Mini Task 1: Build & Explain a Simple Blockchain

Theoretical Part:

1. **Blockchain Basics:**
    - A blockchain is a decentralized, distributed ledger technology that records data in a series of blocks, each of which is cryptographically linked to the previous one. Every block contains transactional data, a timestamp, a reference to the previous block's hash, and a unique hash of its own. This structure ensures data integrity and immutability, as altering any block would require changing all subsequent blocks across the network. Blockchains operate without a central authority, relying on consensus mechanisms among participants to validate transactions and add new blocks. This makes blockchain highly secure, transparent, and resistant to tampering, enabling trustless transactions between parties.

    - Supply Chain Management: Blockchain tracks the movement of goods from origin to consumer, ensuring transparency and authenticity.

    - Digital Identity: Individuals securely control their digital identities, reducing fraud and simplifying verification processes.

2. **Block Anatomy**
    - The Merkle root is a single hash representing all transactions in a block. Transactions are hashed in pairs, and their hashes are combined and hashed again, recursively, until only one hash remains—the Merkle root. For example, if a block has four transactions, their hashes are combined in pairs, hashed, and then those results are hashed together to form the Merkle root. This structure allows efficient and secure verification of any transaction's presence in the block without revealing all data, ensuring data integrity.

3. **Consensus Conceptualization**
    - **Proof of Work (PoW):** PoW is a consensus mechanism where network participants (miners) solve complex mathematical puzzles to validate transactions and add new blocks. This process requires significant computational power and energy because miners must perform countless hash calculations to find a valid solution, making attacks costly and impractical.

    - **Proof of Stake (PoS):** In PoS, validators are chosen to create new blocks and confirm transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Unlike PoW, PoS consumes less energy, as it does not require intensive computation; selection is based on stake size and sometimes randomization.

    - **Delegated Proof of Stake (DPoS):** DPoS involves stakeholders voting for a small number of delegates or validators who are responsible for block production. The delegates with the most votes are selected to validate transactions, making consensus faster and more democratic, as voting power is distributed among token holders.