NOC22-CS44: Blockchain and Its Applications
Assignment 4

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

1. After a hard fork, the emerging two chains are incompatible. True or False?
    a. True
    b. False

    Hint: After adding a new rule to the code, it creates a fork in the blockchain: one path follows the updated blockchain, and the other path continues along the old path, hence incompatible with each other. After a short duration, those on the old chain will realize that their version of the blockchain is outdated and quickly upgraded to the latest version.

2. Which is/are the possible example/s of a double-spending attack?
    a. Sammy has a total of 90 unspent bitcoins from two different transactions with an equal amount of bitcoins each. He tries to send the entire amount at a time each to Nikita and Ayush as transactions

    b. Brady bought a car using ‘m’ bitcoins. On delivery, the bitcoins are transferred from his wallet to the dealer’s wallet.

    c. Karan has 180 unspent bitcoins. He sends the equal amount each to Dev and Tarun one by one

    d. Deepak has 20 unspent bitcoins. He tries to transfer those 20 bitcoins to his two each of his friends simultaneously.

    Hint: Double spending is when a person tries to use the same bitcoin for more than one Transaction knowingly or accidentally.

3. Blocks of a blockchain?

    a. Transaction data
    b. Hash
    c. Time stamp
    d. None of the above

    Hint: All of a,b,c

4. What are some Bitcoin exchanges available in India*: Please select the most appropriate choice among the options.*
    a. BuyUCoin

b. ZebPay
c. WazirX
   i. a and b
   ii. b and c
   iii. a and c
   iv. a, b and c

Hint: Refer to this post.All of a,b.c are correct.

5. “We can achieve consensus with a single crash failure in a perfect asynchronous network.” This scenario is ___________?

   a. Always true
   b. Sometimes true
   c. Can’t say
   d. Impossible

   Hint: As The Impossibility Theorem states Consensus is not possible in a perfect asynchronous network even with a single crash failure

6. What is the correct order of adding a new block to blockchain
   i. Block Mining
   ii. Block propagation
   iii. Block Flooding
   iv. Transaction Flooding

   a. iii, iv, ii, i
   b. iv, i, iii, ii
   c. iv, iii, ii, i
   d. ii, i, iii, iv

   Hint: Refer to Week 4 Slide

7. Double spending is reusing digital assets intentionally or inadvertently. True or False?
   a. True
   b. False

   Hint: Double spending is when a person tries to use same bitcoin for more than one Transaction knowingly or accidentally.

8. The primary difference between the permissionless and permissioned blockchain is ____________?

   a. Hash Algorithms
   b. Confidentiality
   c. Availability
   d. Access control for the participants in the blockchain network

   Hint: Permissionless blockchain is an open network, e.g. bitcoin, anyone can join, transact, leave, and rejoin the network whereas permissioned blockchain is a closed network e.g. Hyperledger. Both networks use the same hash algorithms and Offer confidentiality and availability.

9. What is an advantage of a permissionless blockchain?
    a. It does not use disinterested third parties to secure blocks, as all participants have a vested interest.
    b. It is open to everyone in the world without permission and approval requirements.
    c. It is more resilient against fraud because it uses federated nodes to combat fraud.
    d. Its networks are built by for-profit companies and the working of the network is guaranteed.

    Hint: Refer to the Week 4 Slide

10. Bitcoin protocol directly runs over

    i. TCP
    ii. HTTP
    iii. HTTPS

    a. i, ii, iii
    b. Only ii
    c. Only i
    d. All of the above

    Hint: Bitcoin protocol runs over TCP as reliability is required for transactions.