Blockchain Basics

What is blockchain?
Blockchain is like a digital notebook that stores records or transactions safely. It is decentralized, meaning no single person or company controls it. Instead, many computers called nodes keep a copy of the same data. Data is stored in groups called blocks, and each block is connected to the one before it—like links in a chain.

It uses hash functions, which are like secret codes that turn the data into fixed-length strings. These hashes encrypt the data so it can't be changed easily. There's no need to decrypt them—just compare hashes to check if anything was changed. This makes the data secure and immutable (can’t be changed).

To make sure everyone agrees on what goes into the blockchain, systems use consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS).

Two real-life use cases:

1. **Supply Chain**: Companies use blockchain to track where products come from (e.g., farm to store). This helps make sure food is fresh.
2. **Digital Identity**: People use blockchain to keep their identity safe and log in without passwords.

Block Anatomy

Structure of a block:

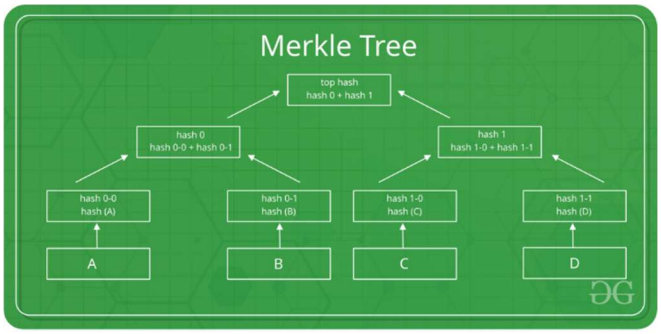
Block Index
Data
Timestamp
Previous Hash
Merkle Root
Nonce

- **Data** – Transaction Information (e.g., who paid whom)
- **Previous Hash** – Connects the block to the one before it
- **Timestamp** – When the block was created
- **Nonce** – A random number miners change to get a valid hash
- **Merkle Root** – Summarizes all the transactions in one hash

What is Merkle Root?
The Merkle Root is like a summary of all the data inside the block. Every transaction is first turned into a hash. Then, those hashes are combined into pairs and hashed again until only one final hash remains—the Merkle Root.

Example: If you have 4 transactions (T1, T2, T3, T4):

- Hash each: H1, H2, H3, H4
- Combine & hash: H12 = hash(H1+H2), H34 = hash(H3+H4)
- Final root = hash(H12 + H34)



Source: GeeksforGeeks

If any single transaction is changed, the root changes too. This helps in quickly checking if data is correct without looking at all transactions.

Consensus Conceptualization

- **What is Proof of Work (PoW)?**
  Proof of Work is a system where computers (called miners) race to solve a hard puzzle (a math problem). They change the nonce again and again until they find a hash that starts with a set number of zeros (like “0000”). This uses a lot of electricity and computing power, but it makes sure blocks are added honestly. Bitcoin uses this method.

- **What is Proof of Stake (PoS)?**
  Proof of Stake doesn’t use miners or puzzles. Instead, people who own coins lock them up (called staking) for a chance to be picked as the next block creator. The more you stake, the better your chance. PoS uses less energy than PoW and works faster. Ethereum has moved to PoS to save energy and increase speed.

- **What is Delegated Proof of Stake (DPoS)?**
  In DPoS, people vote for a few trusted people called delegates or validators. These validators are the only ones allowed to create new blocks. If they cheat, they can be voted out. It’s like a blockchain democracy. DPoS is faster and used in networks like EOS and Tron, where community trust and high speed are important.