Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 11 - Week 11 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

Number of questions: 10 **Total mark: 10 X 1 = 10**

QUESTION 1

What is Hyperledger Aries primarily used for?

a) Facilitating decentralized identity management
b) Managing cryptocurrency transactions
c) Building supply chain solutions
d) Developing blockchain consensus algorithms

Answer: (a)

Detailed solution:
Please refer to the Week 11 Lecture 51.

QUESTION 2

Which of the following is/are key jobs(s) that/those Hyperledger Aries mainly perform(s)?

a) Proof-of-Stake consensus
b) Aries can work as IIN (Interoperable Identity Network) agent
c) Verifiable credentials exchange
d) Cryptographic currency generation

Answer: (b), (c)

Detailed solution:
Hyperledger Aries plays a key role as an Interoperable Identity Agent. It supports DID communication and Verifiable Credential exchange.

QUESTION 3

Which of the following does NOT pose a direct risk to the security and reliability of blockchain operations?

a) Vulnerability to 51% attacks
b) Compromise of private key security
c) Exploitation of double-spending vulnerabilities
d) High transaction fees

Answer: (d)

Detailed solution:
Blockchain inherently relies on distributed ledger technology, ensuring redundancy by design. The other options—51% attacks, private key compromises, and double spending—are well-recognized risks that can directly undermine blockchain security and integrity. High transaction fees do not pose any direct risk.

QUESTION 4

In what ways can high computing power/stake be misused in blockchain systems?

a) Taking control of consensus to manipulate transactions and enable double-spending
b) Temporarily accelerating block generation to disproportionately increase mining rewards
c) Compromising transaction privacy by analyzing cryptographic hashes
d) Manipulating the blockchain to censor or exclude competitors' transactions

Answer: (a), (b), and (d)

Detailed solution:
a) Taking control of consensus to reverse transactions and enable double-spending: With over 50% of the network's hashing power, an attacker can reverse transactions, enabling double-spending, and disrupt the blockchain's integrity.

b) Temporarily accelerating block generation to disproportionately increase mining rewards: High hashing power allows miners to generate blocks faster, collecting more rewards until the network adjusts difficulty, giving them an unfair advantage.

d) Manipulating the blockchain to censor or exclude competitors' transactions: Miners with significant hashing power can choose to exclude specific transactions from blocks, blocking competitors or others from being able to transact.

QUESTION 5

What is the main objective of a Selfish Mining Attack in a blockchain network?

a) To increase the transaction fees by monopolizing block creation.
b) To disrupt the blockchain's consensus by manipulating the chain's length to gain mining rewards unfairly.
c) To control over 50% of the network's hashing power and reverse transactions.
d) To expose private transactions by decrypting the block headers.

Answer: (b)

Detailed solution:
The goal of a **Selfish Mining Attack** is for miners to withhold their mined blocks, thus secretly building a longer chain. Once they have a longer chain, they release it, causing the network to adopt it, and unfairly gaining more mining rewards.

QUESTION 6

A blockchain network has a 10-minute block interval. A miner, "Miner X," controls 40% of the network's hashing power. Miner X mines a block and does not broadcast it immediately. Instead, Miner X continues mining a second block in secret.

What is the most likely result of Miner X's actions in this scenario?

a) Miner X's second block will automatically become part of the blockchain, and the first block will be always discarded.
b) Miner X's second block will possibly create a fork in the blockchain, which will later be resolved through a chain reorganization
c) Miner X will always successfully steal the rewards of other miners on the network.
d) Miner X's actions must cause the network to collapse due to a 51% attack.

Answer: (b)

Detailed solution:
Miner X's secret mining creates a temporary fork in the blockchain, where two competing chains exist. The network will eventually adopt the longer chain, causing the shorter chain to be abandoned and reorganized.
Please also refer to the Week 11 Lecture 53.

QUESTION 7

Which of the following plays the most crucial role in establishing trust in a blockchain network?

a) Encryption
b) Consensus Mechanism
c) Smart Contracts
d) Distributed Ledger

Answer: (b)

Detailed solution:
A consensus mechanism ensures that all network participants agree on the validity of transactions before they are recorded on the blockchain. This decentralized verification process is fundamental to maintaining trust. **Encryption** secures data but does not establish consensus. **Smart Contracts** execute automated agreements but rely on consensus for validation. **Distributed Ledger** provides transparency but needs consensus to maintain integrity and trust.

QUESTION 8

Which of the following is/are primarily responsible for validating transactions in the Ethereum 2.0 blockchain (Proof of Stake)?

a) Miner
b) Validator
c) Peer-to-peer network
d) Core consensus protocol

Answer: (b)

Detailed solution:
In Ethereum 2.0, which operates on a Proof of Stake (PoS) consensus mechanism, **validators** are responsible for validating transactions and creating new blocks, replacing the role of miners from Ethereum's original Proof of Work (PoW) mechanism in older versions.

QUESTION 9

Which of the following is a potential consequence of an Eclipse Attack on a blockchain node?

a) The targeted node may mine blocks more efficiently due to controlled connections.
b) The targeted node may accept fraudulent transactions or blocks, leading to potential double-spending.
c) The targeted node will immediately disconnect from the blockchain network to prevent further damage.
d) The targeted node will become immune to any form of attack after the Eclipse Attack

Answer: (b)

Detailed solution:
In an Eclipse Attack, the attacker isolates a node by controlling all its inbound and outbound connections. This manipulation can cause the targeted node to accept fraudulent or incorrect information, such as invalid transactions or blocks, leading to issues like double-spending. It does not enhance mining efficiency or make the node immune to other attacks.
Please also refer to the Week 11 Lecture 54.

QUESTION 10

Which of the following is a common technique used by attackers in a front-running attack on decentralized exchanges (DEXs)?

a) Manipulating the gas price to prioritize their transaction over others.
b) Encrypting transactions to hide them from miners.
c) Using a 51% attack to gain control over the network.
d) Altering the smart contract code to change transaction outcomes.

Answer: (a)

Detailed solution:
In a **front-running attack** on a decentralized exchange (DEX), attackers often manipulate the **gas price** (transaction fees) to ensure that their transaction is processed first, ahead of other pending transactions. By offering a higher gas price, the attacker increases the likelihood of their transaction being included in the block before the targeted transaction. This allows the attacker to profit from any price movement caused by the original transaction.