

#### Note 1

Blockchain is a decentralized, distributed system, meaning it's a network of computers (nodes) working together without a central authority. This structure is key to its security and resilience.

#### Note 2

The Byzantine Generals Problem illustrates the challenge of achieving consensus in a distributed system where some nodes might be malicious. Blockchain solves this using consensus algorithms like Proof of Work (PoW).

#### Note 3

A block is a bundle of verified transactions linked together chronologically and cryptographically to form a blockchain. Each block contains a timestamp, a nonce, and a hash pointer to the previous block.

#### Note 4

Blockchain offers several key features: decentralization, transparency, immutability, security, and the ability to transfer value (e.g., cryptocurrency) and execute smart contracts.

#### Note 5

The CAP theorem states that a distributed system can only have two of the following three properties at the same time: consistency (all nodes have the same data), availability (the system is always accessible), and partition tolerance (the system continues to function even if some nodes are isolated). Blockchain prioritizes consistency and partition tolerance.

#### Note 6

There are different types of blockchains: public (open to anyone), private (permissioned access), hybrid (combination of public and private), and consortium (governed by multiple organizations).

#### Note 7

Consensus mechanisms ensure all nodes agree on the state of the blockchain. PoW requires miners to solve complex puzzles to add new blocks, while PoS relies on users staking their cryptocurrency. Other mechanisms include PoC, DPoS, PoET, PoA, and Pol.