**Cyptocurrency & Blockchain**

**ASSIGNMENT**

* **Name: Muhammad Istafa Malik**
* **Roll: P19-0033**
* **Section: 7A**

**Question 1.**Explain the **key advantages** behind **Segregated**

**Witness**(**SegWit**) in Bitcoin transactions. How does **SegWit improve**

**the efficiency**of the Bitcoin network? How does **SegWit**contribute to the

overall **functionality and usability** of the Bitcoin ecosystem?

Answer: **Key Advantages:**

* Transaction Capacity
* Fee Reduction
* Security
* Compatibility

**SegWit improves the efficiency of the Bitcoin network** by separating transaction signatures (witness data) from transaction data, allowing more transactions to fit in each block. This reduces transaction fees, enhances scalability, and fixes transaction malleability issues, making Bitcoin transactions faster, cheaper, and more secure.

**Contribution to Functionality and Usability:**

It lowers transaction fees, making Bitcoin more affordable to use for both regular and micro transactions. It increases the transaction capacity of the network, reducing congestion and improving transaction processing times. While also providing Security by fixing transaction malleability issues, enhancing the security of Bitcoin transactions. SegWit is backward-compatible with older Bitcoin software, ensuring a smooth and safe network upgrade.

This way it contributes to its Functionality and Usability.

**Question 2.**Discuss the concept of **Hierarchically Deterministic**

**Wallets (HDWallets)** and their role in enhancing the **security and**

**manageability** of Bitcoin keys. How do the **HD Wallets** contribute to

the overall functionality and usability of the Bitcoin ecosystem?

Answer: **HD Wallets:**

Hierarchically Deterministic Wallets (HD Wallets) are a type of cryptocurrency wallet that generates an infinite number of public and private key pairs from a single seed or master key. This hierarchical structure simplifies key management, enhances security, and allows for easy backup and recovery. HD Wallets have become a standard in the crypto world, improving the usability and security of digital asset storage and transactions.

**Security and Manageability:** HD Wallets enhance the security and manageability of Bitcoin keys by simplifying key management through a single seed, reducing the risk of key loss, and making it easier to create and organize keys for various purposes, ultimately improving the overall security and usability of Bitcoin storage and transactions.

**Contribution to Functionality and Usability:**

HD Wallets contribute to the overall functionality and usability of the Bitcoin ecosystem by simplifying key management, enhancing privacy, enabling easy backup and recovery, and facilitating the creation of multiple addresses for different purposes, making it easier for users to engage with Bitcoin securely and efficiently.