1. Blockchain Basics

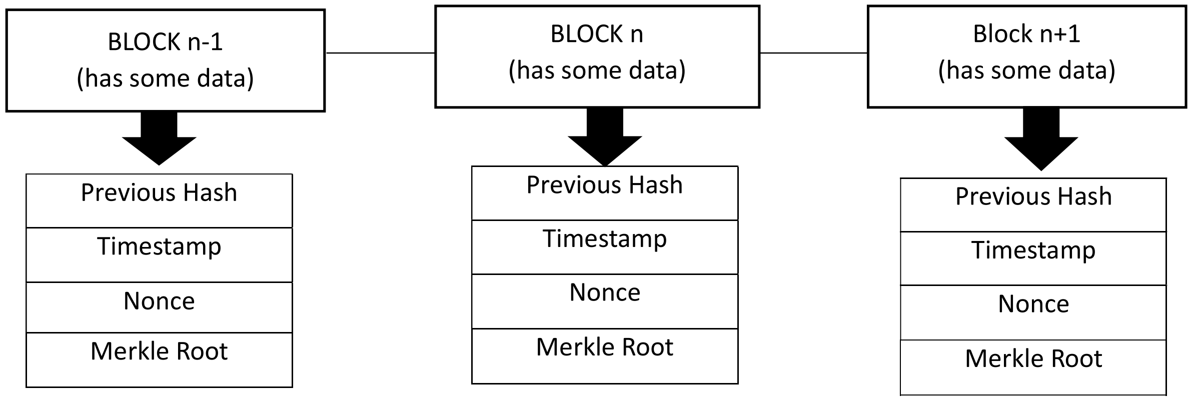
Blockchain is a special kind of database that stores information in a secure, transparent, and decentralized way. It is made up of a chain of blocks, where each block holds a list of transactions or data. Each block has a unique identifier called a hash and also includes the hash of the previous block, linking them together. This creates a chain that cannot be easily changed because altering one block would affect all the blocks after it. The data is distributed across many computers (nodes), so no single person controls it. This makes blockchain very reliable and trustworthy for recording things like financial transactions, ownership, or records without needing a middleman.

Real-life Examples:

1. In Supply Chain Management for Tracking products to ensure authenticity and reduce fraud.
2. Allowing secure, private verification of identity online without central authorities.

2. Block Anatomy

Block Diagram:



Merkle Root :

The Merkle root is a single hash that summarizes all the data inside a block by combining hashes of individual transactions. It helps check if data has been changed because even a tiny change in any transaction will produce a different Merkle root. For example, if someone tries to alter a transaction, the Merkle root will not match, so the system will know the data is tampered with.

3. Consensus Conceptualization

Proof of Work (PoW):

PoW requires miners to solve complex puzzles by trying many random numbers (nonces) until the correct hash is found. This process needs a lot of computing power and electricity, which secures the network against attacks. The miner who solves the puzzle first adds the new block and earns a reward. This method ensures that altering past blocks is very expensive and difficult.

Proof of Stake (PoS):

PoS chooses validators to create new blocks based on the amount of cryptocurrency they hold and lock up as a stake. Validators are selected proportionally to their stake, so those with more coins have a higher chance to add the next block. This process uses far less energy than PoW because no puzzles need to be solved. PoS is faster and more environmentally friendly.

Delegated Proof of Stake (DPoS):

DPoS lets token holders vote for a small group of trusted delegates who manage block creation. These delegates take turns adding blocks and validating transactions. This system is very fast and efficient because only a few validators participate at a time. However, it depends on voting honesty and delegate accountability.