NOC22-CS44: Blockchain and Its Applications
Assignment 4

Correct choices are highlighted in <mark>Yellow</mark>. Give partial marks for partially correct answers.

1. Double spending is reusing digital assets intentionally or inadvertently. True or False?
   a. <mark>True</mark>
   b. False

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

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

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

3. Which is/are the example/s of the double-spending attack?
   a. <mark>Anita has a total of 80 unspent bitcoins from two different transactions with an equal amount of bitcoins each. She sends the entire amount each to Deepak and Tanmay from one of the transaction</mark>
   b. <mark>Bibhu bought a car using 'p' bitcoins. On delivery, the bitcoins are transferred from his wallet to the shopper's wallet. Simultaneously, he uses that bitcoins for another purchase</mark>
   c. Anita and Bibhu each have 40 unspent bitcoins. Both of them transfer 20 bitcoins to each other
   d. <mark>Bibhu has 40 unspent bitcoins. He sends the entire amount each to Deepak and Tanmay</mark>

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

4. The primary difference between the permissionless and permissioned blockchain is _____?
   a. <mark>Access control for the participants in the blockchain network</mark>
   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 the network uses same hash algorithms and offer confidentiality and availability.

5. 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

6. 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 realise that their version of the blockchain is outdated and quickly upgraded to the latest version.

7. Which transaction(s) is/are valid with the current blockchain?
   a. No conflict with other transactions
   b. No double spending
   c. No infinite loops
   d. All of the above
   Hint: Refer to the Week 4 Slide

8. Bitcoin protocol runs over
   a. TCP
   b. UDP
   c. HTTP
   d. HTTPS
   Hint: Bitcoin protocol runs over TCP as reliability is required for transactions.

9. What it 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 the Week 4 Slide

10. What are Bitcoin exchanges available in India:
    a. Coinbase
    b. CoinDCX

c. UNOCoin
d. CoinSwitch Kuber

Hint: Refer to this post.