NOC22-CS44: Blockchain and Its Applications
Assignment 3

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

1. Bitcoin mining is performed by ____.
    a. Miner nodes
    b. Internal Nodes
    c. External Nodes
    d. Orphan Nodes

Hint: Bitcoin mining is proposed by Miner nodes.

2. DLT can be used to maintain financial information only.
    a. False
    b. True

Hint: DLT can even be used to store various types of information, codes, etc., apart from financial data. Please refer to the slide.

3. Which of the following is/are true for basic PoW consensus?
    a. Miner needs to propose a block
    b. The miner needs to solve a puzzle to obtain target block hash
    c. The puzzle solution is added as proof for leadership
    d. Successful miner node is rewarded

Hint: All of the above are true for general PoW consensus. Please refer to the slide.

4. Bitcoin Scripting Language:
    a. Not Turing Complete
    b. Supports Cryptography
    c. Stack Based
    d. Supports infinite time/memory

Hint: Bitcoin Scripts are simple, compact, stack-based, support cryptography, and not Turing complete.

5. Permissioned blockchain is regarded as more secure than open blockchain as the participants are known beforehand and pre-authenticated.
    a. True
    b. False

Hint: Please refer to the slide. Permissioned blockchain is closed network among known pre authorized participants and more secure from unknown nodes.

6. What is nonce?
    a. The transaction id number

b. A miners ASIC chip array
c. The generator point used in elliptic curve cryptography

d. The number miners run through to generate a correct hash

Hint: Miners propose new blocks by solving the puzzle i.e., finding the nonce corresponding to a target block hash, and add that solution as proof. of solving the challenge to be the leader

7. Which one of the following opcodes is needed to remove the top stack item.
   a. OP_POP
   b. OP_DEQUE
   c. OP_DROP
   d. OP_DELETE

   Hint: Refer https://en.bitcoin.it/wiki/Script to get to know more opcodes.

8. Which of these fields is present in a Bitcoin block summary?
   a. Difficulty
   b. Gas Used
   c. Gas Limit
   d. Private Key of the Sender

   Hint: The bitcoin block header contains mining statistics timestamp, nonce and difficulty

9. If the four-byte difficulty bits in hex form are 0x1b0404cb, and the target value is calculated using X * 2^(Y), what is the values for X and Y respectively,
   a. X = 0x0404cb, Y = 0x1b
   b. X = 0x0404cb, Y = 0x18
   c. X = 0x0404cb, Y = 0xc0
   d. X = 0x1b0404, Y = 0xcb

   Hint: In difficulty = 0x1b0404cb, the exponent is 1b and coefficient is 0404cb
   Target = 0x0404cb * 2^(0x08 * (0x1b - 0x03))
   On solving the above equation
   ⇒ target = 0x0404cb * 2^(0x08 * 0x18)
   ⇒ target = 0x0404cb * 2^(0xc0)

10. In bitcoin block header, the block identifier is calculated

    a. Using SHA256 on the current block header
    b. Using Double SHA256 on the previous block hash
    c. Using Double SHA256 on the Difficulty bits
    d. Using Double SHA256 on the current block header

    Hint: Block identifier is calculated by using Double SHA256 algorithm on the current block header