Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 10- Week 10(Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1

What is the purpose of zero-knowledge proofs in Hyperledger Indy?

a. Anonymous cryptocurrency transactions
b. Reduced smart contract execution time
c. Verification of credentials without revealing all details
d. Public visibility of all credential details

Answer: (c)

Detailed solution:
Zero-knowledge proofs allow claims to be verified without disclosing unnecessary information.

QUESTION 2

Which of the following is/are true regarding timelocks and hashlocks in blockchain contracts?

a. Hashlocks allow spending only when a specific secret is revealed
b. Timelocks prevent spending until a predefined time or block height
c. Hashlocks rely on timestamps for cryptographic verification
d. Hashlocks allow spending even if the specific secret is not revealed

Answer: (a) and (b)

Detailed solution:
Refer to Week 10 Lecture Notes

QUESTION 3

Which of the following is/are true regarding cross-chain Hashed Timelock Contracts?

a. They enable cross-chain transactions without trust
b. They require central authorities to enforce conditions
c. They ensure atomicity in swaps between networks
d. The funds go to the intended recipient instead of returning to the original sender if the secret is not revealed before the timeout occurs

Answer: (a) and (c)

Detailed solution:
HTLCs ensure trustless cross-chain atomic swaps using hashlock and timelock mechanisms.

QUESTION 4

Which of the following statements is/are correct regarding trusted third-party (TTP) based asset transfer?

a. Slow transaction speed in comparison to decentralized asset transfer framework
b. Improved transaction transparency
c. Centralized exchanges can act as TTP for asset transfer
d. Security bias can be caused due to third party in general

Answer: (c), (d)

Detailed solution:
TTP-based transfers rely on centralized control and intermediaries. It also has a possibility of security bias on third party. There have been several cases of theft from centralized exchanges.

QUESTION 5

Which of the following statements is/are true about public blockchains operating as isolated silos?

a. They use the same protocols across networks.
b. They operate independently without interoperability.
c. They inherently allow seamless cross-chain communication.
d. They often have different standards and protocols.

Answer: (b), (d)

Detailed solution:
Public blockchains operate with different protocols and standards and lack built-in interoperability.

QUESTION 6

What is an escrow? Select the best possible and concrete answer

a. Escrow is an agreement in which assets are held and distributed when conditions are met
b. Escrow is payment for smart contracts
c. Escrow is a permissioned blockchain
d. Escrow is the cost of execution of smart contracts

Answer: (a)

Detailed solution:
Without the presence of any Escrow, the funds are in control of the sender and receiver parties.

QUESTION 7

Which of the following are guaranteed in the ideal atomic swap protocol ?

a. All swaps will take place only when all parties conform to the protocol
b. If some parties deviate from the protocol, then all conforming party ends up worse off
c. No coalition has an incentive to deviate from the protocol
d. Swaps can take place partially

Answer: (a), (c)

Detailed solution:
Refer to Week 10 Lecture Notes

QUESTION 8

Which of the following steps are involved in the verifiable data transfer protocol in permissioned blockchain?

a. Generate a proof request with verification policies
b. Validate proofs against verification policies
c. Send responses with attestations and proofs
d. Access control policies are not checked

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

Detailed solution:
Verifiable data transfer involves generating proof requests, validating attestations and checking access control policies. Refer to Week 10 Lecture Notes.

QUESTION 9

Suppose Alice has a time-locked contract with a target account as:
Funding Contract - 1 BTC
Hash: ...Fa4509
Timeout: 2Δ

What will happen if Alice refuses to reveal the key and a timeout occurs?

a. 1 BTC is refunded to Alice
b. 1 BTC is transferred to a target account
c. BTC less than 1 is refunded to Alice as Some BTC deducted as penalty.
d. BTC less than 1 is transferred to target account

Answer: (a)

Detailed solution:
Refer to Week 10 Lecture Notes.

QUESTION 10

What is a verifiable credential in Hyperledger Indy?

a. A digital certificate stored on-chain
b. A cryptographic token for mining
c. A smart contract validation key
d. A permissioned blockchain token

Answer: (a)

Detailed solution:
Verifiable credentials are digital certificates stored on a blockchain that provide authenticity.