NOC22-CS44: Blockchain and Its Applications
Assignment 10

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. Alice has an account in the Ethereum network and wants to transfer ETH to Bob who has an account in the bitcoin network. Is it possible to do so?
    a. Yes, it is always possible
    b. No it is not possible
    c. Yes, possible via a trusted third party
    d. None of the above

    Cross Chain Asset Transfer is possible via TTP

3. One major issue with TTP based Asset Transfer is, it is very slow. True or False
    a. True
    b. False

    In TPP once the deposit is done, the transfer to the destination network is often very fast (in milliseconds).

4. One of the advantages of TTP based Asset Transfer is, it is very secure and no money has been stolen from here till date. True or False?
    a. True
    b. False

    Centralised exchanges were compromised and stolen many times.

5. What are some of the issues that exist in Asset Exchange?
    a. Synchronisation among sender and receiver networks
    b. Agreement of exchange rates
    c. Denial of Service
    d. All of the above

Refer to Week 10 Lecture Notes

6. What is an escrow?
    a. Escrow is an agreement in which assets are held and distributed when conditions are met
    b. Escrow is payment for smart contracts
    c. Escrow is a permissioned blockchain
    d. Escrow is cost of execution of smart contracts

Without the presence of any Escrow, the funds are in control of the sender and receiver parties.

7. Which of the following are guaranteed in the atomic swap protocol ?
    a. All swaps will take place only when all parties conform to the protocol
    b. If some parties deviate from the protocol, then all conforming party ends up worse off
    c. No coalition has an incentive to deviate from the protocol
    d. All of the above

Refer to Week 10 Lecture Notes.

8. Can Alice send 1 BTC to its own account using timelocked contract.
    a. No the target account should be different from the sender
    b. Yes she can send to her own account
    c. Only possible if she wants to send more than 1 BTC
    d. It depends on the time value mentioned in the contract.

Because, Timelocked contract restricts the spending/transfer of some currency until a specified future time. Block height may be used as a proxy for time.

9. Suppose Alice has a timelocked contract as:

    Funding Contract - 1 BTC
    Hash: **...Fa4509**
    Timeout: **2Δ**

    What will happen if Alice refuses to reveal the key and timeout occurs?
    a. 1 BTC refunded to Alice
    b. 1 BTC transferred to target account
    c. BTC less than 1 refunded to Alice as Some BTC deducted as penalty.
    d. BTC less than 1 transferred to target account

Refer to Week 10 Lecture Notes.

10. Which of the following statements is valid for Multi-Party Atomic Cross-chain Swap where Alice, Bob and Carol are the parties?
    a. If Alice halts while contracts are being deployed, then all contracts eventually time out and trigger refunds
    b. If Alice halts during triggering of contracts, all the three parties ends up worse off
    c. If Bob halts while contracts are being deployed, then Bob's contracts eventually time out and trigger refunds
    d. If Carol halts during triggering of contracts, only Carol ends up worse off

Refer to the Week 10 Lecture Notes.

NOC22-CS44: Blockchain and Its Applications
Assignment 11

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

1. In which attack, the attacker initially populates the victim node's peer tables with attacker's IP addresses
    a. Eclipse Attack
    b. Selfish Mining Attack
    c. 51% Attack
    d. Front-runnung Attack

    In Eclipse Attack, attacker populates tables with attacker IPs so that the victim node only connects to the attacker IPs.

2. Which of the following can be used to identify a good blockchain use-case ?
    a. Participants
    b. Assets
    c. Transactions
    d. Independent of everything

    A business problem, an identifiable business network consisting of participants, assets and transactions and need for trust is helpful to identify a good blockchain use-case.

3. Alice is performing an Eclipse Attack, and If her IP replaces another attacker IP, the evicted IP is resend and eventually replaced by honest IP. Is this a valid statement?
    a. Yes
    b. No

4. Which of the following is not a risk in blockchain operation mechanism.
    a. 51% vulnerability
    b. Transaction privacy leakage
    c. Double spending
    d. Birthday attack

    Refer to Week 11 Slide for “Risk in Blockchain”

5. In a selfish mining attack, discovering more blocks by pool develops a longer lead on the public chain, and continues to keep these new blocks _____
    a. Private
    b. Public

    Refer to Week 11 Slide for Selfish Mining Attack

6. When a node can be restarted?
    a. Power failure
    b. Network failures
    c. Security updates
    d. DoS attacks

It is normal that a node can be restarted in all the above scenarios.

7. What is a major problem with Proof Of Work?
    a. It is difficult to implement
    b. It is unreliable
    c. Multiple miners have to be rewarded
    d. It is CPU-intensive and consumes enormous amounts of power.

    Proof of Work is based on solving complex mathematical puzzles to validate the transaction. For this powerful computers are required and inherently they consume a lot of energy. Also to maintain and run such computers comes with additional cost associated with it.

8. In Practical Byzantine Fault Tolerance, ___.
    a. A master node selects the next node that adds the next block
    b. The node with most coins is chosen for adding the next block
    c. The nodes elect a leader and that leader adds the next block
    d. None of the above

    Even if malicious nodes are present in the system, pBFT can then also work. Because the nodes are sequentially ordered with one node being the the leader and others as backup nodes. The ultimate aim is to reach consensus by the help of all honest nodes.

9. Transaction rate on bitcoin blockchain is a main concern for many practical applications?
    a. True
    b. False

10. List two solutions for improving scalability ?
    a. Larger block size and on-chain transactions
    b. Larger block size and off-chain transactions
    c. Smaller block size and on-chain transactions
    d. Smaller block size and off-chain transactions

    First Layer of solutions provides improvement in the key properties and attributes of the blockchain network, like increasing the block size or decreasing the block verification time. Second Layer scalability solution provides Off-chain scaling. Second Layer solutions are the extra protocols that are installed on top of the main blockchain, and used for ‘offloading’ transactions off the main blockchain.

NOC22-CS44: Blockchain and Its Applications
Assignment 12

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

1. Can blockchain help in maintaining medical records.?
    a. Yes
    b. No
    c. Not Always

    It is one of the use cases of blockchain networks.

2. In a medicine supply chain business network, who can be the participants?
    a. Drug manufacturers
    b. Wholesale distributors
    c. Doctors
    d. Patients

    In the Pharma or Medicine supply chain the Manufacturers collect the raw materials, prepare the product or medicine and package it and send them to wholesale distributors, which transfer the medicine to hospitals, clinics, pharmacies or drug stores, from where the patient makes the purchase.

3. In a medicine supply chain business network, what can be the assets?
    a. Medical equipments
    b. Pharmaceutical Inventory
    c. Ultrasound equipment
    d. Hospital

    Hospital is one of the participant in medicine supply chain not an asset.

4. In a medicine supply chain business network, what can be the transactions?
    a. Transfer drug
    b. Distribute drug
    c. Sell drug boxes
    d. All of the above

    A manufacturer transfers the drug to distributors, the distributors distribute it to various stores and stores sell the drugs. Hence all of the above is correct.

5. What is the correct order of phases in Project Ubin?
    i. Cross-border Payment versus Payment (PvP)
    ii. Tokenized SGD
    iii. Delivery versus Payment (DvP)
    iv. Re-imagining RTGS
    v. Enabling Broad Ecosystem Collaboration
        a. i, ii, iii, iv, v
        b. ii, iv, iii, i, v
        c. ii, iii, v, vi, i
        d. i, iii, v, ii, iv

    Refer to Week 12 Slide for detail explanation of Project Ubin

6. In which of the attacks, end-user consumers can create multiple accounts/identities for accessing the consortium services?
    a. Byzantine faults
    b. Sybil attacks
    c. Impersonation attacks
    d. Sensitive information Leakage

    Refer to Week 12 slide for Threat Model

7. To allocate consumer requests among Service Providers, which of the following scheduling algorithms is implemented?
    a. Fair Scheduling Algorithm
    b. Capacity Scheduling Algorithm
    c. Dynamic Round Robin
    d. A* Algorithm

    In Cloud Federation to allocate consumer requests among Service Providers, Fair scheduling algorithm is implemented. Each SP will be allocated the number of consumer requests proportional to its infrastructure contribution in the federation.

8. Quorum supports transactions with
    a. Only private state
    b. Only public state
    c. Both private and public state at the same time
    d. Either private or public state for a transaction

    In Quorum a transaction has to be either public or private. If the transaction is private all the data within that transaction is private for that set of entities in the blockchain. Public transactions are transactions where the payload is visible to all participants.

9. 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

    The nodes elect themselves as a committee member by winning a local computation which makes the protocol to have good performance while allowing anyone in the network to participate.

10. What are the advantages of Hyperledger?
    a. Open source
    b. Identities of parties must be known
    c. Private channels
    d. None of the above

    In Hyperledger, identities of parties are not required to be known apriori.