Blockchain

In the times of rise of nationalism in Europe,revolutionaries envisioned a utopian society—one where power is decentralised, and the community unites against wrongdoing.While such a society seemed impractical, blockchain technology offers a pathway to achieving this decentralised ideal. So let's dive into the trench of **Blockchain**.

What is Blockchain?

A blockchain is essentially a distributed database of records of digital events that have been executed and shared among parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system.**Ethereum** is the most valued blockchain and smart contract platform now.

Smart contracts:

In traditional systems, trust between parties is crucial, and broken promises can lead to significant losses. Smart contracts are a set of instructions executed automatically in a decentralised manner without the need of a third-party and everyone in the blockchain can see through the terms of agreement, showing transparency in the network.

Blockchain oracle:

Decentralised oracle networks (DONs) enable the creation of hybrid smart contracts, where on-chain code and off-chain infrastructure are combined to support advanced decentralised Dapp(Decentralised application).Chain-link is the most popular and a powerful decentralised oracle network.

Basic structure of blocks and the chain:

Block: A block is a list of transactions and smart contracts.

- **Hash/Hashing:** A unique fixed length string, meant to indicate a chunk of data. They are created by placing data into a hashing algorithm. **Ethereum** uses Keccak-256 algorithm to produce hash for the data.
- **Nonce:** Nouce is basically the number that is going to be a solution to a problem and is also used to define the transaction number for an account.The problem can vary, for example: In some blockchains the problem is to find a Nonce that produces a hash which starts with four zeros.

Mining: Mining is the process of finding the solution to the blockchain problem. Nodes (can also be termed as miners and validators) get paid for mining blocks.

- **Private key:** The user can use his/her private key as a password to quote, unquote, digitally sign transactions. A user can sign a contract by their private key being hashed with the transaction data. The user has to use his key in hexadecimal form.

- **Public key**:The public key is derived from the private key itself, it is used by the people of the blockchain to verify the transaction quoted by the user.

Chain: The chain in blockchain is a sequence of blocks that are linked together with their block number, in a chronological order, is the backbone of decentralised systems.

- **Prev:** Prev is simply the hash of the block which precedes the given block. The first block in the chain is known as "Genesis Block", which has a prev as 0.
- **Hash:** It is the hash of the data of the block.

The role of miners in the blockchain:

The miners add and validate transactions into the block, solve the problems/puzzles of the blockchain to produce a Nonce to a block. Miners create new blocks in the blockchain. They prevent bad users from manipulating the data in the blockchain.so with the help of the miners, certain attacks like "51% attack" can be prevented to a great extent.Miners get paid in two ways: **transaction fee (**This fee is paid directly by the user itself **)** and **Block rewards (**Block rewards are given to the miners by the protocol of the blockchain**)**.

Transactions in the blockchain:

Gas: Gas is a unit of computation measurement. The more computations the transaction involves, the more gas the user has to pay as transaction fee.In Ethereum, **Gwei** (1 ether = 10^9 Gwei) is used to price gas. The base fee adjusts automatically based on network demand.

Block confirmations: Block confirmations are the number of additional blocks that are added to the blockchain after the user's transaction went through the block.

How blockchain ensures security and immutability:

Consensus is the mechanism which is used for ensuring that all the nodes agree to the current state of blockchain and authenticity of the transaction.

1. **Proof of work:** In proof of work (PoW), nodes are competing against each other to be the first to solve the computational puzzle of the user 's transaction. In some blockchain, the system sets up a time limit to earn the block rewards by solving the problem. Proof of work costs more energy.

- **Blocktime:** Block time is the amount of time it takes to verify and publish into the blockchain. It is directly proportional to the difficulty of the algorithm of the certain blockchain.
- **Longest chain rule:**It is a rule that states that the valid version of the blockchain is the one with the largest chain of blocks. The larger the blockchain, the more secure it will be.

2. **Proof of stake:** In proof of stake (PoS), nodes put up collateral as a sybil resistance mechanism. Here, miners are referred to as validators, they are chosen

based on the stake of cryptocurrency they hold to validate and publish the new block into the blockchain.Proof of stake uses much less energy.It is used in platforms like avalanche .

- **Scalability:** The network's capacity is determined by scalability, which also affects the number of network nodes, the number of transactions the network can handle, how quickly the network can handle transactions, and other factors.
- **Sharding:** Sharding is a technique for improving scalability by splitting a blockchain up into smaller, more agile blockchains so it can handle more transactions.

3. Delegated proof of stake(DPos): In DPoS consensus, users can either directly vote or give their voting power to another entity to vote on their behalf. Selected witnesses are responsible for creating blocks by verifying transactions.

Attacks on blockchain:

- **Sybil attacks:** A Sybil attack is when a single entity attempts to gain control over a blockchain network through the use of multiple fraudulent nodes.
- **51% attack:** A 51% attack is an attack on a blockchain network where a single entity gains control of more than half (51%) of its staking or computational power. This can be prevented by Making it difficult for one miner to become the majority player and using more secure consensus mechanisms like proof of stake (PoS).

Real-world applications of the blockchain:

- **Healthcare:** Blockchain's immutability ensures that patient records cannot be altered or tampered with, increasing trust in the system. Platforms like "Medrec" use blockchain .
- **Logistics:** A major complaint in the shipping industry is the lack of communication . Blockchain resolves communication issues in the shipping industry by improving transparency. Oracle is a tracking application which is operated entirely by blockchain.
- **NFTs:** Non-fungible tokens (NFTs) have been the trending blockchain application since cryptocurrency. These digital arts are sold on blockchain so that the owner can claim whole rights on it.

Blockchain technology is more than just the backbone of cryptocurrencies like Ethereum. Its decentralised, transparent, and secure nature has the potential to evolve industries from healthcare to logistics, providing innovative solutions to traditional problems.