Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 8 - Week 8 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1

Which of the following is/are correct?

a. PoW always ensures consensus finality
b. PoW does not ensure consensus finality
c. PBFT protocol always ensures consensus finality
d. PBFT protocol does not ensure consensus finality

Answer: (b) and (c)

Detailed solution:
PBFT protocol ensures total ordering of transactions, thus ensuring consensus finality. Whereas PoW does not ensure consensus finality.

QUESTION 2

Which of the following is/are true regarding the CoSi protocol?

a. Witnesses are organized in a tree structure
b. Three rounds of PBFT can be emulated using one round of CoSi protocol
c. It can be used to sign a message by multiple authorities collectively
d. Three rounds of PBFT can be emulated using two rounds of CoSi protocol

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

Detailed solution:
Refer to Week 8 Lecture Notes

QUESTION 3

Which of the following factor(s) distinguish Bitcoin-NG from Bitcoin?

a. Decoupling the leader election and transaction serialization
b. Use of key blocks and macroblocks
c. Bitcoin-NG has lower transaction throughput as compared to Bitcoin
d. Leader election using PBFT

Answer: (a) and (b)

Detailed solution:
Bitcoin-NG has a higher transaction throughput than Bitcoin. It decouples the leader election from transaction serialization using key blocks and microblocks.

QUESTION 4

Which of the following is/are true regarding Bitcoin-NG?

a. Microblock generation rate is lower than the key block generation rate
b. Microblock generation rate is higher than the key block generation rate
c. The interval between the generation of two key blocks is exponentially distributed
d. The key block contains the ledger entries

Answer: (b), (c)

Detailed solution:
Microblocks contain the ledger entries and microblocks have a higher generation rate as compared to key blocks. Refer to Week 8 Lecture Notes

QUESTION 5

Which of the following is/are correct?

a. PBFT protocol ensures total ordering of transactions
b. Bitcoin has lower node scalability as compared to Standard BFT protocols
c. Standard BFT protocols never produces lower transaction throughput as compared to Bitcoin
d. Bitcoin-NG has higher node scalability as compared to Standard bitcoin protocols in general

Answer: (a), (d)

Detailed solution:
BFT is faster for small networks. Bitcoin NG decouples transaction serialization from leader election. Refer to 'Performance vs Scalability' in Week 8 Lecture Notes.

QUESTION 6

What is the primary function of a Fabric smart contract (Chaincode)?

a. Performing cryptocurrency mining
b. Defining the business rules and logic in the ledger
c. Defining consensus algorithms
d. Monitoring the transaction throughput

Answer: (b)

Detailed solution:
Fabric smart contracts define common data, rules and processes for businesses to transact through the ledger.

QUESTION 7

Which API is used for implementing Fabric chaincodes?

a. hyperledger-client-api
b. smart-contract-builder
c. fabric-contract-api
d. fabric-identity-manager

Answer: (c)

Detailed solution:
fabric-contract-api is used for implementing chaincode in Hyperledger Fabric.

QUESTION 8

Which of the following is/are true regarding fabric transactions?

a. The transactions should be endorsed by peers
b. The transactions are committed without validation
c. A transaction does not change the world state
d. World state holds current updated consensus view

Answer: (a) and (d)

Detailed solution:
In Hyperledger Fabric, transactions are endorsed by peers and are committed only after validation. Also, a transaction can update the world state.

QUESTION 9

Which of the following factor(s) limits Bitcoin's scalability?

a. Low transaction fees
b. Fixed block size
c. Wallet address complexity
d. Fixed block frequency

Answer: (b) and (d)

Detailed solution:
Bitcoin's scalability is limited due to its fixed block size and block frequency. Refer to Week 8 lecture notes.

QUESTION 10

Which of the following is/are correct regarding Schnorr Multisignature in CoSi protocol?

a. It is difficult to verify the signature
b. Signature can be verified using a single collective public key
c. It is easy to verify the signature
d. It relies on group G of any composite order

Answer: (b) and (c)

Detailed solution:
In the Cosi protocol, Schnorr Multisignature is easy to verify by using a single collective public key. Also, it relies on a group of prime order.