NOC22-CS44: Blockchain and Its Applications
Assignment 10

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

1. Which of the following statements is true for PBFT. Choose the best possible answer
    a. It requires a core non consensus group
    b. For scalability, it always requires O(n) for communication complexity
    c. It is not possible to create multiple pseudonymous identities to subvert the 3f+1 requirements of PBFT
    d. None of the above

    In PBFT 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 without any external help
    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. Which of the following denotes properties of Hashed Timelock Contracts?
    a. If the secret is not revealed, the transaction creator cannot get back the fund even after timeout
    b. Spending of fund is blocked till the secret is publicly revealed or timeout occurs
    c. If timeout occurs, all the parties have distributed the funds equally
    d. Fund goes to the intended fund recipient after timeout occurs If the secret is not revealed

4. One of the advantages of centralized TTP-based Asset Transfer is it is very secure and always considered reliable. True or False?
    a. True
    b. False

    Centralized exchanges were compromised and stolen many times.

5. What are some of the issues that exist in Asset Exchange?
    a. Synchronization problem 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? Select the best possible and concrete answer
   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 ideal 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 her own account using a time locked contract.
   a. No the target account should be always 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, Time Locked 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 time locked contract with a target account 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 is used as a public permissioned ledger based DID registry?
    a. Hyperledger Indy
    b. Bitcoin
    c. Ethereum
    d. Sidetree