Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

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 attacks

* Coding Phase: Pseudo Code / Flow Chart / Algorithm

ALGORITHMS:

1. Study the basic structure of blockchain and how transactions are verified through consensus.
2. Identify common blockchain attacks such as 51% attack, double spending, Sybil, and phishing.
3. Observe how these attacks can affect blockchain integrity using online simulators or explorers.
4. Analyze blockchain's security mechanisms like hashing, decentralization, and cryptographic signatures.
5. Record findings and suggest preventive measures to strengthen blockchain security.

* Softwares used

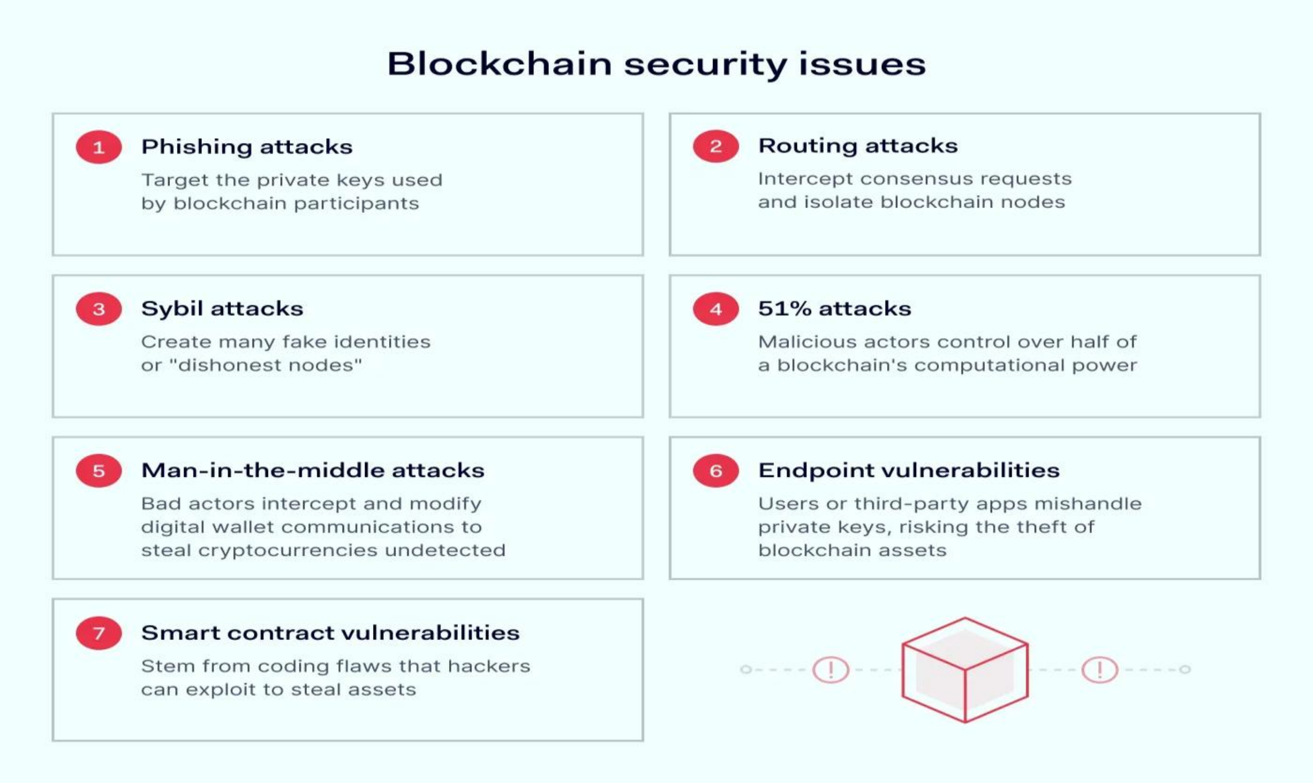
- Brave Web Browser
- Etherscan Explorer
- Metamask Wallet
- Text Editor(VS Code etc.)

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

* Testing Phase: Compilation of Code (error detection)

THEORY:

Blockchain is a distributed ledger technology that ensures data integrity, transparency, and immutability through cryptographic algorithms. Despite its robust design, blockchain systems can be vulnerable to certain attacks if not properly implemented. Common types of blockchain attacks include: 1. 51% Attack: Occurs when an entity controls more than half of the network's mining power, allowing it to manipulate transactions. 2. Double Spending: An attacker spends the same cryptocurrency twice by exploiting transaction confirmation delays. 3. Sybil Attack: Malicious actors create multiple fake identities to influence the network consensus. 4. Phishing Attack: Attackers trick users into revealing private keys or credentials through fake websites. 5. Routing Attack: Intercepting data during transmission between blockchain nodes to delay or modify transactions. The blockchain's main defense lies in its decentralized nature, cryptographic hash functions, and consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS).



Blockchain security issues

1 **Phishing attacks**
Target the private keys used by blockchain participants

2 **Routing attacks**
Intercept consensus requests and isolate blockchain nodes

3 **Sybil attacks**
Create many fake identities or "dishonest nodes"

4 **51% attacks**
Malicious actors control over half of a blockchain's computational power

5 **Man-in-the-middle attacks**
Bad actors intercept and modify digital wallet communications to steal cryptocurrencies undetected

6 **Endpoint vulnerabilities**
Users or third-party apps mishandle private keys, risking the theft of blockchain assets

7 **Smart contract vulnerabilities**
Stem from coding flaws that hackers can exploit to steal assets

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

* Implementation Phase: Final Output (no error)

- In this experiment, I explored how blockchain ensures data security and how different attacks can affect it.
- Using **Blockchain.com Explorer** and **Remix IDE**, I observed how transactions are digitally signed and verified in real time.
- I studied examples of **51% attacks**, **double spending**, and **phishing** using online blockchain simulators to understand their impact.
- Through the **Ganache test network**, I simulated simple attack scenarios and analyzed how consensus mechanisms like **Proof of Work (PoW)** prevent them.
- The output confirmed that blockchain provides strong protection through decentralization, hashing, and cryptographic validation.

* Observations

•Any change in one block affects all subsequent blocks, proving the immutability of data.
•Each transaction in a blockchain is verified and recorded in a distributed ledger, ensuring transparency.
•Real-world examples show blockchain's strong defense in systems like Bitcoin and supply chain tracking.

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.***