Note 1

Blockchain is a decentralized, distributed system, a shared, cryptographically-secured ledger enabling peer-to-peer value exchange without intermediaries.

Note 2

The Byzantine Generals Problem highlights the challenge of achieving consensus in a distributed system with potentially malicious nodes. PBFT offers a solution through message signing and verification.

Note 3

A block contains a header, previous block hash, timestamp, nonce, transaction counter, and transactions themselves. Blockchain is a chain of these blocks, cryptographically linked.

Note 4

Blockchain elements: addresses (public key derived), transactions (value transfer), blocks, P2P network, scripting language, virtual machine, state machine, nodes (various roles), and smart contracts (business logic).

Note 5

Blockchain benefits: decentralization, transparency, immutability, high availability, security, simplified paradigms, faster dealings, cost savings. Limitations: scalability, adaptability, regulation, immaturity, privacy.

Note 6

Consensus ensures all honest nodes agree on a data value. Algorithms include PoW (computationally intensive), PoS (stake-based), DPoS (delegated staking), and BFT-based approaches.

Note 7

CAP theorem: distributed systems can't simultaneously achieve consistency, availability, and partition tolerance. Blockchain prioritizes consistency and fault tolerance through replication and consensus.

Note 8

(i) Anonymous users: Public blockchain (e.g., Bitcoin) offers pseudonymity. (ii) High throughput: Private or Consortium blockchains are better suited due to controlled network size and permissions.

Note 9

Byzantine Generals Problem: achieving agreement despite traitorous actors. PBFT solution: multiple rounds of message exchange with digital signatures ensure honest nodes reach consensus.

Note 10

Blockchain evolution: 1.0 (cryptocurrency), 2.0 (smart contracts/dApps), 3.0 (broader applications beyond finance), X.0 (future vision of ubiquitous blockchain services).