NOC22-CS44: Blockchain and Its Applications
Assignment 4

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

1. "We can achieve consensus with a single crash failure in a perfect asynchronous network." This scenario is ___________?

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

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

2. Which is/are the example/s of a double-spending attack?

   a. Anwesha has a total of 60 unspent bitcoins from two different transactions with an equal amount of bitcoins each. She sends the entire amount each to Arpita and Ankur from one of the transactions
   b. Bobby bought a bike using 't' bitcoins. On delivery, the bitcoins are transferred from his wallet to the shopper 's wallet. Simultaneously, he uses that bitcoins for another purchase
   c. Bibhu has 140 unspent bitcoins. He sends the entire amount each to Deepak and Tanmay
   d. Deepak and Bibhu each have 70 unspent bitcoins. Both of them transfer 20 bitcoins to each other

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

3. 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, iii, ii, i
   c. ii, i, iii, iv
   d. iv, i, iii, ii

   Hint: Refer to Week 4 Slide

4. 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.

5. In the blockchain, cryptography ensures the authenticity of a transaction and also helps prevent double-spend. Is the above statement True or False?
   a. True
   b. False

   Hint: Cryptography techniques enforce strong integrity of its transaction record and the validation in the longest chain prevents double spending in blockchain

6. What are Bitcoin exchanges available in India:
   i. BuyUCoin
   ii. ZebPay
   ii. WazirX
      a. i and ii
      b. ii and iii
      c. i and iii
      d. i, ii and iii

   Hint: Refer to this post.

7. The primary difference between the permissionless and permissioned blockchain is ____________?
   a. Access control for the participants in the blockchain network
   b. Hash Algorithms
   c. Confidentiality
   d. Availability

   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.

8. 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 more resilient against fraud because it uses federated nodes to combat fraud.
   c. It is open to everyone in the world without permission and licensing requirements.
   d. Its networks are built by for-profit companies and the working of the network is guaranteed.

   Hint: Refer to the Week 4 Slide

9. 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.

10. Bitcoin protocol runs over

    i. TCP
    ii. UDP
    iii. HTTP
    iv. HTTPS

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

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