NOC22-CS44: Blockchain and Its Applications
Assignment 9

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

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
    c. All individuals use a fixed same identity for every one of them
    d. All identity holders are also identity providers

2. Which of the following sequence of steps is valid for Algorand?
    i. A block is prepared
    ii. Run Byzantine agreement on the block
    iii. Prepare the digital signature and propagate
    iv. Block is propagated through gossiping

    a. i, ii, iv, iii
    b. i, ii, iii, iv
    c. i, iv, ii, iii
    d. I, iii, ii, iv

Hint:

- **A random user prepares a block**
- **Propagate the block through gossiping**
- **To validate the block created by the random user(can be valid or adversarial user), a byzantine agreement is required**
- **Once it is found that the block is valid, then it is digitally signed and propagate the digital signature in the network.**

3. Which of the following statements regarding Solidity is true?
    a. Solidity is compiled to bytecode which is executed by Ethereum Virtual Machine.
    b. Solidity interpreter executes the program by Ethereum Virtual Machine.
    c. Solidity interpreter executes smart contracts in Ethereum nodes.
    d. Solidity is compiled to bytecode which is executed by Ethereum node's interpreter.

4. **Which of the following can be used for setting up Verifiable Credentials?**
    a. Hyperledger Aries
    b. Litecoin
    c. Ethereum
    d. Solidity

5. Which of the following is true about the selection of the random committee in the Algorand network?
    a. There is a dedicated node which chooses the nodes to form the committee
    b. A distributed algorithm decides the list of nodes participating in the committee
    c. A specific pool of node choose are given the responsibility of forming the committee
    d. The nodes elect themselves as a committee member by winning a local computation

    Algorand is an open model which mean anyone can join the network. Also it is a permissionless model i. 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. In which every user can elect himself as the part of the committee. The individual committee members run certain local computation on their own machine to find out whether they won the lottery or not. If they won, they can participate.

6. Which of the following is not a valid distinct component in Distributed Identifiers(DID) Architecture.
    a. DID Controller
    b. Verifiable Data Registry
    c. DID Subject
    d. DID Randomizer

    Refer to Week 9 slide

7. Consider the following statement - “Say Alice has generated two Distributed Identifiers (DID) DID1 and DID2 for her pairwise relationships maintained in Hyperledger Indy”. Which part of the above statement is false with respect to the concepts of Hyperledger Indy?
    a. Generation of DID by Alice
    b. Assignment of SEED to Steward
    c. Acceptance of incoming invitation by Alice
    d. None of the above

    Refer to Week 9 Lecture Notes

8. In Verifiable Credential (VC), a claim is a statement about a non participant.
    a. True
    b. False

    Refer to Week 9 Lecture Notes.

9. Which of the following statement(s) is/are true
    I. In Hyperledger Indy, any authorised party can read the ledger.
    II. In Hyperledger Indy, only registered parties and can write to the ledger.

        a. I
        b. I, II

c. II

d. None of the above

Hyperledger Indy is a public permissioned ledger based registry which is readable to all but only a group of selected entities can write.

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

    a. Hyperledger Indy

    b. Corda

    c. Hyperledger Fabric

    d. None