Blockchain Basics

Define blockchain in your own words (100–150 words).
A **blockchain** is a digital ledger that securely records data or transactions in a chain of connected blocks. Each block contains a collection of information, a unique digital signature called a hash, and a reference to the hash of the previous block. This linking of blocks makes it extremely difficult to alter past records, ensuring transparency and security. Blockchain operates on a decentralized network where multiple participants (called nodes) share the ledger, removing the need for a central authority. Whenever new data is added, it gets verified by the network through consensus mechanisms like Proof-of-Work or Proof-of-Stake, then stored in a new block that joins the chain. This technology is widely valued for its ability to provide trust, traceability, and tamper-proof records in both digital and real-world applications.

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

Supply Chain Management:
Tracks the movement of goods from producers to consumers, ensuring product authenticity, reducing fraud, and improving transparency in industries like food, fashion, and pharmaceuticals.

Healthcare Data Management

Blockchain can securely store and manage patient health records, giving patients control over who can access their data while ensuring privacy, integrity, and easy sharing across hospitals and clinics. It reduces the risk of data breaches, allows for faster medical record transfers during emergencies, and ensures that medical histories remain accurate and tamper-proof. This leads to better patient care and streamlined hospital operations.

Block Anatomy

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

https://app.diagrams.net/?title=Copy%20of%20Draw%20a%20block%20showing%3A%20data%2C%20previous%20hash%2C%20timestamp%2C%20nonce%2C%20and%20Merkle%20root.&client=1

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

The merkle root helps verify that the data in a block hasn't been changed. It works by taking all the transactions in a block, hashing them, and then combining those hashes in pairs until a single final hash is produced — that's the merkle root. This root is stored in the block header. If even one transaction is altered, the hash will change, and the final merkle root will no longer match. For example, if a block has four transactions and someone tries to change just one of them, the resulting merkle root will be completely different, showing that the data has been tampered with. This way, the merkle root ensures data integrity without needing to check every transaction manually.

Consensus Conceptualization

What is Proof of Work and why does it require energy?
Proof of Work is a consensus mechanism used in blockchains like Bitcoin where miners compete to solve complex mathematical puzzles to validate transactions and add new blocks. This process requires significant computational power, which consumes a large amount of electricity. The difficulty of the puzzle ensures security and prevents tampering. Only the first miner to solve the puzzle gets to add the block and earn rewards.

What is Proof of Stake and how does it differ?

Proof of Stake is an alternative where validators are chosen to create new blocks based on how much cryptocurrency they hold and are willing to "stake" as collateral. It doesn't rely on solving puzzles, so it consumes far less energy than proof of work. The more coins a person stakes, the higher their chances of being selected. It's designed to be more eco-friendly and scalable.

What is Delegated Proof of Stake and how are validators selected?
Delegated Proof of Stake is a variation where token holders vote to elect a small number of trusted validators, often called delegates, to produce blocks and verify transactions. The selection is based on reputation and community support rather than raw computational power or coin ownership alone. This system allows for faster transactions and lower fees. However, it introduces more centralization since fewer participants control the network.