

1 What cybersecurity property of blockchain ensures that recorded transactions cannot be altered?

- A. Availability
- B. Confidentiality
- C. Immutability
- D. Authentication

2 Which cryptographic technique is primarily used to secure blockchain transactions?

- A. Symmetric encryption
- B. Hashing and public key cryptography
- C. Steganography
- D. Digital watermarking

3 What type of cyberattack targets blockchain networks by controlling the majority of mining power?

- A. Sybil attack
- B. DDoS attack
- C. 51% attack
- D. Man-in-the-middle attack

4 How does decentralization improve cybersecurity in blockchain?

- A. By reducing transparency
- B. By removing the need for cryptography
- C. By eliminating a single point of failure
- D. By increasing centralized control

5 Smart contracts can introduce cybersecurity risks primarily due to:

- A. High transaction speed
- B. Poorly written or vulnerable code
- C. Lack of cryptography
- D. Too many nodes

6 Which consensus mechanism is most energy-intensive and has cybersecurity implications?

- A. Proof of Stake (PoS)
- B. Proof of Authority (PoA)
- C. Proof of Work (PoW)
- D. Delegated PoS

7 Which cybersecurity principle is enhanced by digital signatures in blockchain?

- A. Availability
- B. Non-repudiation
- C. Redundancy
- D. Fault tolerance

8 What is the main cybersecurity risk of storing sensitive data directly on a public blockchain?

- A. Data loss
- B. Lack of immutability
- C. Permanent public exposure
- D. Weak encryption

9 Which cybersecurity control can mitigate smart contract vulnerabilities?

- A. Regular backups
- B. Smart contract code audits
- C. Antivirus software
- D. Password rotation

10 Blockchain can improve cybersecurity in identity management by enabling:

- A. Centralized user databases
- B. Shared passwords
- C. Decentralized identity (DID)
- D. Manual verification

Part 2: Scenario-based questions

1 Exchange Wallet Breach

A cryptocurrency exchange stores user funds in an online wallet connected to the internet. Hackers exploit a server vulnerability and steal large amounts of cryptocurrency.

Which cybersecurity control would have BEST reduced the impact?

- A. Proof of Stake
- B. Cold Wallet Storage
- C. Faster Block Confirmation
- D. Increased Mining Difficulty

2 Majority Network Control

A small blockchain network with limited miners is targeted by attackers who gain control of most of the hashing power and start reversing transactions.

Which attack is occurring?

- A. Sybil Attack
- B. Replay Attack
- C. 51% Attack
- D. Phishing Attack

3 Vulnerable Smart Contract

A decentralized finance (DeFi) application loses funds due to a logic flaw that allows attackers to repeatedly withdraw money.

Which security practice would BEST prevent this?

- A. Increasing block size
- B. Smart contract code audit
- C. Using stronger hashing algorithms
- D. More blockchain nodes

4 Fake Nodes Flooding the Network

An attacker creates thousands of fake blockchain nodes to influence network decisions and disrupt consensus.

Which attack does this describe?

- A. DDoS Attack
- B. Sybil Attack
- C. Man-in-the-Middle Attack
- D. Double-Spending Attack

5 Private Key Theft

A user stores their blockchain private key in plain text on a laptop that gets infected with malware.

Which cybersecurity principle was violated?

- A. Availability
- B. Confidentiality
- C. Transparency
- D. Decentralization

6 Blockchain Data Privacy

A healthcare blockchain stores patient data directly on a public blockchain. Regulators raise concerns about privacy and compliance.

What is the BEST solution?

- A. Delete old blocks
- B. Encrypt and store sensitive data off-chain
- C. Increase block confirmations
- D. Switch to Proof of Work

7 Irreversible Transactions

A user accidentally sends cryptocurrency to the wrong address and requests a reversal.

Why is reversal not possible?

- A. Weak encryption
- B. Lack of authentication
- C. Blockchain immutability
- D. High transaction fees

8 Compromised Consensus Node

A validator node in a Proof of Stake (PoS) blockchain behaves maliciously.

Which security mechanism discourages this behavior?

- A. Mining rewards
- B. Node anonymity
- C. Slashing penalties
- D. Hash collision resistance

9 Decentralized Identity Attack

An attacker tries to impersonate a user in a decentralized identity (DID) system.

Which blockchain feature helps prevent this?

- A. Public ledger visibility
- B. Private key digital signatures
- C. Faster transaction speed
- D. Smart contract automation

10 Blockchain Network Availability

A blockchain network experiences service disruption due to massive traffic floods targeting nodes.

Which cybersecurity attack is this?

- A. Phishing
- B. DDoS
- C. Replay Attack
- D. Double Spending