1. What are the features of a hash function?

    a. Puzzle-friendly
    b. Collision-resistance
    c. Deterministic
    d. Post image resistance

Hint: except d all are the properties of cryptographic hash functions.

2. For a SHA 256 bit hash function, the attacker needs to compute how many hash operations in order to find two matching outputs?

    a. 0.3×2^{128}
    b. 0.2×10^{50}
    c. $0.25X2^{130}$
    d. 1×2^{256}

Hint: If a hash function produces N bits of output, an attacker needs to compute only $2^{N/2}$ hash operations on a random input to find two matching outputs. $2^{256/2} = 2^{128} =$
=(0.25)X2^130

3. What is the hash value of 6666 if SHA-256 is used?
    a. d7697570462f7562b83e81258de0f1e41832e98072e44c36ec8efec46786e24e
    b. d7597570462f7562b83e81258de0g1e41832e98072e44c36ec8efec46786e24e
    c. c7697570462f7562b83e81258de0f1c41832e98072e44c36ec8efec46786e24e
    d. d7697570462f7562m83e81258de0f1e41832e98072e44c36ec8efec46786e24es

Hint: Verify the result https://emn178.github.io/online-tools/sha256.html

4. Which of the statements below is/are true for decentralized distributed systems?
    a. Players may or may not trust each other
    b. Players must trust each other
    c. Central body should govern the communication
    d. None of the above

Hint: Answer a. Every participant may not trust each other

5. Miner nodes only execute new transactions but can not verify previous transaction hash?
    a. True

b. False

Hint: Answer b. miners can verify previous transaction hash and create new transactions

6. Which of the following is/are true for blockchains?
   a. Works based on Push technique
   b. Existing data can be deleted easily
   c. Tamper-proof
   d. None of the above

Hint: Answer a,c.

7. Where are the ledger logs stored in a blockchain?
   a. On a SQL Database
   b. On a central immutable ledger
   c. On a metadata table
   d. In ledger of each peer

Hint: Each peer keeps the log

8. Which of the following is an avalanche effect to a cryptographic hash function?
   a. given the same message the hash function would not return the same hash
   b. it is not very difficult to generate the original message from the hash
   c. a small change in the message, impacts large change the hash value
   d. None of the above

Hint: answer is c.

9. Genesis blocks may not contain the
   a. First transaction
   b. First transaction block
   c. Last transaction block
   d. None of the above

Hint: answer is c. The Genesis block always contains the first transaction block but not necessarily the last one.

10. Which of the below is/are blockchain based app examples?
    a. Cross-border payments
    b. Supply chain
    c. Anti-money laundering tracking system
    d. UTXO

Hint: answer is a,b,c. UTXO is feature for handing unspent amount, it is not an blockchain app