NOC22-CS44: Blockchain and Its Applications
Assignment 3

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

1. The transaction Merkle Tree root value in a Bitcoin block is calculated using ____.
   a. Number of transactions
   b. None
   c. Previous block’s hash
   d. Hash of transactions

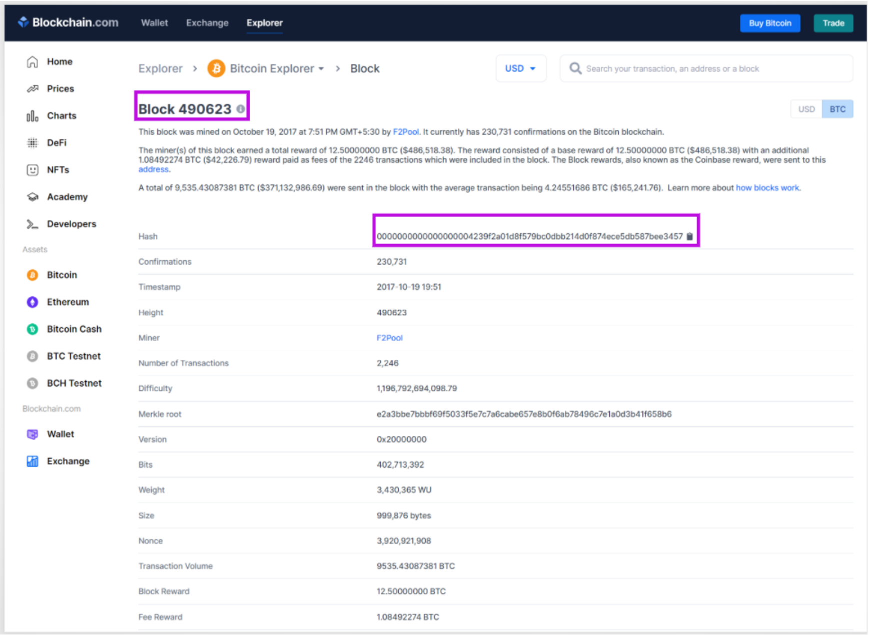
Hint: Transactions are organised as a Merkle Tree. The Merkle Root is used to construct the block hash

2. Proof of work is the __________ used by Bitcoin blockchain and Ethereum Byzantium Metropolis blockchain.
   a. Transaction confirmation
   b. Incentive function
   c. Consensus Protocol
   d. Trust function

   Hint: In 2008, the whitepaper titled, “Bitcoin: A peer to peer Electronic Cash System” got floated in the internet, in which they used the Proof of Work or Nakamoto Consensus as the consensus protocol.

3. Inspect and explore block #490624 using this link to solve the below question. What is the hash of the previous block for Bitcoin block #490624? Copy and paste the answer into the box below.
   Ans: 0000000000000000004239f2a01d8f579bc0dbb214d0f874ece5db587bee3457

Hint:



Block 490623

This block was mined on October 19, 2017 at 7:51 PM GMT+5:30 by F2Pool. It currently has 230,731 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 12.50000000 BTC ($486,518.38). The reward consisted of a base reward of 12.50000000 BTC ($486,518.38) with an additional 1.08492274 BTC ($42,226.79) reward paid as fees of the 2246 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 9,535.43087381 BTC ($371,132,986.69) were sent in the block with the average transaction being 4.24551686 BTC ($165,241.76). Learn more about how blocks work.

Hash	0000000000000000004239f2a01d8f579bc0dbb214d0f874ece5db587bee3457
Confirmations	230,731
Timestamp	2017-10-19 19:51
Height	490623
Miner	F2Pool
Number of Transactions	2,246
Difficulty	1,196,792,694,098.79
Merkle root	e2a3bbe7bbbf69f5033f5e7c7a6cabe657e8b0f6ab78496c7e1a0d3b41f658b6
Version	0x20000000
Bits	402,713,392
Weight	3,430,365 WU
Size	999,876 bytes
Nonce	3,920,921,908
Transaction Volume	9535.43087381 BTC
Block Reward	12.50000000 BTC
Fee Reward	1.08492274 BTC

4. Bitcoin Scripting Language:
    a. Turing Complete
    b. Supports Cryptography
    c. Stack Based
    d. Supports infinite time/memory

    Hint: Bitcoin Scripts are FORTH like language: simple, compact, stack based and processed left to right.

5. Which of the following bitcoin scripts will generate a TRUE outcome?

    i. scriptSig: <sig>
    scriptPubKey: <pubKey> OP_DUP OP_HASH256 <pubKeyHash> OP_EQUAL OP_VERIFY OP_CHECKSIG

    ii. scriptSig: <pubKey>
    scriptPubKey: OP_HASH160 <pubKeyHash> OP_EQUAL

    iii. scriptSig: <pubKey>
    scriptPubKey: <pubKey> OP_EQUALVERIFY

    iv. scriptSig: <sig>
    scriptPubKey: <pubKey> OP_CHECKSIG
        a. i, ii, iii
        b. iii, iv
        c. i, ii, iv
        d. i, iii, iv

    Hint: Equality is checked between the top two items in the stack

6. What is nonce?
    a. The number miners run through to generate a correct hash
    b. The transaction id number
    c. A miners ASIC chip array
    d. The generator point used in elliptic curve cryptography

    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 a 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_DROP
    b. OP_POP
    c. OP_DEQUE
    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. Gas Used
    b. Gas Limit
    c. Difficulty
    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 Double SHA256 on the current block header
    b. Using SHA256 on the current block header
    c. Using Double SHA256 on the previous block hash
    d. Using Double SHA256 on the Difficulty bits

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