

BlockseBlock

Name: Akhil Solomon K

Mini Task

Blockchain Basics

Define blockchain in your own words (100–150 words)

A blockchain is a distributed digital ledger that securely records transactions in a transparent and tamper-resistant way. Unlike centralised systems, blockchain is decentralised, meaning no single authority controls it. Each block contains transaction data and is linked to the previous block, creating a chain. Cryptographic algorithms and consensus mechanisms ensure that only valid transactions are added. This makes blockchain a reliable and secure way to record data, preventing unauthorised changes. Blockchain's decentralised nature allows participants to trust the system without needing to trust each other directly.

List 2 real-life use cases

1. Supply chain tracking to improve transparency and reduce fraud.
2. Digital identity management to verify identities securely and reduce identity theft.

Block Anatomy

Block 1
Data: {transaction data} Previous Hash: <hash> Timestamp: <time> Nonce: <random number> Merkle Root: <hash of data>

Merkle root explanation

The Merkle root is a single hash representing all transactions in a block. If any transaction changes, the Merkle root changes too. This helps quickly verify the integrity of all data in the block.

Consensus Conceptualization

What is Proof of Work and why does it require energy?

Proof of Work (PoW) is a consensus mechanism used in blockchain networks like Bitcoin to validate transactions and add new blocks. It requires miners to solve complex mathematical problems by repeatedly hashing data with a nonce until they find a hash that meets the network's difficulty target. This process involves significant computational power, resulting in energy consumption. The energy requirement acts as a deterrent to malicious attacks, as manipulating the blockchain would require immense computing resources.

What is Proof of Stake and how does it differ?

Proof of Stake (PoS) is a consensus mechanism that selects validators based on the number of coins they hold and are willing to "stake" as collateral. Unlike PoW, PoS does not require energy-intensive computations. Validators are incentivized to act honestly because if they validate malicious transactions, they risk losing their staked assets. This makes PoS more environmentally friendly and efficient compared to PoW.

What is Delegated Proof of Stake and how are validators selected?

Delegated Proof of Stake (DPoS) is a variation of PoS where token holders elect a small group of trusted delegates to validate transactions and produce new blocks. These delegates, also called validators or witnesses, are chosen through a voting process. DPoS systems are generally faster and more scalable because they limit the number of validators who participate directly in block production, relying on the broader network to vote for and hold them accountable.

