Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 7 - Week 7 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1

Which statement(s) are not true about Byzantine Dissemination Quorum:
   a. Any two quorums have at least one correct replica in common
   b. There is always a quorum available with no faulty replicas
   c. Any two quorums have at most one correct replica in common
   d. There is always a quorum available with some faulty replicas

Answer: (c), (d)

Detailed solution:
Refer to Lecture 31: Byzantine Dissemination Quorum: Intersection: Any two quorums have at least one correct replica in common. Availability: There is always a quorum available with no faulty replicas

QUESTION 2

If you have f number of total faulty nodes, then you need at least how many replicas to reach consensus considering the possibility of both crash fault or byzantine fault.
   a. $2f + 1$
   b. $3f + 1$
   c. $f + 1$
   d. $3f$

Answer: (b)

Detailed solution:
Considering the byzantine fault, $3f + 1$ replicas are required to reach a consensus. This is greater than $2f + 1$ replicas, which is enough to handle crash faults, too.

QUESTION 3

Which cryptographic technique is primarily used in PBFT to validate message integrity?

    a. Hashing
    b. Symmetric encryption
    c. Digital signatures
    d. Sharding

Answer: (c)

Detailed solution:
PBFT utilizes digital signatures to ensure the authenticity and integrity of messages

QUESTION 4

Which mechanism ensures PBFT liveness when the primary fails?

    a. Cryptographic signatures
    b. View change protocol
    c. Pre-prepare and Prepare phases
    d. Timeout mechanism

Answer: (b)

Detailed solution:
The view change protocol allows the system to elect a new primary when the current primary fails.

QUESTION 5

Which of the following statement(s) are not true regarding Hyperledger frameworks?
    a. Hyperledger frameworks are primarily used for building permissioned blockchains for organizations.
    b. Hyperledger frameworks are developed for mainly building public blockchains.
    c. Hyperledger frameworks can not use CouchDB.
    d. Hyperledger frameworks are only used for building smart contracts for public blockchains

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

Detailed solution:
Fabric is primarily used for building permissioned blockchains for organizations. It is an open source project so anyone can use it to build a permissioned blockchain and deploy smart contracts on it. The states can be maintained using light weight databases such as Level DB, CouchDB etc.

QUESTION 6

Which of the following(s) is/are benefits of Blockchain for Business?

    a. Reduced transaction time in general, from days to near instantaneous for legacy based cross-border interactions
    b. The sole centralized authority has been able to remove overheads and cost
    c. Supports transparency and traceability in transactions
    d. Always increases transaction costs due to complexity

Answer: (a) and (c)

Detailed solution:
Refer to Lecture 33. The benefits of Blockchain for business include **reduced transaction time** by enabling near-instantaneous cross-border transactions and **supporting transparency and traceability** through immutable ledger. Blockchain does not involve a **centralized authority** to remove overheads, and while complexity may increase costs, the goal is to ultimately **reduce transaction costs**.

QUESTION 7

Which of the following are characteristics of permissioned blockchains (in comparison with permissionless blockchains)?

    a. Closed membership consensus protocol in permissioned blockchains
    b. The identities of nodes are not pre-known in permissioned blockchains
    c. Always lower transaction throughput in permissioned blockchains
    d. Permissioned blockchains are highly scalable for a large number of nodes

Answer: (a)

Detailed solution:

Permissioned blockchains use closed membership consensus algorithms and have a high transaction throughput. However, they are less scalable in accommodating a large number of nodes compared to permissionless blockchains. Refer to Lecture 33.

QUESTION 8

Which of the following abstractions in Hyperledger Fabric primarily provides confidentiality to individual ledgers ?

    a. Ordering Services
    b. Peers
    c. Channels
    d. Consensus

Answer: (c)

Detailed solution:
Refer to Lecture 35: Fabric channels refer to different separate ledgers such that only organizations belonging to a particular channel can read/write to that ledger.

QUESTION 9

What is the role of Membership Service Provider (MSP) in Hyperledger Fabric?
    a. Assigning sequence numbers to transactions
    b. Identity management for network participants
    c. Storing ledger data securely
    d. Defining consensus mechanism for network

Answer: (b)

Detailed solution:
MSP handles the identity management for network participants. It ensures that only authorized participants are allowed to interact with the network.

QUESTION 10

Which of the following are key features of Hyperledger Fabric?

a. Modular architecture with pluggable components
b. Permissionless blockchain framework
c. Support for smart contracts (chain codes) in general-purpose languages
d. Use of native cryptocurrencies for transactions

Answer: (a), (c)

Detailed solution:
Hyperledger Fabric is a permissioned blockchain framework with a modular design and support for smart contracts (chain codes) written in languages like Go, Java, and Node.js. It does not have native cryptocurrencies.