Centurion University
Shaping Lives... Empowering Communities...

School: ..... Campus: .....

Academic Year: ..... Subject Name: ..... Subject Code: .....

Semester: ..... Program: ..... Branch: ..... Specialization: .....

Date: .....

Classroom Learning

(Learning by Listening and Observations)

Name of the Topic: Consensus Mechanism (PoW)

Learning Outcome:

Concepts learned (Mention 2/3 principles):

Based on the classwork, the principal concepts I have learned include:

1. The fundamental concept of Proof-of-Work (PoW) as a consensus mechanism that requires participants to perform computationally intensive work to validate transactions and create new blocks.
2. The complete architecture of the mining process, where miners compete to solve a cryptographic puzzle, and the first to succeed earns the right to add the next block to the blockchain.
3. The characteristics of PoW that ensure network security, including its resistance to Sybil attacks, the immutability of confirmed blocks, and the decentralized nature of achieving agreement.

* New techniques learned:

Additionally, I have acquired new knowledge in the following areas:

1. Techniques for understanding the cryptographic hash function (e.g., SHA-256 in Bitcoin) and how miners vary a nonce in the block header to find a hash value below a specific target difficulty.
2. Procedures for how the network adjusts the difficulty of the cryptographic puzzle periodically to maintain a consistent average time between blocks, regardless of the total network hash rate.
3. The process of block propagation and verification, where the solved puzzle is quickly verified by all other nodes, and the longest valid chain is accepted as the truth.
4. Methods for analyzing the economic incentives of PoW, where the block reward (newly minted coins) and transaction fees motivate miners to contribute honest computational power.

* Related Project/Practice work experienced and learned:

During the practice sessions of the lab work, I engaged in and developed proficiency with programs and simulations in the following areas:

1. Writing a basic Python program to simulate the mining process by repeatedly hashing block data with an incrementing nonce to find a hash with a predefined number of leading zeros.
2. Calculating the probability of a single miner finding a valid block hash based on their share of the total network hash rate.
3. Analyzing real Bitcoin block data from **Blockchain.com** to study the hash rate, difficulty, and nonce values of recently mined blocks.
4. Modeling a scenario to understand how a 51% attack becomes theoretically possible but economically infeasible as the network grows.

---

* New Software/Machine/Tool/Equipment/Experiment learned:

During the lab session, I used **Bitcoin Core** to sync with the blockchain and observe the PoW process. I also used online mining simulators and cryptographic hash calculators (like **SHA-256**) to understand the computational challenge visually.

* Application of concept(s) (preferably real life scenario):

1. **Network Security:** The immense computational power required to solve the puzzle makes it prohibitively expensive for any single entity to attack the network or alter transaction history, securing the blockchain.
2. **Decentralized Consensus:** PoW enables a distributed network of strangers to agree on the state of a ledger without needing a trusted central authority, enabling trustless transactions.
3. **Currency Distribution:** The block reward mechanism provides a fair and transparent way to distribute new coins into circulation, incentivizing miners to participate and secure the network from its inception.

---

* Case Studies/Examples:

1. **Bitcoin Mining:** The Bitcoin network, the largest PoW blockchain, uses an estimated 100+ Exahashes per second of computational power to secure over $1 trillion in value, making it the most secure computational network in the world.
2. **Energy Consumption Debate:** The significant electricity usage of PoW mining has led to a global debate on its sustainability, pushing innovations in using stranded energy (e.g., flared gas) and renewable sources for mining operations.
3. **Resistance to Censorship:** PoW makes Bitcoin censorship-resistant. For example, during the 2020 Nigerian protests against police brutality, protestors used Bitcoin to receive donations after the government froze their traditional bank accounts.

Assessment:

Marks Obtained: ..... / 10

Signature of the Faculty:

Signature of the Student:

Name : PN Archana

Regn. No. : 240720100147

**As applicable according to the topic.*
One sheet per topic (10-20) to be used.