Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 1 - Week 1 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1

Which of the following statements is true regarding the foundational concepts of blockchain and cryptography?

a) Decentralization in blockchain ensures that a single authority controls the network for higher efficiency.
b) SHA-256 is a cryptographic hash function widely used in blockchain due to its fixed output size and collision resistance.
c) A hash chain is a sequence of cryptographic keys used to decode blockchain data.
d) Cryptographic hash ensures that the blockchain data cannot be read by anyone outside the network.

Answer: (b)

Detailed solution:
Option (b) is correct because SHA-256 is a cryptographic hash function with features like fixed output, pre-image resistance, and collision resistance, making it ideal for blockchain.

QUESTION 2

An attacker wants to find a collision in a cryptographic hash function with a 256-bit output. What is the approximate number of hash operations required to succeed?

a) 1×2^{128}
b) 0.75×2^{128}
c) 1×2^{256}
d) 0.5×2^{256}

Answer: (a)

Detailed solution:
Option (a) is correct because If a hash function produces □ bits of output, an attacker needs to compute only $2^{□/2}$ hash operations on a random input to find two matching outputs.$2^{256/2} = 2^{128} = 1 \times 2^{128}$

QUESTION 3

A blockchain network uses SHA-256 for its hashing process. If it takes 10^{-6} seconds to compute a single SHA-256 hash, how long would it take (approximately) to compute 2^{128} hashes for a collision attack?

a) 10^{10} years
b) 10^{15} years
c) 10^{20} years
d) 10^{25} years

Answer: (d)

Detailed solution:
Total time to compute 2^{128} hashes: $2^{128} \times 10^{-6} \approx 3.4 \times 10^{32}$ seconds.
Convert seconds to years: 1 year = 3.15×10^{7} seconds $\Rightarrow (3.4 \times 10^{32}) / (3.15 \times 10^{7}) \approx 10^{25}$ years.

QUESTION 4

In a decentralized distributed system with 100 participants, which of the following statements is true regarding trust and communication?

a) At least 50 participants must trust each other for the system to function.
b) A central body governing communication among all 100 participants is mandatory.
c) Participants may or may not trust each other, as the system ensures integrity using cryptographic protocols and agreement through consensus protocols.
d) All the 100 participants must trust each other.

Answer: (c)

Detailed solution:
Option (c) is correct because decentralized systems rely on cryptographic mechanisms and consensus protocols, making trust among participants unnecessary. Option (a) is incorrect, as trust among the participants is not a requirement for decentralized systems. Option (b) is incorrect, as decentralized systems operate without a central governing body.

QUESTION 5

A blockchain network achieves an average block generation time of 5 minutes under normal conditions. However, due to scheduled maintenance, the network's hash rate is reduced by 50% for 4 hours daily. If the network operates for 12 hours in total (including the maintenance period), how many blocks will be added to the blockchain?

a) 120
b) 200
c) 216
d) 240

Answer: (a)

Detailed solution:
For 8 hours at full efficiency: (60 min / 5 min) = 12 blocks/hour, so 12 × 8 = 96 blocks.
For 4 hours at 50% efficiency: (12 blocks / 2) 6 blocks/hours, so 6 × 4 = 24 blocks.
Total blocks = 96 + 24 = 120 blocks.

QUESTION 6

Where are the transaction logs stored in a blockchain network?

a) In a centralized SQL database.
b) On an immutable ledger controlled by a central authority.
c) In metadata tables on each peer.
d) In the distributed ledger of each peer across the network.

Answer: (d)

Detailed solution:
Blockchain transaction logs are stored in a **distributed ledger** across all peers (nodes) in the network, ensuring decentralization and immutability.

QUESTION 7

Which of the following describes the **avalanche effect** in a cryptographic hash function?

a) Given the same input, the hash function returns a different hash 99.99% of the time.
b) It takes 10^5 attempts to reverse-engineer the original message from the hash.
c) A small change in the input causes a drastic change in the hash, flipping nearly all the bits.
d) The hash function always returns the same hash for the same input.

Answer: (c)

Detailed solution:
The **avalanche effect** ensures that even a tiny change in the input (like flipping a single bit) results in a significantly different hash, with most of the output bits changing.

QUESTION 8

Which of the following statements accurately describes a **blockchain**?

a) A centralized database where data is stored on a single server.
b) A distributed ledger where data is stored across multiple nodes and is immutable.
c) A system that only stores cryptocurrency transaction data on a single node.
d) A network that uses a single user to control access and updates to the data.

Answer: (b)

Detailed solution:
A **blockchain** is a decentralized and distributed ledger system where data is stored across multiple nodes (computers), ensuring that no single entity has control. It is also immutable, meaning once data is recorded in a block, it cannot be altered without the consensus of the network.

QUESTION 9

Which of the following is/are possible use cases of blockchain technology?

a) Cross-border payments
b) Supply chain management
c) Centralized Anti-money laundering tracking system
d) Maintaining data over a single database server

Answer: (a) and (b)

Detailed solution:
Blockchain technology is used in cross-border payments, supply chain management, and decentralized anti-money laundering tracking systems for decentralization, transparency, and security.

QUESTION 10

In a blockchain using **SHA-256**, if the hashes of strings A and B are concatenated and then hashed again, what is the length of the final hash?

a) 256 bits
b) 512 bits
c) 128 bits
d) 1024 bits

Answer: (a)

Detailed solution:
SHA-256 always produces a fixed 256-bit hash, regardless of input size. Even after concatenating two hashes and rehashing, the output will still be a 256-bit hash.