NOC22-CS44: Blockchain and Its Applications
Assignment 5

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

1. What is the limitation of using the consensus algorithm Proof of Work (PoW) with respect to Proof of Elapsed Time (PoET) ?
    a. PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.
    b. PoET has generally lower transaction costs than PoW
    c. PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.
    d. PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

Hint: PoET has lower transaction costs than PoW due to the hardware required for PoET is more specific than the hardware needed for PoW. Also the lower no of competing nodes makes PoET faster than PoW.

2. "A low-cost and fast consensus algorithm, where a node needs to deposit cryptocurrency to guarantee the transaction." The above description defines which consensus algorithm?
    a. Proof of Work (PoW)
    b. Proof of Burn (PoB)
    c. Proof of Stake (PoS)
    d. Proof of Elapsed Time (PoET)

    Hint: Refer to the Week 5 Lecture slide for definition of PoS.

3. What is the correct sequence involved in a block creation:
    1. Transactions validated
    2. Transactions Bundled & broadcasted
    3. Transaction initiated
    4. Block added to the local chain and propagated to the network.
    5. Proof of work consensus problem solved
        a. 5,3,1,2,4
        b. 1,2,3,4,5
        c. 3,1,2,5,4
        d. 3,2,1,4,5

    Hint:

1. First a transaction is initiated i.e. a block representing the transaction is created
2. The block is sent to every nodes in the network, which validate the transactions
3. The validated transactions bundled and broadcasted in the network
4. The miner tries to solve the PoW consensus problem
5. Finally the block is added to the local chain and propagated to the network.

4. Proof of Burn consensus algorithms consider virtual resources or digital coins for participating in the mining activity? True or False?
    a. True
    b. False

    Hint: Proof of Burn consensus algorithms consider virtual resources or digital coins for participating in the mining activity unlike PoW which used real resource.

5. 1 ether equals
    a. 10 ^ 16 wei
    b. 10 ^ 18 wei
    c. 10 ^ 6 wei
    d. 10 ^ 8 wei

    Hint: Ether to Wei converter: https://eth-converter.com/

6. How an attacker could manipulate the transaction history of a blockchain to be able to spend a token or a cryptocurrency twice.
    a. The attacker modified the transaction on his node and propagated it in the network.
    b. The attacker modified the smart contract and recovered the investor's cryptocurrency.
    c. The attacker gained control of more than 51% of the network's computing power.
    d. The attacker hard-forked the network and created a new blockchain network.

    Hint: Refer to the Week 5 Lecture slide for 51% attack.

7. What is the CLI command used to send ethers after the nodes have been initialized?
    a. eth.submitTransaction()
    b. eth.sendIBANTransaction()
    c. eth.sendRawTransaction()
    d. eth.sendTransaction()

    Hint: Once the transaction is prepared using syntax

    var **transaction** = {from: "0x7dad3a076678a05b2b4e2b93206dbecef0d7b0",
    to:"0x35F18427567108F800BDC2784277B9246eED3A" ,
    value: Web3.utils.numberToHex(10000000000000000) },

    it can be sent using:

    web3.eth.sendTransaction(transaction).then(console.log)

8. What library/API is used for smart contract deployment and invocation from Dapp ?
    a. web3
    b. admin
    c. eth
    d. Contract

    Hint: web3 is the Collection of libraries that allow you to interact with a local or remote ethereum nodes

9. In which scenario is a smart contract the best solution to the problem?
    a. A restaurant manager wants to force customers to pay for their food by transferring cryptocurrency to his wallet.

b. A chief engineer wants her smart watch to notify her when her partner enters their front door.
c. A grid company wants to automatically buy power when the price reaches a predetermined rate.
d. An insurance company wants to pay out a small vendor whenever the case manager feels it is best to do so.

Hint:
Option a is incorrect. Because Smart contracts do not force another party to transfer funds.
Option b is incorrect. Because a smart contract is a contract between two or more parties. Here, there is no second party, hence a smart contract is not suitable.
Option d incorrect. Because, Smart contracts get triggered by events that are predetermined. The willingness of a company does not automatically trigger the code.

10. Which of the following syntax is correct to write data in a smart contract using solidity
    a. myContract.methods.store("99").send()
    b. myContract.methods.write("99").send()
    c. myContract.methods.write("99").set()
    d. myContract.methods.store("99").set()

Hint: Please refer to the Week 5 Lecture slides on how to execute smart contract.