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)?
    a. A lot of mining power is wasted as only one gets success in mining at a time
    b. PoW is used for permissioned blockchain
    c. Low transaction throughput
    d. It is used for blockchain mining

Hint: Please refer to the slide Week 5 slide. The PoW has limitation of wastage of power and low throughput.

2. Which statement(s) is/are true for PoS(Proof of Stake) consensus?
    a. Depends on the work done by the miner
    b. Depends on the amount of crypto currency the miner holds
    c. Provides less protection in general
    d. None of the above

Hint: Refer to the Week 5 Lecture slide for description of PoS. Amount of bitcoin that the miner holds decides its stake.

3. Which of the following is/are applicable for PoET(Proof of Elapsed Time) consensus
    a. Each participant in the blockchain network waits a random amount of time
    b. The first participant to finish becomes the leader for the new block
    c. Trusted execution platform and attestation are used to verify that the proposer has really waited
    d. None of the above.

Hint:POET uses a trusted execution platform, say as Intel SGX and H/W attestation. Please refer to the slide for details.

4. Proof of Burn consensus algorithms do not consider virtual resources or digital coins for participating in the mining activity?
    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 uses real resources.

5. 5 ether equals
    a. 5X(10 ^ 16) wei
    b. 5X(10 ^ 8) wei
    c. 5X(10 ^ 6) wei
    d. 5X(10 ^ 18) wei

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

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

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

7. 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 hard-forked the network and created a new blockchain network.
    b. The attacker modified the transaction on his node and propagated it in the network.
    c. The attacker modified the smart contract and recovered the investor's cryptocurrency.
    d. The attacker gained control of more than 51% of the network's computing power.

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

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

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

9. 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)

10. 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.