BLOCKCHAIN TECHNOLOGY LAB

(20CP406P)

LAB ASSIGNMENT - 5

B.Tech in Computer Science and Engineering Dept.,

Pandit Deendayal Energy University,

Gandhinagar

Name: Mire Kishorkumar Patel

Roll No.: 19BCP080

Branch: Computer Engineering

Lab Assignment 5

Aim: Understanding and Exploring the Data Structures and Cryptographic Primitives for Blockchain

Introduction:

Cryptographic primitives:

Cryptographic primitives are used for building cryptographic protocols for a strong secured network. They are the low-level algorithms that are used to build algorithms. They are the basic building blocks of the cryptosystem. The programmers develop new cryptographic algorithms with the help of cryptographic primitives.

Importance Cryptographic primitives:

Cryptographic primitives are the basic building blocks for the development of security protocols. Hence, they are an integral part of the blockchain because of the following reasons:

- **Security:** To secure a transaction in the network or confidential information, strong cryptography is required. So cryptographic primitives are used to develop high-level algorithms.

- **Encryption and Decryption:** The Cryptographic primitives are used to develop encryption and decryption algorithms. Encryption algorithms encrypt the data and decryption algorithms decrypt the data as and when required.

- **Validation:** The validation of data is done with the help of digital signatures. These digital signatures are public key primitives which the receivers use to validate the message.

- **Specific:** Cryptographic primitives are very specific in nature. It means one cryptographic primitive can perform only one function. For example, the encryption algorithms developed using crypto primitives are only responsible for encrypting the text. It is not responsible for hashing or decryption.

Combining Cryptographic Primitives:

Cryptographic primitives are very specific in nature and new Cryptographic primitives cannot be developed even by experts because it is very prone to errors and requires complex mathematical analysis.

- Cryptographic designers combine the cryptographic primitives to form a strong security protocol.
- For example, It is always beneficial to have a security protocol that can detect flaws and remove the flaw as well.
- In the blockchain, SHA-256 a hashing algorithm is used in combination with a public key algorithm to encrypt the data.

Types of Cryptographic Primitives

Below are some of the common cryptographic primitives:

- **One way Hash Functions:** It is a mathematical function used to encrypt variable length data to fixed binary data. It is a one-way function. It means that once the input has been converted to a binary sequence, there is no scope for reverting back. It is also known as fingerprint or compression function. It is to be noted that a slight change in input can

also change the hash function. This is known as the avalanche effect. A popular hash function is SHA-256.

- **Symmetric Key cryptography:** This is also known as Symmetric Encryption. Suppose a message is encrypted using a key. The message is now converted to ciphertext which is readable but has no meaning. The same key is used to decrypt the message. A key is a variable used to encrypt or decrypt a text. It is basically used to 'lock' or 'unlock' data. In this cryptography, the key is shared between two users. The sharing of keys is a problem. However, this technique is faster than public-key cryptography. Examples are Advanced Encryption Standard (AES) and the Data Encryption Standard (DES)

- **Asymmetric key cryptography:** It is also known as public key cryptography. Since there is a problem with sharing keys in symmetric encryption, this method is used. Here one key is public and another key is private. The public key is used to encrypt or 'lock' data. The private key is only accessible to the receiver. The receiver uses a private key to 'unlock' the data. For example, Suppose Bob encrypts the data using the public key. The public key is available to everyone but this key works in one way. The receiver has the private key which works in one way and is used to decrypt the message. Examples of public key algorithms are DSA and RSA

- **Randomized Algorithms:** These algorithms produce random ciphertexts for encryption. The ciphertext is an encrypted text. It is very secure as random texts are produced for encryption. It is impossible for hackers to find various combinations of texts. It employs randomness as a logical part. It uses random inputs and gives correct output. For Example, Monte Carlo

- **Mix Network:** It is a routing algorithm that uses public key cryptography to encrypt data. The proxy servers take messages, encrypt them, and shuffle them so that communication cannot be traced. It basically breaks the flow of messages between the sender and the target.

- **Retrieval of Private information:** It is a protocol that allows the user to retrieve information from the database. Other users do not get to know about it. The user can anonymously retrieve data without taking permission.

- **Initialization Vector:** It is a number that is used along with a key for encryption. It is used to prevent the duplicate generation of ciphertext.