# Mini Task 1

# Theoretical Part

1. Blockchain Basics

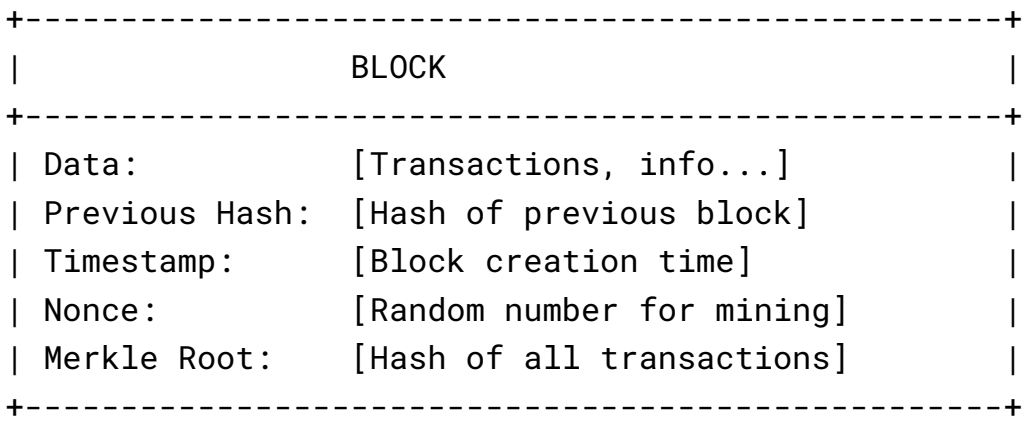
A blockchain is a decentralized, distributed digital ledger that records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively. Each block contains a set of data, a timestamp, and a cryptographic hash of the previous block, forming a secure chain. This structure ensures transparency and security, as every participant in the network holds a copy of the ledger, and any attempt to tamper with the data would require altering all subsequent blocks on every copy of the chain. The consensus mechanism ensures that all nodes agree on the validity of transactions before adding them to the blockchain, making it highly resistant to fraud and unauthorized changes.
Real-life use cases:

- *Supply Chain Management*: Blockchain ensures transparency and traceability of goods as they move through the supply chain, helping to prevent fraud and verify authenticity.
- *Digital Identity*: Individuals can control their digital identities securely, sharing only necessary information and reducing the risks of identity theft.

2. Block Anatomy

A typical block contains:

- Data: The actual information, like transactions.
- Previous Hash: The cryptographic hash of the previous block, linking blocks together.
- Timestamp: The time when the block was created.
- Nonce: A number used once, crucial for mining and consensus.
- Merkle Root: A single hash representing all transactions in the block, built from a Merkle tree.




Merkle Root Example & Data Integrity:
The Merkle root is created by hashing pairs of transactions repeatedly until one final hash remains. For example, if a block has four transactions (A, B, C, D), you hash A+B and C+D, then hash those two results together. If any single transaction changes, the Merkle root changes, making it easy to verify if the data has been tampered with. This allows quick and secure verification of large data sets without checking every transaction individually.

3. Consensus Conceptualization

- Proof of Work (PoW): Miners compete to solve complex mathematical puzzles by varying the nonce until they find a hash below a certain target. This process requires significant computational power and energy, making it expensive to attack the network. The first miner to find a valid hash adds the new block and earns a reward.
- Proof of Stake (PoS): Instead of mining, validators are chosen to create new blocks based on the amount of cryptocurrency they "stake" (lock up) in the network. The more coins staked, the higher the chance of being selected. This method is energy-efficient compared to PoW.
- Delegated Proof of Stake (DPoS): Token holders vote to elect a small group of delegates (validators) who are responsible for validating transactions and creating blocks. The voting power depends on the number of tokens held, and delegates can be replaced if they misbehave.