Blockchain Basics

Blockchain : -

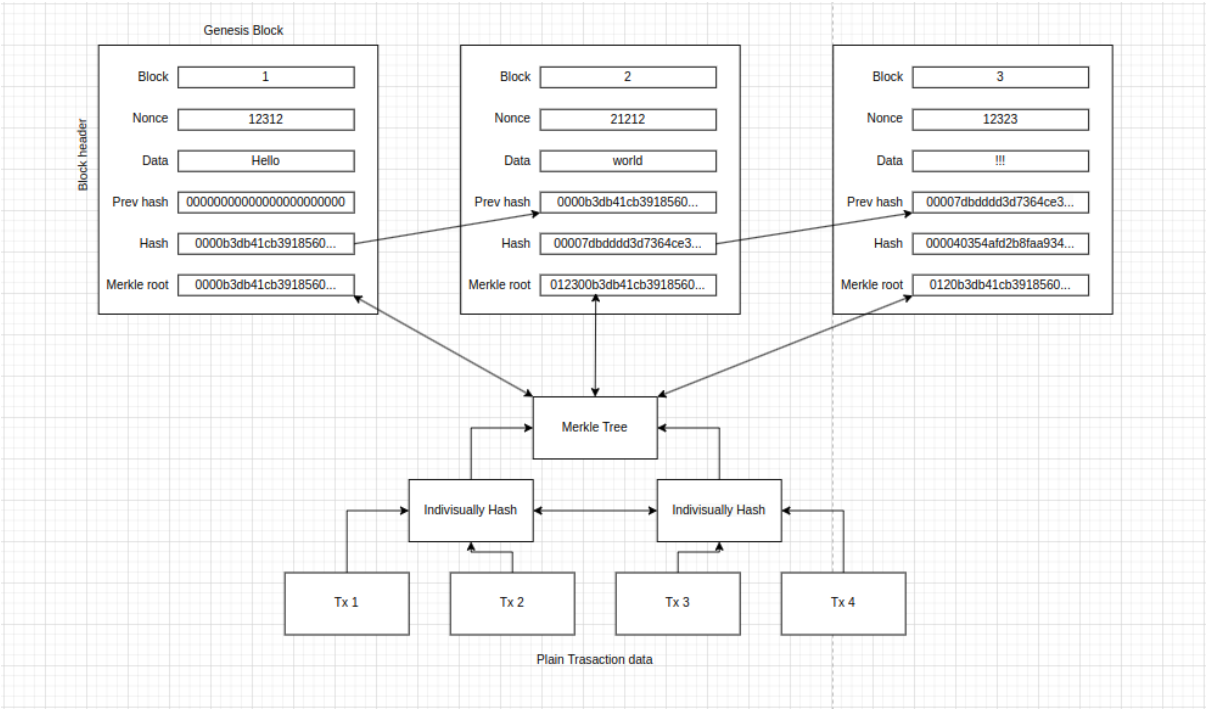
A blockchain is a ***decentralized digital ledger*** that records data in a secure, transparent, and tamper proof way.
It is made up of blocks, where each block contains a list of transactions, a timestamp, and a unique hash.
Every new block is linked to the previous one through this hash, creating a secure and chronological chain.
Instead of relying on a central authority, blockchain operates across a network of nodes that validate and agree on updates using consensus mechanisms like proof of work or proof of stake.
Once data is recorded, it is nearly impossible to alter without the agreement of the majority of the network.

Use Cases : -

Blockchain helps ***track the movement of goods*** from origin to destination with full transparency. Companies like IBM and Walmart use blockchain to verify the authenticity, quality, and journey of a product, reducing fraud and ensuring safety.

Blockchain allows ***physical assets like real estate, gold, or art*** to be represented as digital tokens. This enables fractional ownership, easier transfer, and global access.

Block Anatomy



A **Merkle root** is the top hash of a Merkle tree, which is a ***binary tree of hashes*** built from all transaction data in a block.

Hash each transaction individually.
Pair transactions and hash them.
The Merkle root ensures that any change in any transaction invalidates the block.
It provides efficient integrity verification without checking every transaction.
It's used in Bitcoin, Ethereum, and most blockchain systems for proof of inclusion and lightweight verification.

Proof of Work : -

Proof of Work is a consensus mechanism used by blockchains like Bitcoin to secure the network and validate transactions
It requires miners to solve complex mathematical puzzles (hash calculations / finding nonce) to add a new block to the chain
This process is ***computationally intensive and requires significant energy*** because it involves trying millions of combinations per second to find a valid nonce.
The first miner to solve the puzzle gets to add the block and is rewarded.
The high energy cost helps deter attacks by making it expensive to tamper with the blockchain.

Proof of Stake : -

Proof of Stake replaces miners with validators who are chosen to create new blocks based on the amount of cryptocurrency they "stake" or lock up as collateral.
Instead of consuming power to compete in solving puzzles, ***validators are randomly selected*** with greater chance if they stake more.
This system ***significantly reduces energy usage*** compared to PoW.
PoS is more environmentally friendly and scalable, but it shifts ***influence*** to those who own more of the ***currency***.
It relies on economic incentives and penalties to ensure honest behavior.

Delegated Proof of Stake : -

Delegated Proof of Stake is a ***variation*** of PoS where token holders ***vote to elect a small number of trusted delegates*** or validators who produce blocks on behalf of the network.

Each token acts like a ***vote***, so users with ***more tokens*** have more influence in the ***selection***. The chosen delegates rotate or take turns validating transactions and creating blocks

This system is ***faster*** and more ***efficient***, ***but*** may lead to ***centralization*** since power is concentrated in fewer hands