Blockchain Basics Assignment

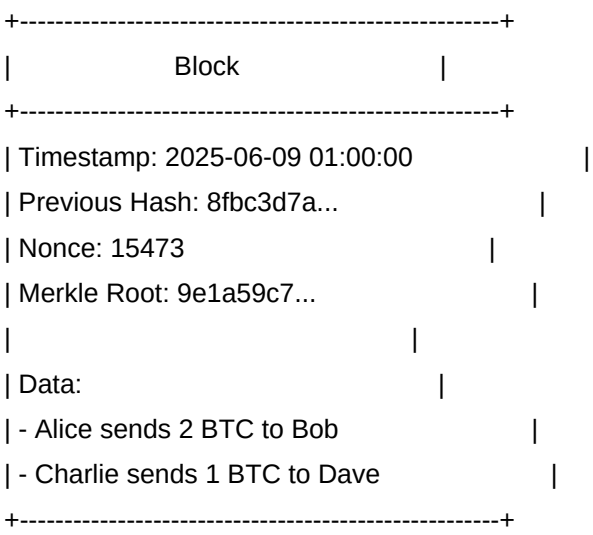
Blockchain Basics

Blockchain is a digital ledger system where data is stored in blocks that are securely linked together in a chain. Each block contains a set of transactions, a timestamp, and a reference to the previous block's hash, making the chain tamper-resistant. Since the data is distributed across many computers (nodes) rather than stored in a central location, it's nearly impossible to alter information without alerting the entire network. This transparency and security make blockchain ideal for trustless environments, where parties don't need to know each other to transact safely. Think of it like a shared notebook that everyone can write in, but no one can erase from.

Real-Life Use Cases

1. Supply Chain Management - Track products from origin to shelf.
2. Digital Identity - Users control their own identity and data.

Block Anatomy (Diagram)



Merkle Root & Data Integrity

A Merkle root is a single hash summarizing all transactions in a block. It's formed by hashing pairs of transaction hashes up the tree until one root remains. If someone alters even a small part of a transaction, the Merkle root will change, signaling tampering. This helps quickly verify the integrity of all data without checking each transaction individually.

Consensus Mechanisms

Proof of Work

Proof of Work (PoW) is a system where miners compete to solve a tough math puzzle. The winner adds a new block to the chain. Solving these puzzles takes a lot of computing power and electricity. It's like a race where everyone burns

energy, but only one wins. This process protects the network against attacks.

Proof of Stake

Proof of Stake (PoS) doesn't involve puzzles. Validators are picked based on how many coins they hold and lock up. The more coins, the better the chance of selection. It's efficient, needing far less energy. Think of it like a lottery: your chances increase with your investment.

Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is like PoS with voting. Token holders vote to choose validators who will confirm blocks. These validators are rewarded for honesty and can be voted out if they cheat. It's like electing trustworthy reps for a group task.