**Blockchain Technology Lab**

**Lab – 2**

**Aim : Explore a tool to learn the architecture of “Blockchain”.**

**Hash:**

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed 256-bit hash value from any input. It is part of the SHA-2 family, designed by the NSA and published by NIST.

Key Characteristics:

* Fixed-Length Output: Always generates a 256-bit hash.
* Deterministic: Same input yields the same hash.
* Fast Computation: Efficiently computes hash values.
* Pre-image Resistance: Infeasible to reverse-engineer the input from the hash.
* Collision Resistance: Infeasible to find two different inputs with the same hash.

A screenshot of a computer

Description automatically generated

**Block:**

**Basic Structure of Block:**

1. Block Number: Unique identifier for every block.
2. Nonce: To make a block valid, we have to add a number called nonce to the input to create a hash that starts with 4 zeros. There is a consensus in a blockchain network that governs what is considered to be a valid hash. In the case of this example, a hash starting with 4 zero will be considered correct.
3. Data: This field contains the data stored in the block
4. Hash: The hash field shows the SHA-256 hash value of the block, which includes the block number, nonce, and data.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Blockchain :**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Why are there a certain number of zero’s in the starting of the hash?**

The leading zeros in a blockchain hash signify the difficulty level set by the network to maintain a consistent block generation time. The requirement for a hash to have a certain number of leading zeros is a way to enforce the difficulty target. A hash is simply a large number, and having more leading zeros means the hash value is smaller.

For example, a target requiring three leading zeros (e.g., 000xxxxxxxxxxxxxxxxxxxxxx) is much harder to find than one with just one leading zero (e.g., 0xxxxxxxxxxxxxxxxxxxxxx).