Centurion University

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 experiment: Blockchain in Supply Chains – Use Case Analysis

*Coding Phase: Pseudo Code / Flow Chart / Algorithm

1. Participant Identification:
Identify the key parties in the supply chain: Manufacturer, Supplier, Transporter, Distributor, Retailer, and Customer.
2. Product Tokenization:
Every product is assigned a unique identifier or token on the blockchain (e.g., Product ID #B456 created by the manufacturer).
3. Transaction Recording:
Each movement (manufacturing, shipping, sale) is logged as a separate block on the blockchain. The block includes:

- Product ID
- Sender & Receiver details
- Timestamp
- Transaction data
- Digital signature for verification

4. Validation & Verification:
Transactions are validated by nodes on the blockchain network, ensuring only legitimate data is added.
5. Linking & Hashing:
Each block is cryptographically linked to the previous one, ensuring the data remains secure and immutable.
6. Consensus Protocol:
A consensus mechanism, like Proof of Stake, is used to confirm transactions, ensuring data consistency across all nodes.
7. Traceability:
All stakeholders can access the complete product journey, from production to final sale.
8. Auditing & Transparency:
The blockchain serves as an immutable ledger for proof of authenticity, offering transparency for regulators, businesses, and customers.

* Softwares use

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)

* The blockchain system is launched with several connected nodes.
* Usual activities such as transaction processing and block creation are monitored.
* A test attack (like Sybil or 51% attack) is simulated to assess system security.
* Network issues such as slow processing or transaction delays are observed.
* Security measures like staking restrictions and node verification are applied.
* The blockchain returns to a steady state with its consensus mechanism functioning correctly.
* The final results show that the security methods effectively protected the network from the attack.
*

* Observations

The safety of a blockchain relies on the reliability of its consensus mechanism and the trustworthiness of participating nodes.

Most attacks take advantage of weak points in the network, software bugs, or user mistakes.

Using multiple verification layers and regularly audited smart contracts helps minimize security risks.

Consensus models like Proof of Stake (PoS) and Proof of Authority (PoA) can provide stronger protection compared to traditional Proof of Work (PoW).

Ongoing system checks and regular security assessments are vital to defend against new and emerging threats.

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

ASSESMENT

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.