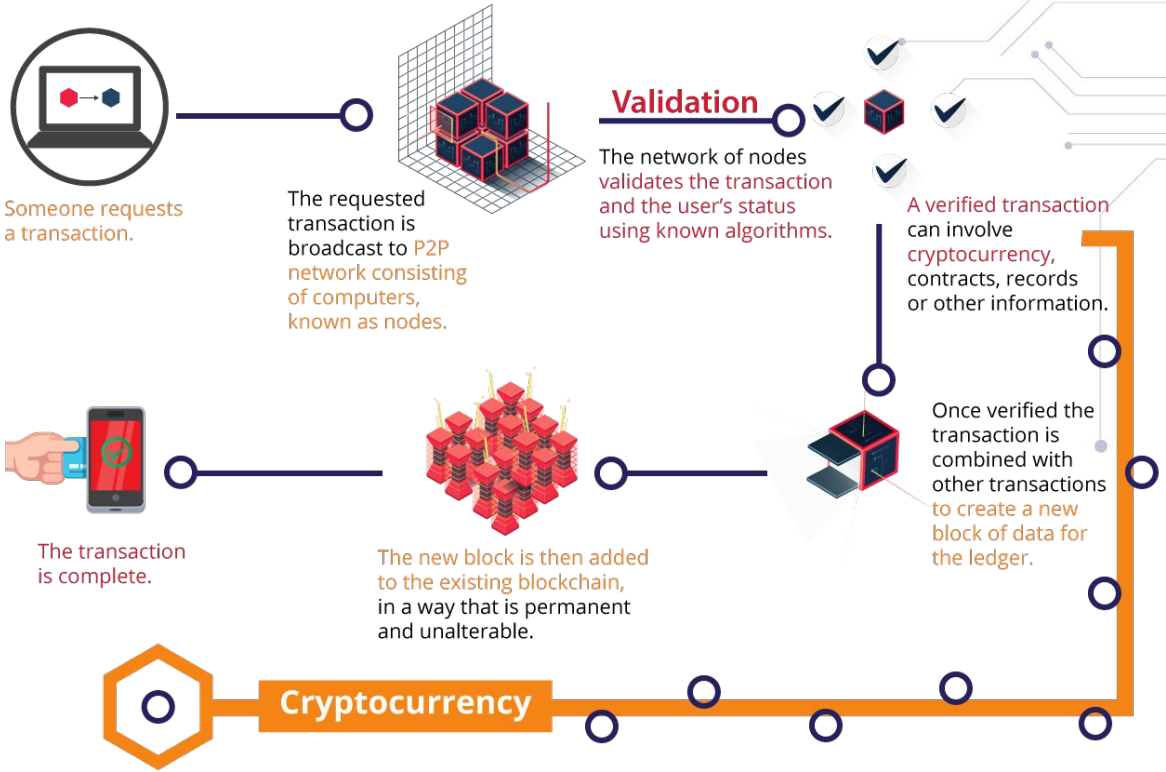
Ledger

- A ledger is a type of a database which is shared, and synchronised amongst the peers in the network.
- In Blockchain a ledger is decentralized which can be used to record the transfer of transactions, digital assets or data.
- A Blockchain ledger consists of the following things
    - Transactions
        - Participants
        - Data
        - Time Stamps
        - Cryptographic Signature / Cryptographic Hash Links
        - Smart Contracts
- There can be several ledgers inside a single blockchain such as in Hyperledger there are separate ledgers for every channel.

Smart Contracts

- Smart Contracts are the computer code that are executed automatically when the terms and conditions that are mentioned in the contract are met.
- The entire process of smart contract is automated and if assigned, a smart contract can control digital assets, currencies or any terms and conditions that are mutually agreed between two parties.
- Smart Contracts simply work on the logic IFTTT (i.e if this then that) statements that are written into code that are on blockchain

Smart Contracts



P2P Network

- A peer-to-peer network can be defined as a network where two or more computers are connected to each other without any third server computer.
- In P2P Network, a peer/node is referred to the computer system who allows provides computer resources to the network such as the Disk Storage, Memory/Processing Power, Network Bandwidth etc.
- A node can have several roles within blockchain ecosystem such as miner, client, full node etc
- A full node gets the copy of the whole blockchain in his device, while he is connected to the network, and in a network there can be n number of full nodes, so the blockchain becomes intact and it is difficult to destroy it.
- At a time in bitcoin you can only connect to 8 peers and in ethereum you can connect to 13.
- In blockchain P2P network there are two types of nodes (i) Reachable Nodes (ii) Unreachable Nodes.
- A reachable node is the node that send and receives the connection where as in unreachable node can only make outgoing connection but do not make any incoming connection

P2P Network

- Less number of Unreachable Nodes is a good news in Blockchain because if a hacker tries to hack the blockchain, he will also need to hack the unreachable nodes which will act as an obstacle and it will be difficult for the hacker to hack.
- According to the bitnode there are currently 10244 nodes in the bitcoin blockchain.

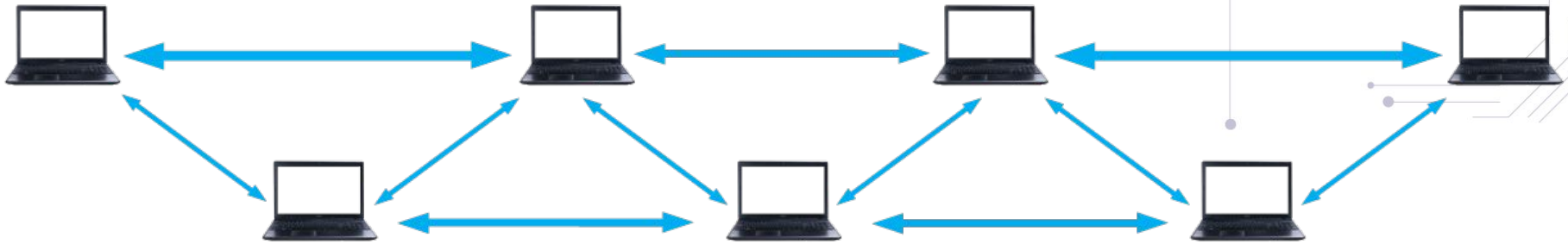


Fig: Illustrating P2P Network

Membership

- Membership in blockchain can usually be seen in permissioned blockchain network, and is used to support variety of credential architecture.
- It is governed by central authorities.
- A membership services code runs in peers. Each peer can authenticate and authorize several blockchain operations.
- The operations in membership are PKI-based implementation (Public Key Infrastructure) of the Membership Services Provider (MSP)

Protocols

- To understand about the Blockchain protocol one must have the understanding of the internet protocols i.e (i) HTTP (ii) TCP (iii) IP
- To give you a brief TCP and IP protocol will route the information over the network and HTTP is an application level protocol that sends the data to TCP/IP stack. HTTP helps web browsers to communicate with the web servers.
- Now, let's jump onto Blockchain Protocols that are namely
    - Distributed Ledgers
    - Encryption
    - Consensus Algorithms
    - Integrated Blocks of Data

Protocols

- **Distributed Ledger**: Modern Internet is powered by the distributed ledger technology which differs with the client-server architecture, because in Blockchain there is no intermediary and each node act as client and server both
- **Encryption**: Blockchain functions on advanced encryption algorithms which makes the blockchain network more secure than the traditional internet protocols. It mainly depends on
    - Digital Signatures (Encryption Puzzles)
    - Hash Functions (SHA-256, RIPEMD, ECC)
    - Public/Private Keys (Symmetric and Asymmetric Cryptography)
- **Consensus Algorithms**: It is a mechanism used to for decision making, in blockchain network participants agree on single version of truth which is later verified by the miners using various complex algorithms
- **Integrated Blocks**: In Blockchain Ecosystem, the integration of blocks is done using hash algorithms. The first block in blockchain also known as the genesis block is hard coded into network

(contd.)

Protocols

- with the initial parameters to the blockchain. When transactions from first block is validated a unique hash value is generated which is then added to the second block. The whole linking feature is what makes blockchain ‘Immutable’. This is a ripple effect which happens throughout the chain and is instantly spotted by every peer in the network

THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org