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: Wallets (Hot /Cold)

Learning Outcome:

Concepts learned (Mention 2/3 principles):

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

1. The fundamental concept of a cryptocurrency wallet as a tool that manages the cryptographic keys (private and public) used to interact with a blockchain network, not a storage for coins.
2. The complete architecture and critical difference between hot wallets (connected to the internet) and cold wallets (offline storage), focusing on their trade-offs between convenience and security.
3. The characteristics of different wallet types, including software wallets (web, mobile, desktop), hardware wallets, and paper wallets, and their respective use cases.

* New techniques learned:

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

1. Techniques for generating a seed phrase (mnemonic recovery phrase), which is a human-readable backup of the private keys that can restore access to funds on any compatible wallet.
2. Procedures for deriving a hierarchy of key pairs from a single seed using deterministic wallet structures (HD Wallets) as defined by BIP-32 and BIP-44 standards.
3. The process of how a wallet constructs and signs a transaction with a private key offline before broadcasting it to the network via a connected node.
4. Methods for securely storing seed phrases and private keys to prevent unauthorized access and permanent loss of funds.

* 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. Setting up and configuring a hot wallet (MetaMask) on a testnet to perform transactions and interact with smart contracts.
2. Simulating the process of transferring assets from a hot wallet to a cold wallet address to understand the flow of moving funds to cold storage.
3. Using a command-line interface (CLI) or a library like web3.js to generate a new Ethereum address and its corresponding private key programmatically.
4. Practicing the recovery of a wallet using a given seed phrase on a different wallet application to verify the importance of correct backup.

---

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

During the lab session, I used **MetaMask** as a browser-based hot wallet, explored the interface of a **Ledger Nano S** hardware wallet (cold wallet), and used **MyEtherWallet (MEW)** to practice offline transaction signing, demonstrating the interaction between different wallet types.

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

1. **Hot Wallets:** Used for frequent, daily transactions, such as holding a small amount of spending crypto, interacting with DeFi dApps, or paying for goods and services, due to their easy accessibility.
2. **Cold Wallets**: Used for long-term, secure storage of significant cryptocurrency holdings ("savings account"), protecting them from online hacking attempts, exchange collapses, and malware.
3. **Multi-Signature Wallets:** Used by organizations or groups requiring enhanced security, where transactions require approval from multiple private keys, preventing single points of failure.

---

* Case Studies/Examples:

1. **Exchange Wallets:** Centralized exchanges like Coinbase use a combination of hot wallets for customer withdrawals and deposits and cold wallets for the vast majority of asset storage to secure funds against breaches.
2. **Personal Asset Security:** An individual investor uses a hardware wallet (cold) to securely store Bitcoin purchased for long-term investment, while keeping a small amount of Ethereum in a mobile wallet (hot) for NFT minting.
3. **Institutional Custody:** Financial institutions offering crypto services partner with specialized custody solution providers (e.g., Fireblocks, Copper) that use advanced cold storage systems with insurance to safeguard billions in client assets.

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.