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

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

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

Date: .....

Applied and Action Learning

(Learning by Doing and Discovery)

Name of the Experiement : Security First – Understanding Blockchain

* Coding Phase: Pseudo Code / Flow Chart / Algorithm

- **Initialize Blockchain Network:**

Set up nodes, miners/validators, and communication channels within a decentralized network.

- **Monitor Network Activity:**

Observe how transactions are broadcast, verified, and added to blocks.

- **Introduce Vulnerability Scenario:**

Simulate conditions such as high control power, fake node creation, or delayed transaction validation.

- **Trigger Attack Simulation:**

Attempt an attack (e.g., 51% or double-spend) by exploiting the introduced vulnerability.

- **Record System Response:**

Analyze how the network handles the malicious activity — detection, delay, or consensus reformation.

- **Apply Security Measures:**

Use defense mechanisms like stronger consensus rules, node verification, and enhanced encryption.

- **Validate Network Recovery:**

Ensure that after countermeasures, the blockchain resumes normal, secure operations.

Software used:

1. VS Code.
2. MS Word.
3. Brave for researching.

*As applicable according to the experiment.
Two sheets per experiment (10-20) to be used.

* Implementation Phase: Final Output (no error)

- Blockchain network is initialized with multiple nodes.
- Normal transaction flow and block creation are observed.
- A specific attack scenario (e.g., Sybil or 51% attack) is introduced.
- Network disruption or delayed confirmation is noticed.
- The system applies preventive measures (e.g., stake limits, identity verification).
- Blockchain resumes stable operation with secure consensus restored.
- Final output confirms that **security protocols successfully defend against threats**.

* Observations:

- Blockchain's security mainly depends on consensus integrity and node honesty.
- Attacks often exploit network control, code loopholes, or human error.
- Implementing multi-layer verification and audited smart contracts reduces vulnerabilities.
- Proof of Stake and Proof of Authority systems offer better protection than traditional PoW in some cases.
- Continuous monitoring and security audits are essential to prevent evolving threats.

*As applicable according to the experiment.
Two sheets per experiment (10-20) to be used.

ASSESSMENT

Rubrics	Full Mark	Marks Obtained	Remarks
Concept	10		
Planning and Execution/ Practical Simulation/ Programming	10		
Result and Interpretation	10		
Record of Applied and Action Learning	10		
Viva	10		
Total	**50**		

Signature of the Student:

Name :

Regn. No. :

Signature of the Faculty:

**As applicable according to the experiment.*
Two sheets per experiment (10-20) to be used.