By – Mahima Saxena

Blockchain Basics

Definition (100–150 words):

Both blockchain and distributed ledger are digital platforms that save information about transactions across many machines. Blocks are used to store every new transaction, and every block is connected to the one before it by cryptographic hashes, so a chain forms. As a result of this organizational approach, the data cannot be modified, making it clear and reliable. With consensus mechanisms, trust in the data is possible since there is no central authority to supervise everything. Blockchain is essential for cryptocurrencies, especially Bitcoin, and it is also used in many industries for reliable data management and checking.

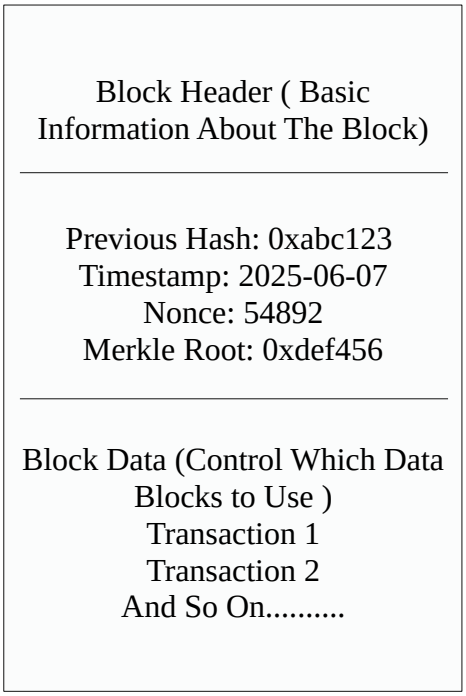
Two Real-Life Use Cases:

1. Using Blockchain in Supply Chain Management, it is easy to track items from the source to their destination, maintain their authenticity, and cut down on fraud in food, pharmaceuticals, and luxury items.

2. With this, individuals are able to keep their identity safe and ensure that KYC processes are carried out securely in banking and government services.

Block Anatomy

Diagram of a Block:



Merkle Root Explanation with Example:

The Merkle Root is a specific hash created to stand for all the transactions in one blockchain block. Merkle Trees are used, as each transaction is hashed by itself, combined with a different hash, and re-hashed several layers until one final hashing is achieved. This last process creates the Merkle

Root. Ensuring the data is not compromised is mainly the role of the hash in a block. A single change in any transaction will modify the Merkle Root, which allows tampering to be quickly found out. This process makes it possible to quickly check all transactions without examining each one, which matters a lot for big blockchain networks and simple wallet software.

Example:

1. Hash each transaction:

   H1 = hash(1)
   H2 = hash(2)
   H3 = hash(3)
   H4 = hash(4)

2. Pair them and hash:

   H12 = hash(H1 + H2)
   H34 = hash(H3 + H4)

3. Get the Merkle Root:

   Merkle Root = hash(H12 + H34)

Consensus Conceptualization

What is Proof of Work and why does it require energy?

Proof of Work (PoW) lets miners try to solve math puzzles in order to verify transactions and append new blocks to the blockchain. The first person to figure out the puzzle gets to place the block and is awarded with a prize. This process relies heavily on computers and electricity since miners are always carrying out millions of calculations each second. Due to how much energy is used, it becomes expensive to carry out an attack on the network. Trust in Bitcoin and the initial cryptocurrencies was kept by using PoW instead of a central managing body.

What is Proof of Stake and how does it differ?

In PoS, validators are selected to develop new blocks because they own and use large amounts of cryptocurrency as a guarantee. Unlike PoW, PoS does not waste a lot of energy since no puzzles have to be solved. Individuals who work as validators can receive a reward if they are straightforward, and they can lose their funds if they act dishonestly. With regard to speed, energy usage, and scalability, PoS is a better option than PoW. It is implemented in some of the more recent types of blockchains, especially Ethereum 2.0 and Cardano.

What is Delegated Proof of Stake and how are validators selected?

DPoS is a kind of PoS where people with tokens vote to decide who among them will be the validators responsible for making blocks and managing the system. It is the job of these delegates to approve transactions and make sure the blockchain works as intended. The influence of voting is usually equal to the number of tokens held, so more community management is possible. While

DPoS is quicker and fairer, it has the risk of being more decentralized since a limited number of people produce the blocks. They have opted for DPoS as their blockchain system.