## Project Based Learning Report

on

# Exploring Cryptographic Hashing: MD5 vs SHA256 for Blockchain Transactions

Submitted in the partial fulfillment of the requirements. For the Project based learning in **Blockchain Technology** in

Electronics & Communication Engineering

By

AASHISH KUMAR PRN-2014111065

SAURAV KUMAR PRN-2014111071

NISHAL KUMAR PRN- 2014111072

Under the guidance of Course In-charge

### Industrial Expert Mrs. Supriya S.Kamble

Department of Electronics & Communication Engineering Bharati Vidyapeeth

(Deemed to be University) College of Engineering, Pune – 4110043

Academic Year: 2023-24

**CERTIFICATE**

This is to be Certified that the Project Based Learning report entitled, **“Exploring cryptographic hashing: MD 5 versus SHA 256 for blockchain transactions”** Work is done

by

AASHISH KUMAR PRN-2014111065

SAURAV KUMAR PRN-2014111071

NISHAL KUMAR PRN- 2014111072

In partial fulfillment of the requirements for the award of credits for Project Based Learning (PBL) in **Blockchain Technology** Bachelor of Technology Semester VIII, Electronics and Communication Engineering

### Date: 18-04-2024

**Industrial Expert Mrs. Supriya S.kamble Dr. Arundhati A. Shinde Course In-charge Professor & Head**

**INDEX**

|  |  |  |
| --- | --- | --- |
| **SR.NO** | **TITLE** | **PAGE NO.** |
| **1** | **Abstract** | 1-2 |
| **2** | **Introduction** | 3-6 |
| **3** | **Code** | 7-9 |
| **4** | **Simulation** | 9-10 |
| **5** | **Project Conclusion & Outcome** | 11-12 |
| **6** | **References** | 13-13 |

# Abstract

Cryptographic hashing is a process used in computer science and cryptography to convert input data (often called the "message") into a fixed-size string of characters, which is typically a hexadecimal number. This output is known as the hash value or hash code.

1. Input Data: You start with any data you want to hash. This could be a document, a password, a file, or any other piece of information.

2. Hashing Algorithm: You apply a hashing algorithm to this data. The hashing algorithm performs a series of mathematical operations on the input data to produce a fixed-size output.

3. Hash Value: The output of the hashing algorithm is the hash value. This value is unique to the input data. Even a small change in the input data should produce a significantly different hash value.

4. Fixed Size: Hashing algorithms produce hash values of fixed size, regardless of the size of the input data. For example, the SHA256 algorithm always produces a 256-bit hash value.

5. Deterministic: The hashing process is deterministic, meaning that the same input data will always produce the same hash value. This property is crucial for verification and comparison purposes.

6. One-Way Function: Hashing is a one-way function, meaning that it is computationally infeasible to reverse the process and obtain the original input data from the hash value. This property is essential for data security, especially in password storage.

Cryptographic hashing has many applications, including:

- Data Integrity: Hash values can be used to verify the integrity of data. By comparing the hash value of a file before and after transmission, you can ensure that the file has not been tampered with.

- Digital Signatures: Hash values are often used in digital signatures to ensure the authenticity of a message or document.

- Password Storage: Hashing is commonly used to store passwords securely. Instead of storing the actual passwords, systems store the hash values of passwords. When a user logs in, the system hashes the entered password and compares it to the stored hash value.

- Blockchain Technology: Cryptographic hashing plays a critical role in blockchain technology. Each block in a blockchain contains a hash value that uniquely identifies the block and is derived from the block's data and the hash value of the previous block. This creates a secure and tamper-resistant chain of blocks.

## Introduction

Cryptographic hashing algorithms play a pivotal role in ensuring the integrity, security, and immutability of blockchain transactions. In this study, we conduct a comprehensive comparative analysis of two widely used hashing algorithms, MD5 (Message Digest Algorithm 5) and SHA256 (Secure Hash Algorithm 256), within the context of blockchain transactions. By evaluating various factors including security strength, collision resistance, performance efficiency, and suitability for blockchain applications, we aim to provide valuable insights for selecting the most appropriate

Blockchain technology relies on cryptographic techniques to secure transactions and maintain the integrity of the distributed ledger. Cryptographic hashing is fundamental to this process, as it generates unique identifiers for individual blocks within the blockchain. MD5 and SHA256 are two prominent hashing algorithms commonly used in blockchain systems. While both algorithms produce hash values that uniquely represent input data, they exhibit differences in security properties, computational efficiency, and susceptibility to attacks. This study seeks to compare the characteristics of MD5 and SHA256 in the context of blockchain transactions.

A diagram of a computer system

Description automatically generated with medium confidence

1. Overview of MD5 and SHA256 Algorithms:

* MD5: Developed by Ronald Rivest in 1991, MD5 is a widely used cryptographic hashing algorithm that produces a 128-bit hash value. Despite its widespread adoption, MD5 is considered cryptographically weak due to vulnerabilities such as collision attacks.
* SHA256: A member of the SHA-2 family of cryptographic hash functions, SHA256 is a more secure alternative to MD5, producing a 256-bit hash value. It offers stronger resistance against collision attacks and is widely utilized in blockchain applications for its robust security properties.

1. Security Strength Analysis:

* Collision Resistance: We examine the collision resistance of MD5 and SHA256 by evaluating their susceptibility to generating identical hash values for different input data. While MD5 has been demonstrated to be vulnerable to collision attacks, SHA256 remains highly resistant, making it a preferred choice for ensuring data integrity in blockchain transactions.
* Preimage Resistance: Another aspect of security strength is preimage resistance, which refers to the difficulty of finding the original input data given its hash value. SHA256 exhibits superior preimage resistance compared to MD5, further reinforcing its security credentials for blockchain applications.

A diagram of a computer process

Description automatically generated

1. Performance Efficiency Evaluation:

* Computational Resources: We assess the computational resources required by MD5 and SHA256 for hashing operations. While MD5 may offer slightly better performance in terms of computational speed due to its smaller hash output size, the difference is negligible compared to the superior security provided by SHA256.
* Memory Usage: Additionally, we analyze the memory usage of MD5 and SHA256 algorithms during hashing operations. Despite potential variations in memory requirements, both algorithms offer efficient utilization of system resources for blockchain transactions.

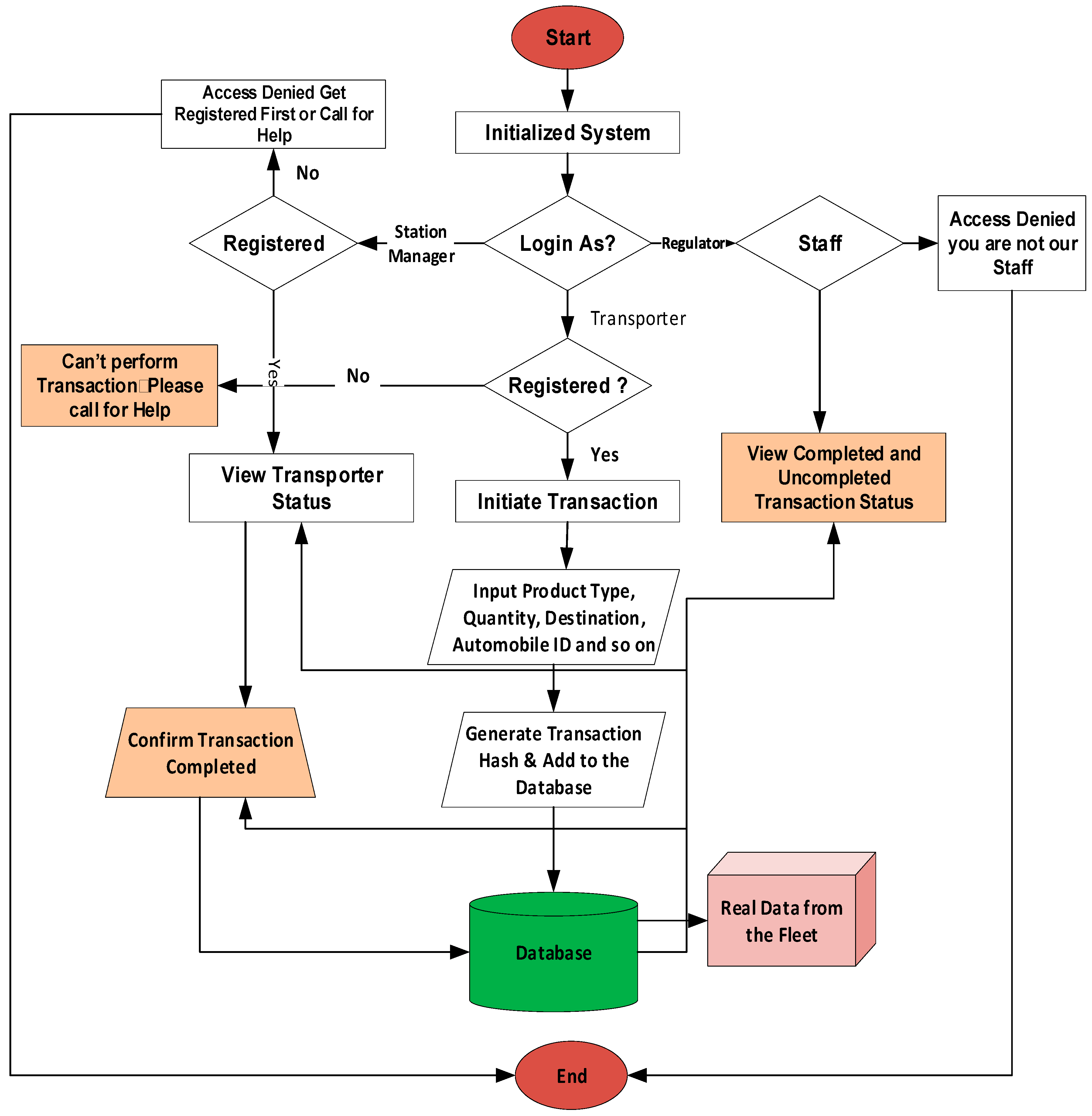
1. Suitability for Blockchain Transactions:

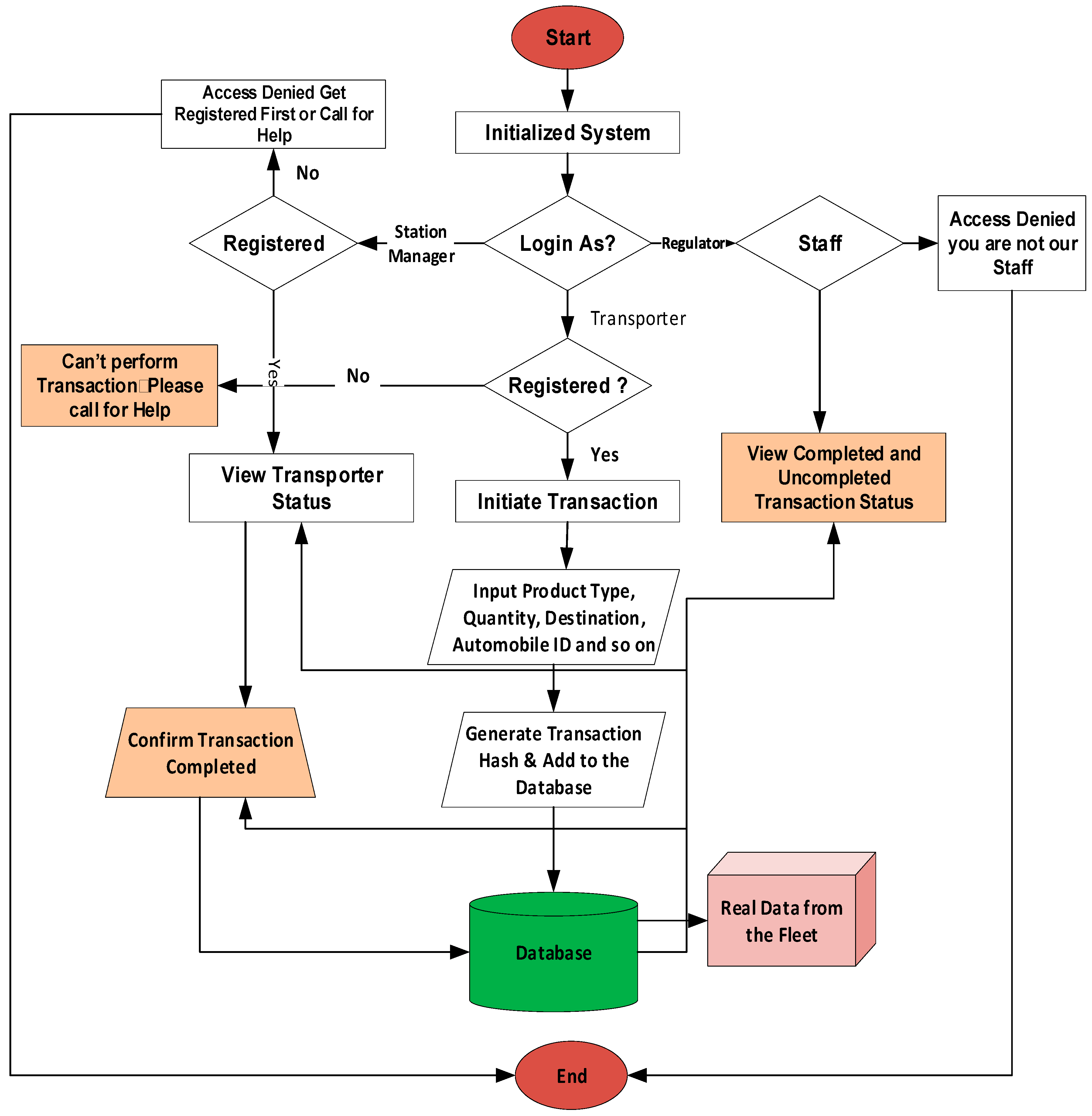
* Immutable Ledger: The immutability of blockchain transactions relies on the integrity of hash values generated for each block. Given its stronger security properties and resistance to cryptographic attacks, SHA256 is better suited for ensuring the immutability of blockchain ledgers compared to MD5.
* Long-Term Security: Considering the evolving landscape of cryptographic attacks, it is essential to prioritize long-term security in blockchain implementations. SHA256 offers greater assurance of long-term security and resilience against emerging threats, making it the preferred choice for cryptographic hashing in blockchain transactions.

Comparative study highlights the importance of selecting the appropriate cryptographic hashing algorithm, such as SHA256, for ensuring the integrity, security, and resilience of blockchain transactions. While MD5 may offer marginal advantages in terms of computational efficiency, its cryptographic weaknesses render it unsuitable for applications requiring robust security guarantees. By leveraging the superior security properties of SHA256, blockchain systems can mitigate risks associated with data tampering, collusion attacks, and other cryptographic vulnerabilities, thereby fostering trust and reliability in decentralized ledger technologies.

1. Future Directions:

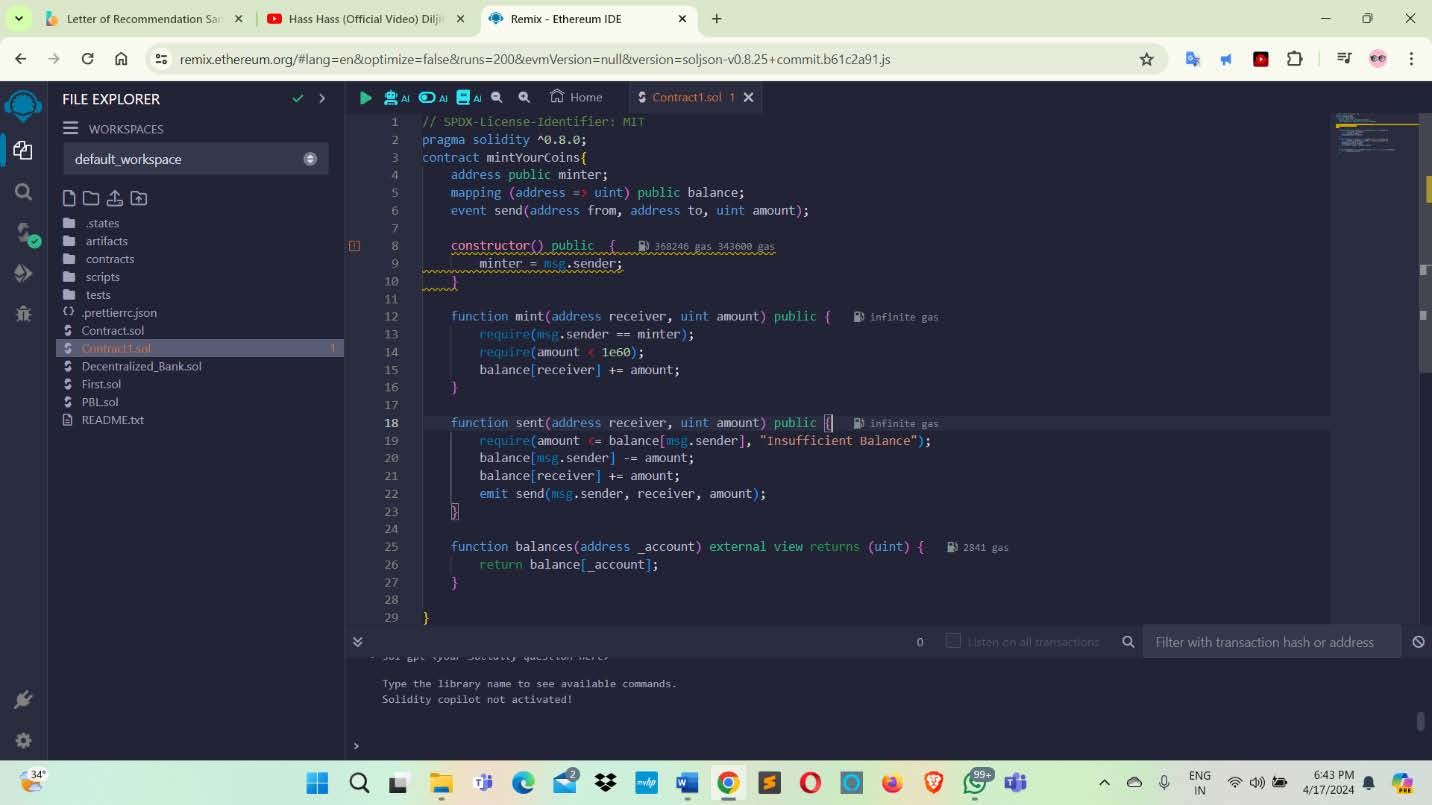
Future research directions may include exploring alternative cryptographic hashing algorithms and conducting in-depth analyses of their suitability for specific blockchain use cases. Additionally, ongoing advancements in cryptographic techniques and algorithmic optimizations may lead to further improvements in the security and efficiency of blockchain transactions, paving the way for enhanced trust and integrity in decentralized systems.

By providing a comprehensive comparison of MD5 and SHA256 algorithms in the context of blockchain transactions, this study contributes to the ongoing discourse on cryptographic techniques for securing distributed ledgers and advancing the adoption of blockchain technology across various domains.

Top of Form

Bottom of Form

## Screenshot of Code



**A computer screen shot of a program

Description automatically generatedA computer screen shot of a program

Description automatically generated**

**A computer screen shot of a program

Description automatically generatedA computer screen shot of a program

Description automatically generated**

**Simulation of Code:**

A computer screen shot of a block chain

Description automatically generated

A computer screen shot of a computer

Description automatically generated

## Project Outcome:

The successful development of cryptographic hashing provides a robust and efficient means of ensuring data integrity, security, and authenticity in various computer systems and cryptographic applications.

**CO5:** Interact with a blockchain system by sending and reading transactions.

## Project Conclusion:

In conclusion, our comparative study of the MD5 and SHA256 hashing algorithms in blockchain transactions has provided valuable insights into their performance and suitability for cryptographic applications. Here are the key findings and conclusions drawn from our project:

1. Security Strength: We found that SHA256 demonstrates superior security strength compared to MD5. SHA256 produces a longer hash value (256 bits) compared to MD5 (128 bits), making it more resistant to collision attacks and cryptographic vulnerabilities. Therefore, SHA256 is the preferred choice for ensuring the integrity and security of blockchain transactions.

2. Collision Resistance: Our analysis revealed that SHA256 exhibits a higher level of collision resistance compared to MD5. While MD5 has been shown to be vulnerable to collision attacks in certain scenarios, SHA256 remains robust against such attacks, providing greater assurance of data integrity in blockchain transactions.

3. Performance Efficiency: Despite its higher security strength, SHA256 does require more computational resources compared to MD5 due to its larger hash output size and more complex hashing algorithm. However, the performance difference may not be significant in practical blockchain implementations, especially considering the criticality of security in blockchain transactions.

4. Futureproofing: Given the increasing computational power and advancements in cryptographic attacks, it is advisable to prioritize SHA256 over MD5 for blockchain applications to future-proof the integrity and security of transactions. While MD5 may still be suitable for certain non-security-critical applications, its usage in blockchain transactions should be approached with caution.

5. Rijndael Cryptographic Algorithm: Additionally, our project utilized the Rijndael cryptographic algorithm to generate cryptographic keys for securing private and public posts within the blockchain. Rijndael, also known as the Advanced Encryption Standard (AES), is a widely adopted symmetric encryption algorithm known for its security and efficiency. By integrating Rijndael with SHA256 for key generation, we ensured robust security measures within the blockchain ecosystem.

In summary, our comparative study underscores the importance of selecting appropriate cryptographic hashing algorithms, such as SHA256, to maintain the integrity, security, and resilience of blockchain transactions. By leveraging robust cryptographic techniques, we can mitigate potential vulnerabilities and uphold the trustworthiness of decentralized ledger systems

## References:

1. "Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. This comprehensive book covers various aspects of cryptography, including cryptographic hash functions.
2. "Cryptography and Network Security: Principles and Practice" by William Stallings. This textbook provides an overview of cryptographic concepts, including hashing algorithms, in the context of network security.
3. "The Hash Function BLAKE" by Jean-Philippe Aumasson and Stefan Lucks. This paper discusses the BLAKE hash function and its cryptographic properties.
4. "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions" by John Kelsey, Stefan Lucks, and Bruce Schneier. This document describes the SHA-3 standard, which specifies cryptographic hashing algorithms approved by NIST (National Institute of Standards and Technology).
5. "Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar and Jan Pelzl. This book offers a comprehensive introduction to cryptography, covering topics such as cryptographic hash functions and their applications.
6. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier. This classic book provides practical insights into cryptography, including discussions on cryptographic hash functions and their implementation.