Blockchain is a decentralized digital ledger that securely records transactions across a network of computers in a tamper-proof way. Each record, or "block," contains a list of transactions, a timestamp, and a unique identifier called a hash. Blocks are linked together using cryptographic hashes, ensuring data integrity. Once data is added, it becomes almost impossible to alter it without modifying all subsequent blocks, making blockchain secure and trustworthy. Unlike traditional centralized databases, blockchains are distributed, meaning no single entity controls the data. This decentralization enhances transparency, reduces the risk of fraud, and removes intermediaries from processes.

Two Real-Life Use Cases:

1. **Supply Chain Management – Companies use blockchain to track the origin and journey of goods from manufacturer to consumer.**
2. **Digital Identity – Blockchain provides secure, verifiable digital IDs, improving privacy and preventing identity theft.**

Merkle Root Explanation with Example:
A Merkle root is a single hash that represents all transactions in a block. Transactions are hashed in pairs, and their hashes are combined and rehashed until one final root is obtained.
Example: **If we have 4 transactions: A, B, C, D →**
Hash A & B → H1, Hash C & D → H2 → then hash H1 & H2 → Merkle Root.
This allows quick verification: if you want to check transaction A, you only need H1 and H2, not the whole dataset. It saves space and ensures integrity efficiently.

Proof of Work (PoW):
PoW requires participants (miners) to solve complex mathematical problems to validate transactions and add new blocks. It's secure because solving these puzzles takes significant computing power and energy. This energy requirement prevents spam and tampering but makes it environmentally intensive.

Proof of Stake (PoS):
In PoS, validators are chosen based on the amount of cryptocurrency they "stake" or lock up as collateral. Instead of burning energy, PoS relies on financial commitment, making it more energy-efficient and scalable than PoW.

Delegated Proof of Stake (DPoS):
DPoS involves token holders voting for a small number of delegates who validate transactions and create blocks. Validators are selected based on popularity (votes), not just wealth or power. This allows fast, democratic, and scalable consensus.