Mini Task 1: Build & Explain a Simple Blockchain

Blockchain Basics

A blockchain is a decentralized, distributed digital ledger that records transactions across many computers so that the record cannot be altered retroactively. Each record (or block) contains a collection of data, a timestamp, a cryptographic hash of the previous block, and a unique hash. All blocks are linked together, forming a secure and tamper-resistant chain.

Since there is no central authority, blockchain ensures trust through consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS). Every participant (node) in the network has a copy of the ledger, and all must agree before a new block is added. This makes it transparent, secure, and immutable, and highly valuable for use cases requiring trust and verification.

Two Real-Life Use Cases

1. Supply Chain Management:

Blockchain helps track the origin, movement, and authenticity of products across the supply chain, ensuring transparency and reducing fraud.

2. Digital Identity:

Individuals can control their identity securely using blockchain, allowing verified access to services like banking, healthcare, and voting without centralized databases.

Block Anatomy

```
+-----------------------------------------------------+
|                      Block                          |
+-----------------------------------------------------+
| Timestamp     : 2025-06-09 12:30:45                 |
| Data          : { 'sender': 'Alice', 'receiver': 'Bob', 'amount': 10 } |
| Nonce         : 125432                               |
| Previous Hash : 000a7d4b...                         |
| Merkle Root   : 29c3ee8f...                         |
| Current Hash  : 00002fa9...                         |
+-----------------------------------------------------+
```

A Merkle Root is a single hash that represents the combined hash of all transactions in a block. Transactions are hashed in pairs, then those hashes are hashed again in pairs, and this continues until one final hash - the Merkle Root - is obtained.

Example:

- Tx1 = hash('A pays B')
- Tx2 = hash('C pays D')
- Then, H1 = hash(Tx1 + Tx2)
- Continue until Merkle Root is formed.

If even one transaction is tampered with, the Merkle Root will change, instantly revealing the issue.

Consensus Conceptualization

Proof of Work (PoW):

PoW is a consensus mechanism where validators must solve a complex mathematical puzzle to add a new block. This requires significant computational power and energy, making it secure but resource-intensive.

Proof of Stake (PoS):

PoS selects validators based on how much cryptocurrency they hold and are willing to 'stake'. It is more energy-efficient as it does not require heavy computation.

Delegated Proof of Stake (DPoS):

DPoS allows coin holders to vote for trusted delegates who validate blocks. It is faster and more democratic, allowing users to indirectly participate in governance.