Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 3 - Week 3 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

Number of questions: 10 **Total mark: 10 X 1 = 10**

QUESTION 1

If the current block reward for Bitcoin is 6.25 BTC, and the difficulty adjustment mechanism is such that, on average, a new block is found every 10 minutes, how much Bitcoin will be mined per day (24 hours)?

a) 75 BTC
b) 144 BTC
c) 900 BTC
d) 1,080 BTC

Answer: (c)

Detailed solution:
The block reward is **6.25 BTC**.
There are **144 blocks** mined in a 24-hour period (24 hours × 60 minutes / 10 minutes per block).
In one day, the total Bitcoin mined would be 144 × 6.25=900 BTC.

QUESTION 2

Which of the following best defines a **permissioned blockchain**?

a) Anyone can join and validate transactions without approval.
b) Only authorized participants can write and validate transactions.
c) It always uses proof-of-work (PoW) for consensus.
d) A permissioned blockchain does not need cryptographic hash operations

Answer: (b)

Detailed solution:
A permissioned blockchain restricts the ability to write or validate transactions to authorized participants. This controlled access enhances security and privacy within the network.

QUESTION 3

Which of the following combinations is correctly used to compute Bitcoin's current block hash?

a) Previous block's hash, Merkle root, block reward, nonce, timestamp, and block size
b) Previous block's hash, timestamp, nonce, Merkle root, difficulty bits, and block version
c) Block creator's public key, Merkle root, timestamp, block reward, nonce, and difficulty level
d) Previous block's hash, nonce, Merkle root, height, timestamp, and difficulty bits

Answer: (b)

Detailed solution:
Please refer to the Week 3 Lecture 13.

QUESTION 4

Which of the following difficulty targets would make it most difficult for miners to find a valid block?

a) 00000000000000000000000000000000000000000000000000000056789abcdef123
b) 0000000000000000000000000000000000000000000000000002dfe34a1b2c3d555
c) 00000000000000000000000000000000000000000000000000afc123987abc
d) 000000000000000000000000000000000000000000000000000af46789

Answer: (d)

Detailed solution:
The difficulty target with **52 leading zeros** (option **d**) is the most difficult for miners to find a valid block.
Therefore,000000000000000000000000000000000000000000000000000af46789 is the correct choice.

QUESTION 5

In the Bitcoin, block identifier refers to

a) SHA1 (128 bits) of the future block header
b) Double SHA256 of the current block header
c) Double SHA256 of the difficulty bits only
d) Triple SHA256 of the future block header

Answer: (b)

Detailed solution:
The Bitcoin block identifier (block hash) contains **Double SHA256** on the current block header. This means performing SHA256 twice. Please refer to the Week 3 Lecture 13.

QUESTION 6

In a Merkle tree with n transactions (n is a power of 2), if one transaction is invalid, how many recalculations are needed to detect and correct the invalid transaction?

a) $n/2$
b) $\log_2(n) + 1$
c) $n-1$
d) $3\log_2(n)$

Answer: (b)

Detailed solution:
The Merkle tree recalculates the hashes at each level up to the root for verification. This requires recalculating one hash at each of the $\log_2(n)$ levels, plus one final hash for the root.

QUESTION 7

Which of the following Bitcoin script opcode is needed to remove the second-to-top stack item?

a) OP_DELETE
b) OP_2POP
c) OP_DEQUE
d) OP_NIP

Answer: (d)

Detailed solution:
Bitcoin Script uses specific opcodes like OP_DROP, OP_NIP, etc., to manipulate the stack. OP_NIP is explicitly designed to remove the second-to-top stack item.

QUESTION 8

If a Merkle tree has 8 transactions, how many hashes are required to compute the Merkle root?

a) 8
b) 15
c) 16
d) 7

Answer: (b)

Detailed solution:
In a Merkle tree with 8 transactions, 7 additional hashes are needed to compute the Merkle root as pairs of transaction hashes are combined recursively at each level. The total hashes, including the leaves, are 15: 8 leaf hashes and 7 parent hashes.

QUESTION 9

What is a nonce in the context of Bitcoin mining?

a) The transaction ID number
b) A miner's ASIC chip array
c) The generator point used in elliptic curve cryptography
d) A value miners iterate through to generate a valid hash

Answer: (d)

Detailed solution:
In Bitcoin mining, the **nonce** is a random or arbitrary number that miners adjust in the block header during mining. This value is modified to change the resulting hash of the block header to meet the required difficulty target.

QUESTION 10

What happens if the number of transactions in a Merkle tree is odd?

a) The tree cannot be built
b) Dummy (duplicate) hashes are added to adjust
c) Transactions are left out of the block
d) The Merkle root is ignored

Answer: (b)

Detailed solution:
If the number of transactions is odd, pairs cannot be formed for the suitable structure of the Merkle tree. To fix this, dummy (duplicate) hashes are added to make the number of transactions even, allowing the tree to be constructed properly. Please refer to the Week 3 Lecture 14.