**Lesson Plan – Hashing and SHA-256**

**Learning objectives -**

1. **Revise concepts of block creation from previous class**
2. **Discuss different available algorithms and explain about hashlib and SHA-256**

**Materials required -**

**repl.it login credentials**

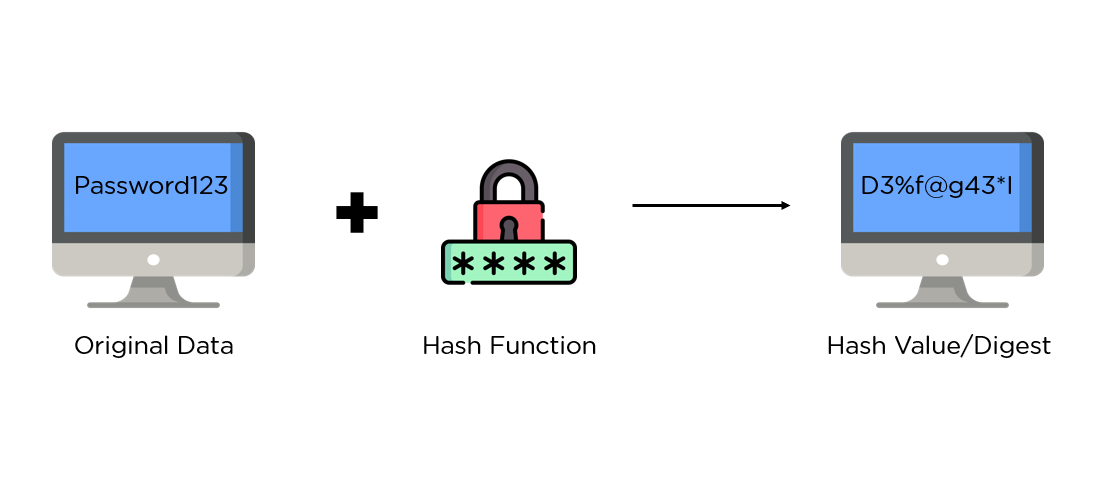
**What is hashing :**

Blockchain hashing is a fundamental aspect of how blockchain technology works. A hash function is a mathematical algorithm that takes input data of any size and produces a fixed-size output. In the context of blockchain, the input data is typically a block of transactions, and the output is a unique digital fingerprint, called a hash.

The process of blockchain hashing involves taking the data within a block, processing it through a hash function, and generating a hash that is unique to that specific block of data. This hash is then added to the header of the block, along with other information such as a timestamp and the hash of the previous block, to create a unique and immutable record of the transactions within the block.

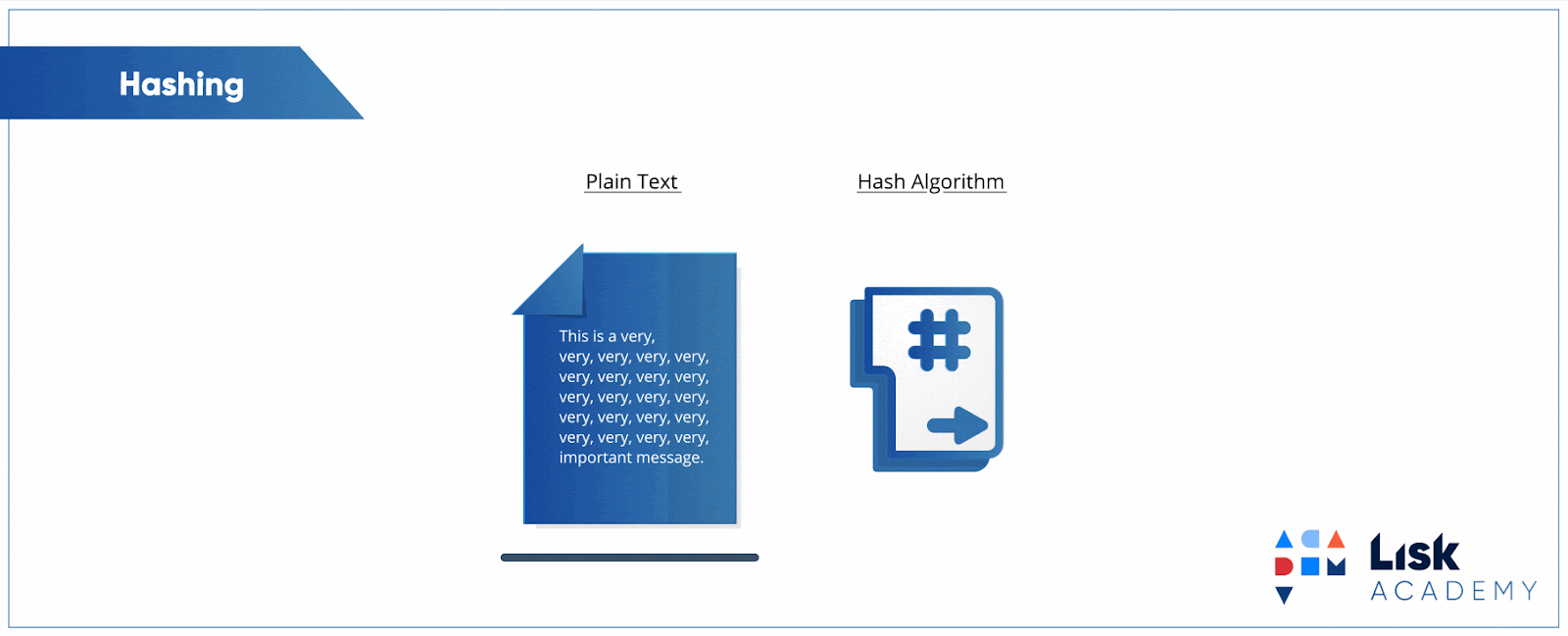
One of the key features of a hash function is that it is a one-way function, which means that it is computationally infeasible to derive the input data from the hash. This makes it extremely difficult to alter the data within a block without being detected, as any changes to the data would result in a different hash value.

The use of hashing in blockchain technology provides a secure and transparent way to record transactions that is resistant to tampering or alteration. As new blocks are added to the blockchain, each block's hash is included in the next block's header, creating a chain of blocks that are linked together by their hashes. This is why the technology is called blockchain.



**Key Terms:**

* **Deterministic:** The same input will always produce the same output, but that output cannot produce the original input.
* **Hash:** A calculated string of letters and numbers produced from a specific input.
* **Hash Function:** A function that takes in an input of a random size, performs hashing on the input, and generates a seemingly random output of a fixed size, also known as the hash



**Functions associated :**

* **encode() :** Converts the string into bytes to be acceptable by hash function.
* **hexdigest() :**Returns the encoded data in hexadecimal format.

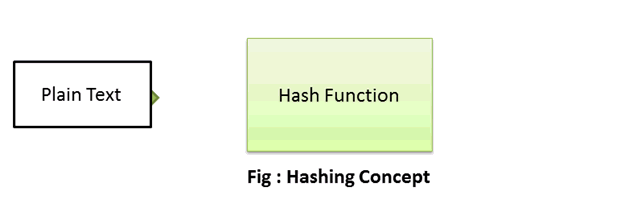
**SHA (Secure Hash Algorithm)**

The different SHA hash functions are explained below.

* **SHA256 :** This hash function belong to hash class SHA-2, the internal block size of it is 32 bits. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits.

The other algorithms in the SHA family are more or less similar to SHA 256. Some of them are as follows :

**SHA384 ,SHA224, SHA512, SHA1**

****

**All about SHA 256**

SHA-256 is a type of cryptographic hash function that is widely used in various digital security applications, including blockchain technology. The acronym "SHA" stands for Secure Hash Algorithm, and the number "256" refers to the fact that the output of the function is 256 bits in length.

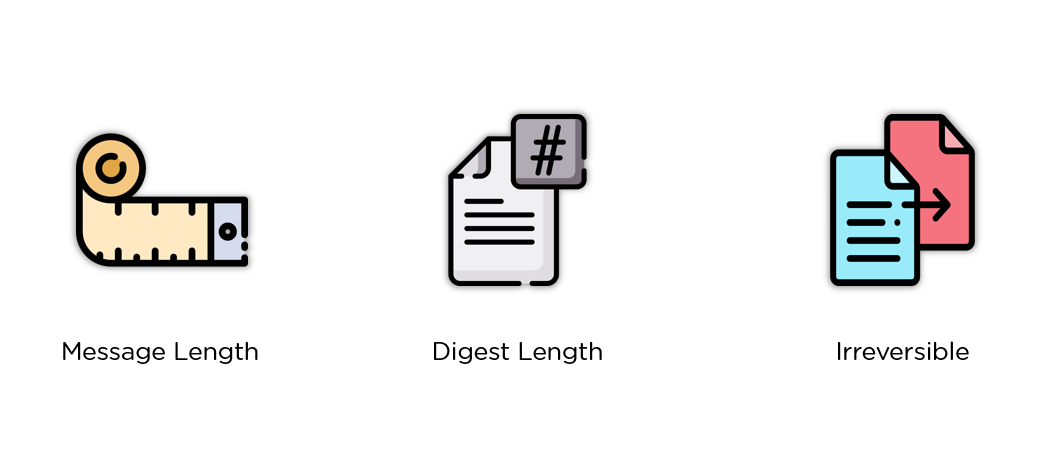
SHA-256 takes an input message of any length and produces a fixed-size output of 256 bits. The function is designed to be irreversible, meaning that it is practically impossible to derive the input message from its hash value. In other words, SHA-256 is a one-way function that produces a unique output for every input message.

The security of SHA-256 comes from the fact that it is resistant to collision attacks, which is when two different input messages produce the same hash value. The hash function is also designed to be resistant to pre-image attacks, which is when an attacker tries to find an input message that produces a specific hash value.

In blockchain technology, SHA-256 is used to generate the digital signature for each block of transactions in the blockchain. The hash value of the previous block is also included in the new block's header, creating a chain of blocks that are linked together by their hashes. This creates a secure and tamper-proof record of all transactions in the blockchain.

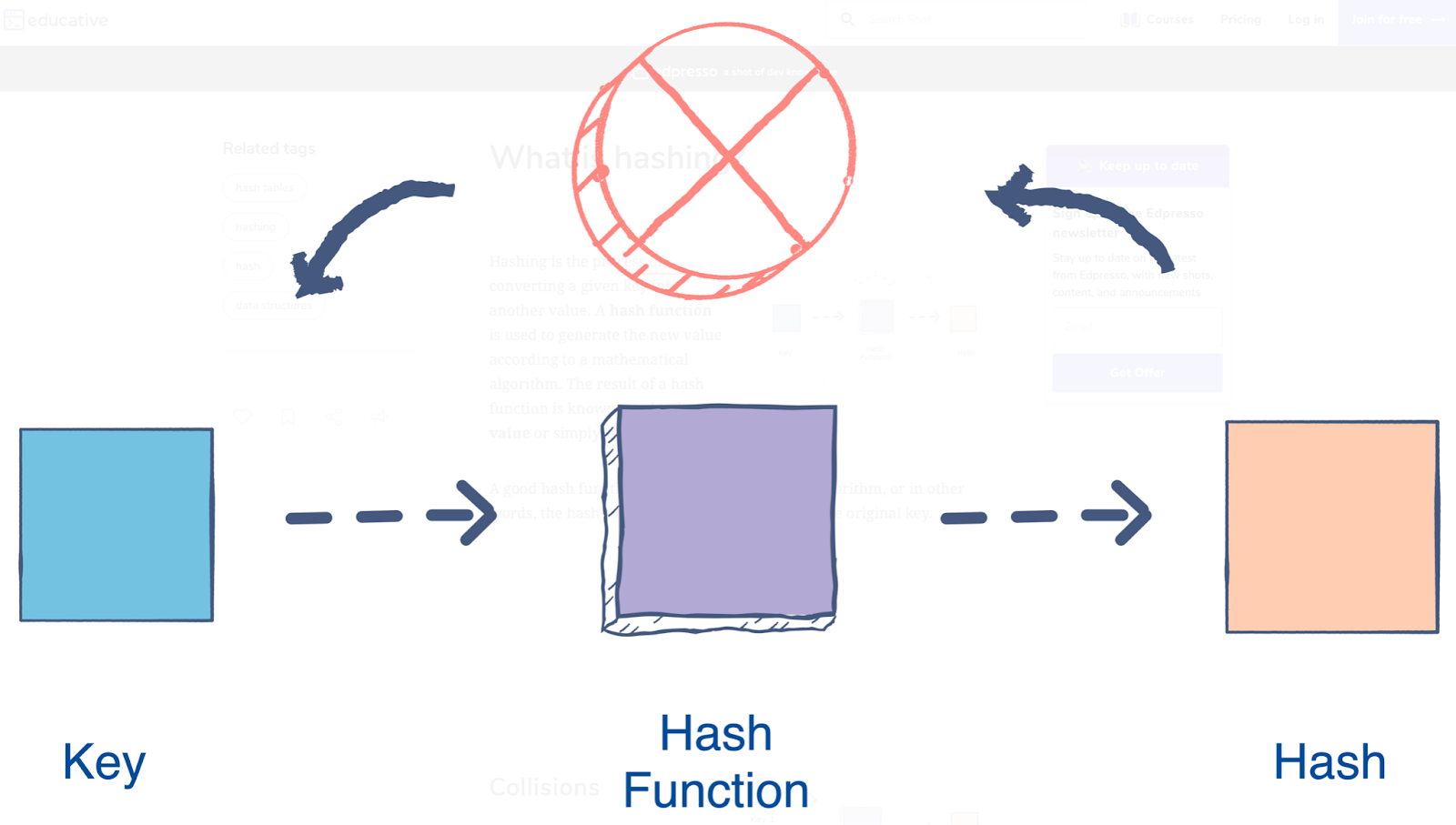
## **Characteristics of the SHA-256 Algorithm** :

Some of the standout features of the SHA algorithm are as follows:

* Message Length: The length of the cleartext should be less than 264 bits. The size needs to be in the comparison area to keep the digest as random as possible.
* Digest Length: The length of the hash digest should be 256 bits in SHA 256 algorithm, 512 bits in SHA-512, and so on. Bigger digests usually suggest significantly more calculations at the cost of speed and space.
* Irreversible: By design, all hash functions such as the SHA 256 are irreversible. You should neither get a plaintext when you have the digest beforehand nor should the digest provide its original value when you pass it through the hash function again.

**Why this one way rule?**

A good hash function uses a one-way hashing algorithm, or in other words, the hash cannot be converted back into the original key.

Imagine a hashing algorithm as a one way road. 

Here we can see the key is plain text on which we are applying a hash function to get hash

code. But we cannot reverse the method to get the original text.

[**https://andersbrownworth.com/blockchain/**](https://andersbrownworth.com/blockchain/)

**Introducing the lesson/project including the concepts (Time - 45 min)**

In the previous class you have learned about what is blockchain. How blockchain works. Here we are going to create our own block and will convert block information into hash code.

Link to Repl it Project :

[L3 -Hashing and SHA 256](https://docs.google.com/document/d/1-JFZD7vqwEyLGdRRjU8YGMbuKvgN6R6xuclIBOwfhls/edit?usp=sharing)

In the second activity we are going to implement something similar using the concepts of class, object and dictionary -

[L3 -Hashing and SHA 256](https://docs.google.com/document/d/1-JFZD7vqwEyLGdRRjU8YGMbuKvgN6R6xuclIBOwfhls/edit?usp=sharing)

Reference : <https://www.geeksforgeeks.org/sha-1-hash-in-java/>

**Homework –**

Write a program to encrypt and decrypt strings using python

https://www.geeksforgeeks.org/how-to-encrypt-and-decrypt-strings-in-python/