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 statements is true for Byzantine Fault Tolerant (BFT) protocol.
    a. The system should work correctly even in presence of malicious users within the defined limit of faulty nodes.
    b. BFT Protocol is used generally in a permissioned system in its basic form.
    c. RAFT is a type of BFT protocol
    d. None of the above

Detailed Solution:BFT can perform in the system with malicious nodes within specified limit, RAFT is Crash Fault Tolerant. So a,b are true. For details please refer to slides.

2. Algorand in general is safe under weak synchrony.
    a. True
    b. False

Detailed Solution: Algorand protocol is safe under weak synchrony. Please refer to slides for details.

3. Which of the following is/are applicable for standard Algorand
    a. Forking issue not present
    b. Highly scalable
    c. Need large network to perform optimally
    d. Uses random committee

Detailed Solution: Algorand selects a random committee and is highly scalable with no forking issues in general. So all options are correct. Please refer to slides for details.

4. Which of the following is/are true for Single Sign-On(SSO) based systems.
    a. Single identity for various purposes
    b. One password to access multiple services
    c. Single identity provider can maintain the identity
    d. None of the above

Detailed Solution: SSO ensures single signing to multiple services. So options a,b and c are true. Please refer to slides for more details.

5. Which of the following is/are true for Decentralized Identifier (DID)
    a. Digital representation of physical identity
    b. Individuals can control the usage of their own identity
    c. Provides Verifiable presentation of the ID
    d. DID helps in trusted data exchange

Detailed Solution: All the options are true. DID provides decentralized identity which can be based on open standards and can perform verifiable presentation of the ID when required and maintains trust. For details please refer to slides.

6. Which of the following is/are true for a DID document.
    a. A set of data describing the DID subject
    b. Includes cryptographic mechanism
    c. Consists mapping of entries
    d. None of the above

Detailed Solution: DID describes the subject, uses cryptographic mechanism and maps as key/value pair. So a,b,c are true.

7. DIDs only allow a DID controller to prove its control over its DID Document.
    a. True
    b. False

Detailed Solution: Option a is true. Please refer to slide.

8. In Verifiable Credential (VC), a claim is a statement about a ________
    a. Holder
    b. Subject
    c. Issuer
    d. Verifier

Detailed Solution: Option b is true. Please Refer to Lecture Notes.

9. Censoring of data registry is a major problem mainly in centralized systems
    a. False
    b. True

Detailed Solution: In a centralized system centralized administration control may introduce hierarchy and censoring. So option b is correct. Please refer to slides for further details.

10. Which of the following steps is/are valid for DID Registration?
    a. Register DID
    b. Create DID Document
    c. Authenticate DID Controller
    d. Update DID Document

Detailed Solution: all of the options are required for DID registration. Please refer to slides for further details.