

I Blockchain Basics

1. Define Blockchain in your own words.

A. We can define blockchain as a distributed digital ledger that stores records securely in blocks, which are linked using cryptographic hashes. It works on a peer-to-peer network without any central authority, so everyone can agree on a single version of truth using consensus mechanisms.

Each block stores transactions and important info like timestamp, nonce & hash. Every block is connected like a chain -- if one breaks, all after it break too. It is trustworthy & tamperproof.

2. List 2 real life use cases.

Food Traceability:

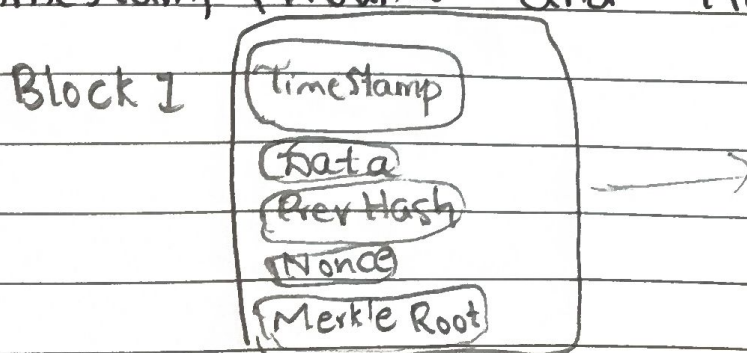
Walmart + IBM use blockchain to trace food origin and freshness.

Digital Identity:

Estonia uses Blockchain to manage citizen eIDs securely.

II Block Anatomy

1. Draw a block showing: data, previous hash, timestamp, nonce and Merkle root.



Date _____
Page _____

2. Briefly explain with an example how the Merkle root helps verify data integrity.

Merkle root is the single hash that represents all transactions in the block. Transactions are hashed and paired again and again until one final root remains. For example, if you change one transaction even a small change, the whole Merkle root changes. This helps system verify whether data was changed or not - like a digital fingerprint for all the transactions.

III Consensus Conceptualization

1. Explain in brief

- What is proof of work & why require energy?

- (a) POW is a consensus method where miner guess a nonce to solve cryptographic puzzle.

- (b) The goal is to find hash that starts with set of zeros.

- (c) Since guessing takes millions of tries, it uses lot of computing power & electricity.

- (d) It's slow & energy-heavy, but it keeps blockchain secure from tampering.

- What is delegated proof of stake & how validators selected?

- (a) DPoS is like an upgraded version of PoS. People vote using their stacked coins to elect a few delegators (validators).

- (b) The top delegators take turns adding the blocks.

- (c) If a validator doesn't do well they can be voted out.

- (d) This is fast, energy efficient involves

community decision making.

• What is Proof Of Stake, how does it differ?

(a) In PoS, validators are selected based on how much Cryptocurrency they lock (stake).

(b) The more stake you have, the higher your chances to validate.

(c) It uses less energy than PoW & doesn't need massive computation, making it faster & more efficient.