Mini Task 1: Build & Explain a Simple Blockchain

Define blockchain in your own words (100–150 words).

Ans:- Blockchain technology is a decentralized digital ledger that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Each transaction is grouped into a block linked to the previous one, forming a chain. This technology underpins cryptocurrencies like Bitcoin and enables smart contracts, supply chain management, and secure data-sharing applications.

Blockchain enables secure, transparent, and decentralized record-keeping without relying on a single central authority. While famously used by cryptocurrencies like Bitcoin, it's also applied in areas like supply chains, digital identities, and smart contracts.

List 2 real-life use cases (e.g., supply chain, digital identity).

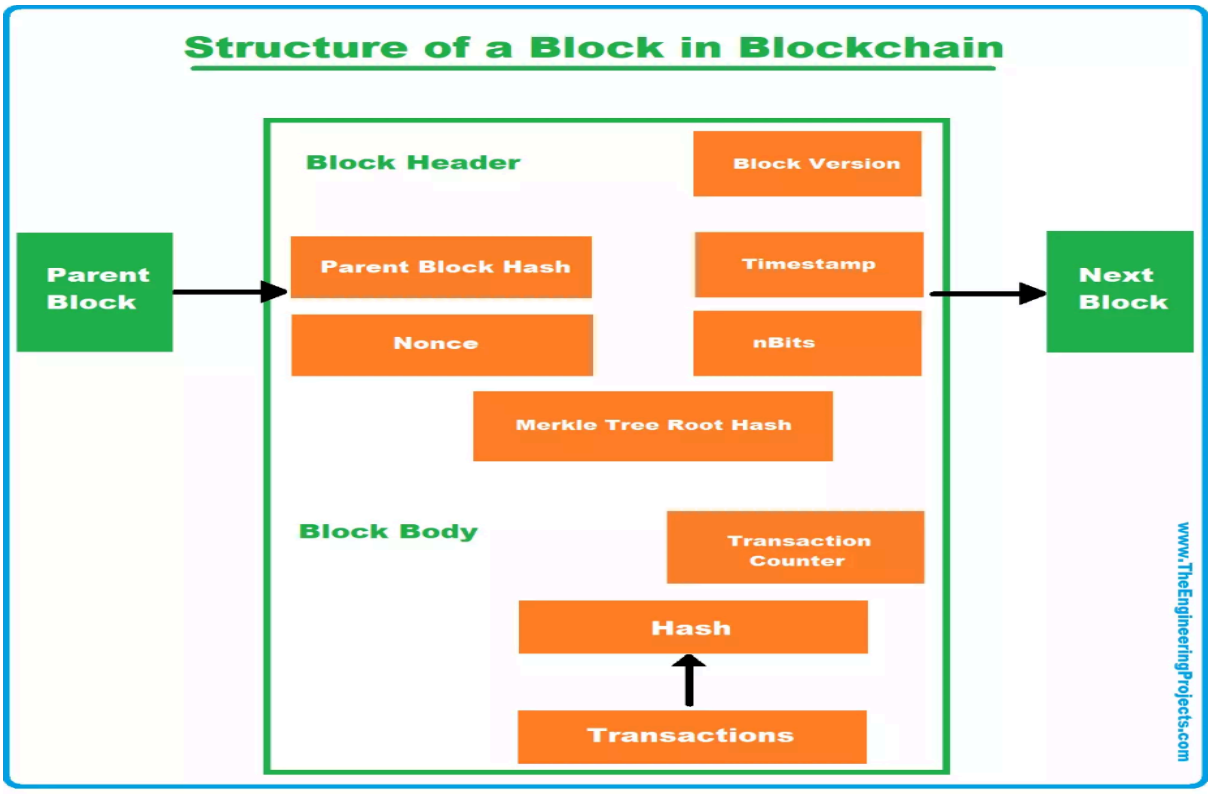
Ans:

Supply Chain Optimization: Companies use AI and blockchain to enhance supply chain transparency, reduce fraud, and improve efficiency. For instance, Maersk and IBM's TradeLens utilize blockchain to track shipping containers, reducing paperwork and streamlining logistics.

Digital Identity Management: Governments and businesses implement decentralized identity solutions to give users control over their personal data. For example, ID2020, in collaboration with Microsoft, works on digital identity systems to help refugees and underbanked populations access essential services securely.

Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root. 4

Ans:



Briefly explain with an example how the Merkle root helps verify data integrity.

A Merkle root is the final hash produced by recursively hashing pairs of data hashes up a binary tree structure called a Merkle tree. Each leaf node of this tree is a cryptographic hash of the original data chunks (such as blockchain transactions), and each non-leaf node is a hash of the concatenation of its two child nodes' hashes. Repeating this hashing process layer by layer culminates in a single top-level hash — the Merkle root — which uniquely summarizes all the underlying data.

How Does This Verify Data Integrity?

- **Tamper-proof hashing**: Cryptographic hash functions used (such as SHA-256) produce fixed-size outputs that are effectively unique for unique inputs. Even a tiny change in any piece of data produces a drastically different hash.
- **Hierarchical validation:** If an attacker alters a transaction or data block at a leaf, the hash of that leaf changes. This in turn changes the hash of its parent node, cascading upward and ultimately changing the Merkle root.
- **Merkle root comparison**: Because the Merkle root is stored securely (e.g., in the block header of a blockchain), anyone can independently calculate the Merkle root from the provided leaf hashes and compare it with the known Merkle root. If the roots differ, data has been modified somewhere in the tree.

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

Ans: Proof of Work is a consensus algorithm used by blockchain networks like Bitcoin to validate transactions and add new blocks to the blockchain without relying on a central authority. Instead, miners (network participants) compete to solve complex cryptographic puzzles — mathematical problems that require intense computational effort. The first miner to find a valid solution earns the right to add the next block and receive cryptocurrency rewards.

Proof of Work Require So Much Energy:

1. C**omputational Effort for Security:** The puzzles miners solve involve "brute force" guessing of nonce values, which requires massive amounts of trial-and-error hashing. This consumes substantial electricity as specialized hardware (like ASIC miners) operate continuously at full power.
2. **Preventing Fraud and Attacks:** The energy cost creates a strong economic disincentive for bad actors. To maliciously alter blockchain data, an attacker would need to redo all the computational work for the targeted block plus all subsequent blocks faster than honest miners—a practically impossible feat without enormous energy and resources. This defense mechanism is sometimes referred to as preventing a "51% attack."
3. **Encouraging Honest Participation:** Mining profits (rewards and transaction fees) motivate miners to act honestly and invest in energy and hardware. Wasted energy on invalid work results in financial loss, aligning incentives towards network security.

What is Proof of Stake and how does it differ?

Ans: Proof of Stake (PoS) is a consensus algorithm used in blockchain networks to validate new transactions and create new blocks. Instead of miners competing to solve complex mathematical puzzles (as in PoW), PoS selects validators based on how many coins they hold and are willing to lock up or "stake" as collateral.

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

Ans: Delegated Proof of Stake (DPoS) was developed by Daniel Larimer in 2014 as an evolution of the traditional Proof of Stake (PoS) consensus system, aiming to address PoS limitations around efficiency, decentralization, and scalability. Its first implementation was in the BitShares blockchain. DPoS introduces a democratic layer to block validation by allowing token holders to vote for trusted representatives (delegates or witnesses) who then produce and validate blocks on their behalf.

Validator Selection Process

Voting Power = Stake Delegates are ranked based on the total tokens staked for them. The top N delegates form the active validator group .

Reputation & Performance Matter

Delegates earn trust and votes by delivering high uptime, reliable performance, and transparent communication . Reward Sharing Many delegates distribute a portion of block rewards back to voters, creating a direct financial incentive to support them .

Continuous Accountability

Because delegates can be voted out at any time, there's strong motivation to act correctly and avoid penalties such as missing blocks or getting slashed