NOC22-CS44: Blockchain and Its Applications
Assignment 9

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

1. Which of following statements are the true for PBFT
    a. It requires a dynamic consensus group
    b. For scalability it requires O(n) for communication complexity
    c. create multiple pseudonymous identities to subvert the 3f+1 requirements of PBFT
    d. None of the above

In PBFT coin their assumption is standard to the normal PBFT system that you have a 3f+1 static group of "trustees" who are there, who will run the PBFT to withstand f number of failures. So, to sustain f number of failures you would require 3f plus 1 number of nodes in the system. The pBFT mechanisms are vulnerable to Sybil attacks, where a node can create multiple pseudonymous Identities. Hence, the node can create multiple such identities to subvert that the 3f+1 requirement of PBFT.

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

- **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. Strong Synchrony ensures liveness of protocol Algorand. True or False
    a. True
    b. False

To achieve liveness, Algorand makes a "strong synchrony" assumption that most honest users (e.g., 95%) can send messages that will be received by most other honest users (e.g., 95%) within a known time bound.

4. Algorand is not always safe under weak synchrony. True or False
    a. True
    b. False

    Algorand achieves safety with a "weak synchrony" assumption: the network can be asynchronous (i.e., entirely controlled by the adversary) for a long but bounded period of time(e.g., at most 1 day or 1 week). After an asynchrony period, the network must be strongly synchronous for a reasonably long period again (e.g., a few hours or a day) for Algorand to ensure safety. The weak synchrony assumption is that in every period of length b (think of b as a day or a week), there must be a strongly synchronous period of length s < b (an s of a few hours suffices).

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. The nodes elect themselves as a committee member by winning a local computation
    d. A specific pool of node choose are given the responsibility of forming the committee

    Algorand is an open model which mean anyone can join the network. Also it is A and 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 component in Distributed Identifiers(DID) Architecture.
    a. DID Controller
    b. DID Validator
    c. Verifiable Data Registry
    d. DID Subject

    Refer to Week 9 slide

7. Consider the following statement - "Say Alice has generated two Distributed Identifiers (DID) DID1 and DID2 for three of 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. Two DID(s) for 3 pairwise relationships
    c. The above statement is completely correct
    d. Both parts of the statement are wrong

    Refer to Week 9 Lecture Notes

8. In Verifiable Credential (VC), a claim is a statement about a _____
    a. Holder

b. Issuer
c. Subject
d. Verifier

Refer to Week 9 Lecture Notes.

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

   a. I
   b. II
   c. I, 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. Which of the following sequence of steps is valid for DID Registration?
    i. Register DID
    ii. Create DID Document
    iii. Fetch DID Document
    iv. Update DID Document

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

Refer to Week 9 Lecture Notes