

Quiz 3 10% in total

Name: _____

Part 1: Multiple Choice Questions (0.5% each, ONLY one correct answer)

1. In a *Byzantine Fault Tolerance* (BFT) storage system with 14 nodes, what is the maximum number of faulty nodes that can be tolerated?

- A) 2
- B) 3
- C) 4
- D) 5

Your Answer: _____

2. Why does the BFT consensus process require multiple phases instead of relying solely on a leader broadcasting messages?

- A) To reduce network bandwidth usage
- B) To ensure total order
- C) To comply with healthcare regulations
- D) To reduce computational requirements

Your Answer: _____

3. In Phase 1 of the BFT consensus process, what do nodes do after receiving messages?

- A) They immediately accept all received messages
- B) They broadcast the messages to all other nodes and also select the majority one they received
- C) They reject any message that seems suspicious
- D) They wait for the leader's confirmation

Your Answer: _____

4. What happens in Phase 2 of the BFT consensus process?

- A) Nodes send the final decision to everyone, and everyone stores the data with a same order
- B) Nodes verify cryptographic puzzles
- C) Nodes elect a new leader
- D) Nodes delete malicious messages

Your Answer: _____

5. In a BFT system, what happens if a leader sends different messages to different nodes?

- A) The system will automatically correct the inconsistency
- B) Nodes will detect the discrepancy during message broadcasting and may report the leader as malicious
- C) The majority message will always be accepted without question
- D) The system will crash immediately

Your Answer: _____

6. What is the main purpose of BFT in blockchain systems?

- A) To increase transaction speed
- B) To ensure all nodes agree on the order of transactions
- C) To reduce energy consumption compared to Proof of Work
- D) To eliminate the need for miners

Your Answer: _____

7. What specific problem in distributed systems does "total order" in BFT address?

- A) Ensuring messages are processed quickly

- B) Ensuring all nodes process transactions in exactly the same sequence
- C) Ensuring only correct messages are accepted
- D) Ensuring minimal network overhead

Your Answer: _____

8. Which of the following is a key difference between Proof of Work (PoW) and BFT?

- A) PoW requires solving cryptographic puzzles, while BFT relies on message broadcasting
- B) PoW is more energy-efficient than BFT
- C) PoW is faster and more scalable than BFT
- D) PoW does not require a leader, while BFT does

Your Answer: _____

9. What percentage of malicious nodes can the BFT system and Bitcoin blockchain system typically handle individually?

- A) Up to 25%, up to 33.3%
- B) Up to 33.3%, up to 49%
- C) Up to 49%, up to 33.3%
- D) Up to 51%, up to 33.3%

Your Answer: _____

10. Why does the performance of BFT degrade significantly when the number of nodes exceeds 30?

- A) BFT requires all nodes to broadcast messages to every other node, leading to exponential growth in network traffic.
- B) BFT becomes less secure as the number of nodes increases.
- C) BFT requires more energy than Proof of Work (PoW) for large networks.
- D) BFT is incompatible with healthcare data regulations.

Your Answer: _____

Part 2: Real interesting scenarios questions.

Scenario 1:

A pharmaceutical company is using blockchain to track the supply chain of medications, from production to delivery to hospitals. Each step of the process is recorded on the blockchain to ensure transparency and prevent counterfeit drugs.

11. What is the primary benefit of using blockchain for drug supply chain tracking?

- A) It reduces the cost of producing medications
- B) It provides an immutable record of every transaction, ensuring transparency and authenticity
- C) It eliminates the need for regulatory oversight
- D) It allows hospitals to purchase drugs at lower prices

Your Answer: _____

12. How can blockchain help prevent counterfeit drugs from entering the supply chain?

- A) By requiring all participants to use the same software
- B) By providing a tamper-proof record of every transaction, making it easy to verify the origin of drugs
- C) By encrypting all drug-related data
- D) By automatically rejecting suspicious transactions

Your Answer: _____

Scenario2:

A patient is using a **private** blockchain-based health app to manage their medical records. The app

allows the patients to grant temporary access to doctors or hospitals when needed so that the patients can control and manage their data by who or when can access their personal data.

13. How does blockchain empower patients in this scenario?

- A) By giving patients full control over who can access their medical records
- B) By automatically updating medical records without patient involvement
- C) By reducing the cost of healthcare services
- D) By eliminating the need for doctors

Your Answer: _____

Scenario 3:

A hospital network is using a **blockchain-based system** to track the supply chain of medications. Each medication package is assigned a unique identifier (e.g., a QR code), and every step of the supply chain (manufacturer → distributor → hospital → patient) is recorded on the blockchain.

A (1%):

14. Draw a simple flowchart showing the workflow of this blockchain-based supply chain. Include the following steps:

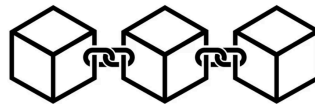
Manufacturer creates the medication info and records it on the blockchain.

Distributor receives the medication and updates the blockchain.

Hospital receives the medication and updates the blockchain.

Patient receives the medication and verifies its authenticity using the blockchain.

Manufacturer →



B (0.5%):

15. Explain how blockchain ensures the authenticity of the medication at each step of the supply chain. (hints: **20 or 30 words** only, you need to discuss the key features of the blockchains)

C (0.5%)

16. Although blockchain can securely record all data, it cannot guarantee the initial authenticity of the data (e.g., if a manufacturer intentionally records fake information). What additional measures could be implemented to improve data authenticity in this system?

- A) Use artificial intelligence (AI) to automatically verify the accuracy of all data entries
- B) Require third-party audits or certifications for each step of the supply chain
- C) Encrypt all data using advanced cryptographic algorithms
- D) Allow patients to manually verify every data entry

Your Answer: _____

Scenario 4:

A blockchain network is designed to be decentralized, meaning it relies on a large number of nodes to validate and record transactions. These nodes are distributed globally and operated by different participants.

17. Why does a blockchain network require so many nodes?

- A) To increase the energy consumption of the network
- B) To ensure decentralization, security, and fault tolerance
- C) To make the network slower and less efficient
- D) To centralize control over the network

Your Answer: _____

Scenario 5:

Blockchain technology can be divided into two main types: public blockchains and private/permissioned blockchains.

Public Blockchains (e.g., Bitcoin):

- Use Proof of Work (PoW) as their consensus mechanisms.
- Anyone can join the network, participate in consensus, and validate transactions.
- Miners or validators compete to earn rewards (e.g., Bitcoin), which incentivizes them to secure the network.
- Highly decentralized and transparent but often slower and less energy-efficient.

Private/Permissioned Blockchains (e.g., Hyperledger, Corda):

- Use Byzantine Fault Tolerance (BFT) or other efficient consensus mechanisms designed for smaller nodes.
- Only authorized participants can join the network and validate transactions.
- More efficient and scalable because they have fewer nodes and no need for competitive mining.
- Suitable for enterprise use cases where privacy, efficiency, and control are important.

18. Which of the following statements are correct? (**Multiple correct answers**, 1%)

- A) Public blockchains are more decentralized but less energy-efficient than private blockchains.
- B) Storing a transaction in private blockchains is faster because they use BFT consensus.
- C) Public blockchains rely on miners who have a financial incentive to secure the network.
- D) Private blockchains rely on a small number of trusted nodes, which can be both an advantage and a limitation.
- E) Public blockchains are better suited for applications requiring high transparency and trustlessness.
- F) Private blockchains are better suited for applications requiring high efficiency and control over participants.

Your Answer: _____