Theoretical Part

1. Blockchain Basics

Definition:
A blockchain is a distributed, immutable digital ledger that records transactions across a network of computers. Each block contains a cryptographic hash of the previous block, creating a secure chain. This decentralized structure eliminates single points of failure and enables trustless transactions.

Real-Life Use Cases:

1. **Supply Chain Tracking:** Companies like Walmart use blockchain to trace food products from farm to store, improving transparency and safety.
2. **Digital Voting:** Blockchain can create tamper-proof voting systems where each vote is verifiable but anonymous.

---

2. Block Anatomy

Block Structure:

Block
Data: Transactions
Previous Hash: abc1
Timestamp: 1234567
Nonce: 42
Merkle Root: xyz9

Merkle Root Example:
Imagine a block with 4 transactions. The Merkle root is a single hash representing all transactions. If even one transaction changes, the Merkle root changes completely, making tampering evident.

---

3. Consensus Mechanisms

Proof of Work (PoW):
Miners compete to solve complex math problems to validate blocks. This requires massive energy because miners must make millions of guesses per second (e.g., Bitcoin).

Proof of Stake (PoS):
Validators are chosen based on the amount of cryptocurrency they "stake" as collateral. More energy-efficient than PoW (e.g., Ethereum 2.0).

Delegated Proof of Stake (DPoS):
Token holders vote for a small number of delegates to validate blocks. Faster than PoW/PoS but more centralized (e.g., EOS).