Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 9 - Week 9 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1

Which of the following is true about Single Sign-on?

a. The same identity can be used to access multiple services
b. Decentralized providers always maintain the identity of individuals participating in single sign-on for each service
c. All individuals always use a fixed same identity for every one of them together
d. All identity holders are also always identity providers

Answer: (a)

Detailed solution:
A single sign-on can be used to log in to multiple services.

QUESTION 2

Which of the following statements regarding Solidity is true?

a. Solidity compiler compiles a solidity program to bytecode which is executed by Ethereum Virtual Machine.
b. Solidity interpreter always executes the program with Ethereum Virtual Device.
c. Solidity interpreter is responsible for executing smart contracts in Ethereum nodes.
d. Solidity program is compiled to high level ascii code which is executed by Ethereum node's interpreter.

Answer: (a)

Detailed solution:
Solidity program is compiled to bytecode, which is executed by Ethereum Virtual Machine

QUESTION 3

Which of the following statements related to Algorand is invalid?

a. A block is prepared
b. The block is propagated through gossiping, Algorand runs Byzantine agreement on the block
c. Prepare the digital signature and propagate
d. A committed block is purged

Answer: (d)

Detailed solution:
A random user prepares a block using sortition, and the protocol propagates the block through gossiping. To validate the block created by the random user (can be a valid or adversarial user), a byzantine agreement is required. Once it is found that the block is valid, then it is digitally signed and propagates the digital signature in the network.

QUESTION 4

Which of the following is true about selecting the random committee in the Algorand network?

a. There is a dedicated node that chooses the nodes to form the committee
b. A distributed algorithm decides the list of nodes participating in the committee, and the committee members are always pre-decided and fixed
c. A specific pool of nodes chosen are given the responsibility of forming the committee
d. The nodes can take part as committee members by winning a local computation

Answer: (d)

Detailed solution:
Algorand is an open model, which means anyone can join the network. Also, it is a permissionless model. It can not have a single node who will select the committee. Cryptographic sortition is used to elect the user to be part of the committee. Every user can elect to be part of the committee. The individual committee members run certain local computations on their machines to determine whether they won the lottery. If they win, they can participate.

QUESTION 5

Which of the following comes with Verifiable Credentials as a native inbuilt feature?

a. Ethereum
b. Litecoin
c. Hyperledger Aries
d. Solidity

Answer: (c)

Detailed solution:
Aries supports natively verifiable credentials and presentations.

QUESTION 6

Consider the following statement - "Say Alice has generated two Distributed Identifiers (DID), DID1 and DID2, for her pairwise relationships maintained in Hyperledger Indy and used in Hyperledger Aries". Which part of the above statement is false with respect to the concepts of Hyperledger Indy and Aries?

a. Generation of DID by Alice
b. Assignment of SEED to Steward
c. Acceptance of incoming invitation by Alice
d. Saving DID metadata always in a centralized Identity ledger

Answer: (d)

Detailed solution:
a,b,c are valid for the situation. Please refer to Week 9 Lecture Notes

QUESTION 7

In Verifiable Credential (VC) scheme

a. The verifiable credentials can be verified by the issuer only.
b. The verifiable credentials can be verified by the holder only.
c. The verifiable credentials can be verified by the verifier (who requests for verifiable presentations) only.
d. Verifiable credentials can be verified by issue, holder, and verifier.

Answer: (d)

Detailed solution:
VC is a claim about a subject that can be verified by the issuer, holder, and verifier

QUESTION 8

Data transfer is an important aspect of interoperability in which of the following permissioned blockchains?

a. Hyperledger Indy
b. Ethereum
c. Hyperledger Fabric
d. Hyperledger Ursa

Answer: (c)

Detailed solution:
Hyperledger Fabric supports interoperability by extending to the Cacti framework.

QUESTION 9

Which of the following is/are true for Hyperledger Indy and related Decentralized Identifier (DID) context. Please choose all possible correct answers.

a. Digital representation of physical identity and Individuals can control the usage of their own identity
b. Facilitates Verifiable presentation (VP) of the ID
c. Indy credential schema defines the structure for Verifiable Credential templates
d. Self-Sovereign Identity (SSI) uses DID as the backbone of its identity handling.

Answer: a, b,c, d

Detailed Solution:
a,b,c, and d are correct. DID provides a decentralized identity that can be based on open standards and can perform a verifiable presentation of the ID when required, maintains trust, and is used in SSI . For details please refer to slides.

QUESTION 10

Which of the following statements is false in context to Byzantine Fault Tolerant (BFT) protocol in general?

a. The system can operate correctly as long as the number of faulty nodes does not exceed the allowable threshold proportion of faulty nodes.
b. Classic BFT Protocol is used in a permissioned system.
c. RAFT is a type of BFT protocol
d. The system assumes all the nodes are honest

Answer: (d)

Detailed Solution: d is the correct option. BFT can perform in the system with malicious nodes within specified limits, and RAFT is Crash Fault Tolerant. For details please refer to slides.