Blockchain and Its Applications 2024
Assignment 3

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

1. Inspect and explore block #828070 using this link to solve the below question. What is the hash of the previous block for Bitcoin block #828070? Copy and paste the answer into the box below.

   a. 0000000000000000000246ef8870310474e18acbd1fd8453abbb6f367f74816f

   b. 00000000000000000001d857c22ab5211e2173e4f970eb15f04f64e692587aa1

   c. 000000000000000000034511894ee97dfa62803bb338335a12e40f6e5a451720

   d. 00000000000000000002c2c0e69e794d1968382626109ed1d6441020105e7d4e

2. Which of the following Bitcoin scripts will generate a **TRUE** outcome?

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

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

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

   d. scriptSig: <sig>
   scriptPubKey: <pubKey> OP_CHECKSIG

   A. a, b, c
   B. c, d
   C. a, b, d
   D. a, c, d

3. In the 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

4. If the six-byte difficulty bits in the hexadecimal form are 0x1a05f20881ab, and the target value is calculated using X * 2^(Y), what are the values for X and Y respectively?

   a. X = 0x5f20881ab, Y = 0x1a
   b. X = 0x1a05f2, Y = 0x0881ab
   c. X = 0x1a05f2, Y = 0x18
   d. X = 0x5f20881ab, Y = 0x1a0

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

6. Which one of the following opcodes is needed to remove the second-to-top stack item?
   a. OP_DELETE
   b. OP_2POP
   c. OP_DEQUE
   d. OP_NIP

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

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

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

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