

Research Article

Enhancing VANET Security using Blockchain and SHA3-256 in Python

Liqaa Saadi Mezher ^{1,2,*} , Muna Hadi Saleh ¹ 

¹ Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, 10071, Iraq

² Department of Computer Engineering, College of Engineering, Mustansiriyah University, Baghdad, 10052, Iraq

*Corresponding Author: Liqaa Saadi Mezher, E-mail: leqaa.saady2302p@coeng.uobaghdad.edu.iq

Article Info	Abstract
Article History	Vehicular Ad Hoc Networks (VANETs) are crucial for modern intelligent transportation systems, enabling real-time communication between vehicles (V2V) and infrastructure (V2I) for applications such as traffic management, accident prevention, and autonomous driving. However, the decentralized and wireless nature of VANETs makes them vulnerable to various cyber threats, including data tampering, eavesdropping, and unauthorized access. Robust security is crucial for protecting sensitive data, maintaining trust, and ensuring the safety of passengers and pedestrians. While existing cryptographic solutions have been proposed, many fail to address the scalability and robustness required for dynamic and resource-constrained VANET environments. This research introduces a novel security framework integrating blockchain technology with SHA3-256 cryptographic hashing. Blockchain provides decentralized trust management, ensuring tamper-proof and verifiable communication, while SHA3-256 enhances data integrity and protects against malicious attacks. A Python-based implementation of this framework demonstrates its scalability and computational efficiency. By securing both V2V and V2I communication, the framework mitigates vulnerabilities, reduces the risk of system malfunctions, and lowers accident rates. This approach establishes a secure and reliable foundation for future intelligent transportation systems, promoting smarter and safer road networks.
Received Nov 12, 2025	
Revised Jan 23, 2025	
Accepted Feb 20, 2025	
Keywords	
VANET	
SHA3	
Blockchain Decentration	
Python	
VANET Security	
 Copyright: © 2025 Liqaa Saadi Mezher, and Muna Hadi Saleh. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license.	

1. Introduction

VANETs have become an active research area due to the growing importance of intelligent transportation systems in modern society [1]. These networks enable communication between vehicles and infrastructure, facilitating traffic management, accident prevention, and autonomous driving, enhancing safety and efficiency. However, security remains one of the main challenges preventing the widespread deployment of VANETs. The decentralized nature of VANETs makes them vulnerable to cyber threats; therefore, ensuring secure communication and data integrity is crucial for their success. Blockchain has shown promise as a solution for providing secure timestamping and enhancing trust in VANETs [2]. A lightweight blockchain model combined with SHA3-256 encryption is proposed to address these security concerns.

Despite the ongoing research in VANET security, existing solutions often fail to address critical issues such as data authenticity, integrity, non-repudiation, and confidentiality [3]. Current security models struggle with the dynamic and distributed nature of VANETs, where information is frequently exchanged among vehicles in an ever-changing topology [4, 5]. Additionally, traditional security architectures for VANETs may not be scalable, efficient, or robust enough to handle the demands of real-time communication in resource-constrained environments. This knowledge gap presents an opportunity to explore alternative security frameworks that are both scalable and practical for deployment in VANETs.

The research question is how to design a secure and efficient framework for VANETs that addresses vulnerabilities such as data tampering, unauthorized access, and a lack of trust management while being scalable and computationally efficient for real-time applications. This study proposes a blockchain-based security framework integrated with the SHA3-256 cryptographic hashing algorithm. The goal is to enhance data integrity, provide decentralized trust management, and improve the overall security of VANET communications.

This study aims to design and implement a security system that leverages blockchain technology and SHA3-256 hashing to create a secure and scalable VANET framework. This framework aims to mitigate the risks associated with malicious attacks, such as spoofing and Sybil attacks, while ensuring data confidentiality and authenticity. A Python-based implementation demonstrates the practical feasibility of the proposed solution, showcasing its computational efficiency, scalability, and resilience to real-world attacks.

This research is significant as it contributes to advancing VANET security by integrating blockchain and cryptographic techniques to address key gaps in existing literature. The proposed solution offers a scalable, reliable, and efficient approach to securing VANETs, providing a solid foundation for the future deployment of intelligent transportation systems. By enhancing the security and trust within these networks, this research could pave the way for the broader adoption of VANETs and their integration into smart cities, improving both safety and efficiency on the roads.

2. Literature Review

2.1. Blockchain for VANET Security and Privacy

Ensuring privacy and security in VANET is crucial, as adversaries may exploit vulnerabilities to launch cyberattacks against the public or turn beneficial VANET applications into disasters. Many security and privacy schemes have been developed [6, 7]. However, these schemes still borrow flawed security properties. Commercial deployment of VANET applications remains rare. As a potential solution, blockchain is a scalable and tamper-evident data structure that prevents double-spending attacks and other security and privacy risks associated with fraudulent transactions [8].

Although blockchain has shown significant promise, it has been utilized to securely and transparently record transactions, thereby verifying financial incentives. This design prohibits interoperability and limits the potential exploitations of the technology. Blockchain can be further exploited to enhance VANET security and privacy in cases where PKI is powerless. A public or private blockchain can provide many flexible and trustworthy security properties [9], as shown in Table 1. We are motivated by the vision of removing the nodes' reliance on many vulnerable third-party certification centers and the anonymous nature of Bitcoin. In this paper, we design a security and privacy enhancement system for VANET that is implemented using blockchain technology. Our forward-thinking approach to VANET security and privacy sets the stage for exploring a myriad of other blockchain applications without limitations and presents significant real-world benefits.

Table 1. A summary of previous studies

No.	Researcher Name	Year	Key Contribution	Methodology	Limitations
1	Kotey, et al. [6]	2023	The research's contributions include a systematic review, identification of open issues, a focus that extends beyond cryptocurrencies, and insights from real-world implementation.	The paper employs a systematic approach to reviewing the current state of heterogeneous blockchain interoperability.	Lack of real-world implementations, focus on cryptocurrency applications, semantic incompatibility, complex frameworks, and absence of Blockchain standards.
2	Dayu J., et al. [7]	2023	The study's key contributions lie in its innovative privacy-preserving methods, federated learning for block classification, a robust evaluation framework for hot blocks, and thorough experimental validation, all of which aim to enhance blockchain storage solutions in IoT environments.	Employs a combination of federated learning techniques, a sharded blockchain model, comprehensive feature evaluation, controlled experimental methods, and synthetic data.	The proposed Blockchain storage method's limitations include challenges related to query efficiency, data classification accuracy, storage requirements, privacy concerns, experimental validity, and scalability.
3	Abdual-Jabber, et al.[8]	2023	Contributions of the research understanding cloud security challenges, techniques for privacy and data integrity, comparison of existing methods, emphasis on cryptographic methods and blockchain	This paper discusses various methods employed to ensure data integrity and privacy in cloud computing environments (Cryptographic techniques).	It highlights several limitations that warrant further investigation and development, particularly in the areas of pre-quantum solutions and Vulnerability to man-in-the-middle attacks.
4	Adeniyi, et al. [9]	2024	The research presents several significant contributions to the field of electronic voting, including the introduction of Biometric Cryptography in systems, the Enhancement of Voter Anonymity, and the Utilization of Blockchain Technology.	Employs several innovative methods (fingerprint scanning, integration with cryptocurrency wallets, and DAPP voting interaction).	The paper has limitations, including scalability issues, dependence on biometric data, technical complexity, and a lack of a verifiable paper trail.

2.2. Vehicular Ad-Hoc Networks (VANETs)

VANETs are a specific adaptation of Mobile Ad-Hoc Networks (MANETs) where the nodes are vehicles [10, 11]. These vehicles are mobile, and the interference from buildings and other obstacles is intense. VANET enables vehicles to establish ad-hoc communication among themselves, sharing safety-related information, and its environment features sensors that can shape the physical nature of a MANET [12]. Moreover, VANET transmits traffic information and safety messages concerning vehicles that are currently within the range of communication, thereby enhancing road safety and traffic efficiency. The prime concern for the multilevel structure of VANET is security. Data transmission through the network enhances vehicular safety, checks for traffic violations, and supports the communication network for the infrastructure of VANET, among other services provided by the network. The quality of service utilized is a significant and deeply rooted issue [13, 14].

It is essential to observe the cyber world for any form of security-related threats with a keen eye [15]. Security challenges are one of the most significant issues facing the deployment of VANETs [16]. To increase trust in communicating vehicles, the use of security techniques is essential. These issues can be addressed using the suggested ideas, and we deem security as a feather that needs to be kept radiant and bright without sully in respect, rather than the opposite, with its consequential catastrophe. Security still raises concerns or becomes even more daunting, requiring a distributed and tamper-proof security method using blockchain in the VANET network.

2.3. Overview and Architecture

VANET is a type of MANET that facilitates communications between vehicles and roadside apparatus nearby [10]. It enables vehicular communication with a roadside network infrastructure to monitor traffic conditions and maintain road safety. Security is necessary for VANETs, given their key applications in traffic safety and management. We propose a blockchain-based security scheme for VANETs. A cryptographic data structure known as a blockchain is created using hashing and then incorporated into VANET applications [17]. Roadside infrastructure is responsible for blockchain-related initial setup work and continuous maintenance. When a new block is formed, fraudulent information can be efficiently detected. VANETs are considered heterogeneous wireless ad hoc networks because they involve mainframes, sensors, and the Internet [18]. Recently, the number of vehicular security applications has increased significantly. Most of the VANET security schemes are designed to ensure the integrity and security of traffic information and the privacy of communicating vehicles, provide the basic security required by VANET communication, and achieve strong security models defined by specific VANET security applications, as shown in Figure 1 [19]. To process such crucial information, the required security model must be secure, as that information is essential.

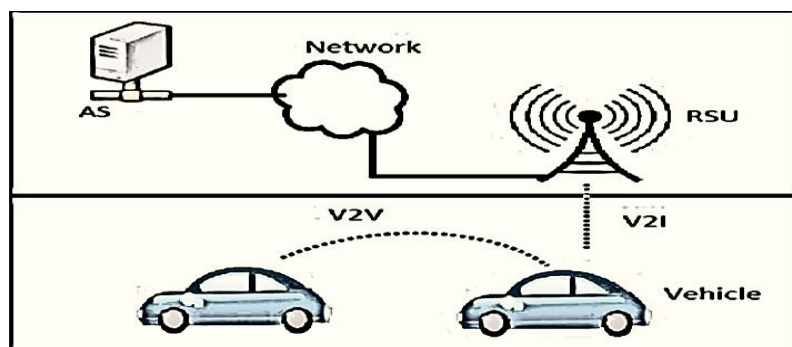


Figure 1. Architecture of VANET

2.4. Challenges and Security Concerns

The security difficulties and concerns of VANET are categorically separated into two primary domains: vehicle monitoring systems or the in-cloud domain and vehicle privacy [20]. This division is mainly due to the service provider's intervention or data requests. Public reliance on network data is necessary to ensure that the vehicle monitoring system relies on accurate and reliable remote sensing. However, the vehicle monitoring system's reliance on this data is deprecated due to bounded latency and security concerns. A straightforward attack on connectivity would result in incomplete or lost data, leading to a significant crash in the crash detection process. The vehicular cloud network cannot cooperate directly since vehicles are location-dependent [21].

Simply put, vehicle-to-vehicle data transmission has the highest probability of data relay. As a result, vehicles rely solely on data relays to collect truthful and reliable data. A service provider can participate in the traffic data game in the in-cloud vehicular network. By participating in an attack on vehicle data relay, attacks, and misinformation can be caused. This can result in gains for either a malicious party or a user of the service provider [22]. Certain vehicles or those with high subscription levels would thus have secured advantages in both attack and information reliability concerns. The cost constraint of deploying a security system ensuring message source authenticity has thus been investigated.

3. Methodology

3.1. Blockchain Technology

A blockchain is a distributed ledger comprising a blockchain [23, 24]. These blocks store transactions and represent the current state of a ledger of these transactions. Any node of the blockchain network can generate blocks for the blockchain ledger. The node can be a gateway, sensor, or authorized network device. Blockchain architecture is designed to resist modification and typically consists of an increasing list of records, called blocks, which are connected using cryptographic hashes [25]. The transaction data, the antecedent block's cryptographic hash, and a timestamp are incorporated into each block, as shown in Figure 2. Decentralized ledger technology is secured because data, once entered, is challenging to change, and only incremental changes can be made based on the consensus of the network participants [26].

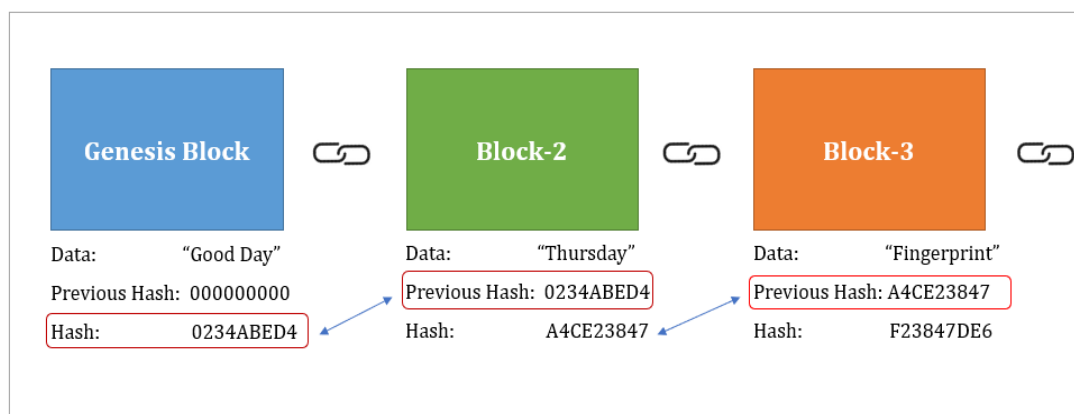


Figure 2. Architecture of blockchain

The data in a blockchain is timestamped so other nodes can verify the integrity and the chronological order of all transactions. The integrity is verified by the consensus mechanism of the five leading nodes, where a 51% agreement achieves consensus [27, 28]. Blockchain technology is most well-known for its implementation and support of cryptocurrencies, where blockchain technology plays a crucial role. Provides a cryptographically secure, publicly accessible register for balances of cryptocurrencies. II. It makes it straightforward for participants to view, verify, and prove ownership of valuable assets. It also provides a fully decentralized way for participating parties to agree with a distributed consensus model. Furthermore, access restriction functionality can be provided using a combination of cryptographic algorithms, as shown in Figure 3, which illustrates the transaction flow in the blockchain network [29].

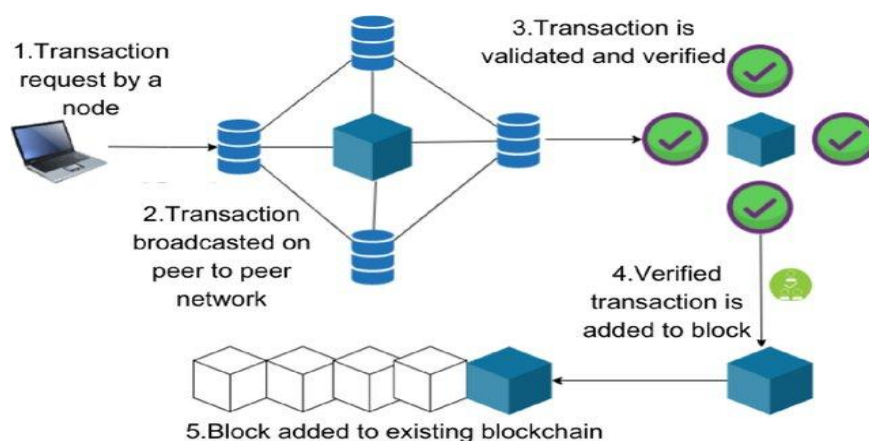


Figure 3. Flowchart of transactions in blockchain network

3.1.1. Fundamentals and Components

This research introduces VANETs, their associated security challenges, and the application of blockchain technology. Additionally, it explores several theoretical concepts underlying quantum computing and other advanced mathematical technologies that can compromise encrypted communication protocols, including the robust Quantum Secure Communications protocols specifically designed for blockchain environments [30, 31]. Subsequently, we summarize the necessity of employing advanced computationally secure cryptographic principles, which remain unchallenged, to ensure that blockchain technology, resistant

to quantum advantages, maintains the security of VANET infrastructure. In contrast, quantum cryptography and similar cryptographic solutions face significant limitations.

Security and privacy are critical parameters in ensuring VANET services, such as comfortable travel, safe driving, journey assistance, and message trust, through the Anonymous Distance Protocol, which promotes drivers' interest in obtaining these services [32]. The privacy of a person's identity is a crucial issue to address in securing VANETs using V2V and V2I communications. Vehicle-to-vehicle communication requires authentication and confidentiality to ensure security, data integrity, tamper resistance, detection of privacy offenses, pseudonymity, and an alternative certification unit [33]. Vehicle-to-infrastructure needs certification to overcome obstacles and reduce the risk of forgery without disclosing the traveler's identity. The market demand for services and control of various breaches is another widespread need. The blockchain can handle the concept of data asymmetry, control, and enhancement of fraudulent messages [34]. The encryption protocol has also been demonstrated to be a powerful tool for maintaining secure cryptographic communications, which is particularly suitable for recent blockchain technology [35]. Moreover, it is theoretically immeasurable to break with a quantum computer model; it is combinatorial.

3.2. SHA3-256 Cryptographic Hash Function

This cryptographic hash function allows high-speed data processing and is mainly used in large enterprise models [36]. Although the input size it handles is relatively large, the output size is also flexible. Thus, it is possible to create tiny memory cells for VANET and have all access, leaving a response, posting, and creating new topics from the surface layer [37]. The input is encoded and divided into block-sized pieces, which are then expanded. Initial values of XOR adjustments from the outer region of the Table XOR each other many times over the fixed rounds. If necessary, values suitable for the dynamic length of the output data will be attained by reflecting on the Table and the purpose of the placement of the construction. Due to the criteria and requirements outlined in tables such as advantages, disadvantages, and examples, we have preferred its usage in our paper.

3.2.1. Overview and Properties

Let us take a moment to introduce blockchain and its fundamental properties. A distributed, tamper-evident and tamper-resistant digital ledger is known as a blockchain [38]. It records transactions in a verifiable way. Each block in the blockchain is encrypted with a cryptographic hash of the preceding block. The hash changes and breaks the chain if a block is maliciously altered. Thus, the whole ledger becomes tamper-evident, meaning a simple change would be noticed immediately and proven easily. The exact property, backed by cryptographic hash functions used in blockchain, also makes it tamper-resistant, as generating a maliciously altered version of a whole tamper-resistant blockchain would be computationally infeasible [39]. However, manipulation with invalid entries in an existing block retained by the chain can occur.

Blockchain's security relies on riddles and elliptic curve cryptography. This also implies that simple chaining can be very costly in terms of time, operational overhead, and longevity of the scheme used in the network. Since the encrypted chain and embedded data form a digital ledger in a known structure, accidental data retention is also a concern. Bloat attacks can be prevented by integrating off-chain data storage, for example, through the use of a decentralized file system, which allows for referencing the data stored rather than the data itself [40].

SHA3-256, a cryptographic hash function, ensures data integrity in secure communications. The role and significance of SHA3-256 is highlighted:

- *Example 1: Blockchain Security and Data Integrity* [41]: In blockchain systems, SHA3-256 is used to generate cryptographic hashes for blocks. These hashes ensure the integrity and immutability of transaction records. For instance, when a new block is added to a blockchain, its hash is calculated using the SHA3-256 algorithm. Any attempt to alter the block's data would result in a completely different hash, making tampering detectable. This property is crucial for maintaining trust and security in decentralized systems like Ethereum, which has incorporated SHA3-256 into its ecosystem.
- *Example 2: Password Hashing in Authentication Systems* [42]: SHA3-256 is also used in password hashing to store user credentials securely. For example, when a user creates an account on a secure platform, their password is hashed using SHA3-256 before being stored in the database. The input password is hashed again and compared to the stored hash during the login process. This ensures that attackers cannot retrieve the original passwords even if the database is compromised due to the pre-image resistance and high computational cost of reversing SHA3-256 hashes. This application is especially significant for protecting sensitive user data in environments where security breaches are a concern.

3.2.2. SHA3-256 Encryption Algorithm

The SHA3-256 quantum-secure hash can be utilized in various computer systems and network applications, including network adapters, random number generators, secure boot processes, data integrity checks, system file authentication, random number drawing, and hardware authentication tokens [43, 44]. This includes a hard token that contains counter number updates and time value validation for the token, as well as creating cryptographic keys with a valid period for a shared, authenticated, encrypted time-secure quantum key agreement [45, 46], as shown in Figure 4.

The SHA3-256 quantum-secure hash can be implemented through a SHA3-256 encryption algorithm, including the steps of converting plaintext into a binary string with 1600 polarization points, splitting the plaintext into r-bit blocks, encoding each plaintext word of the block into the polarizing states of photons

for establishing bit values, generating the bit value by splitting each of the states' linear direction and circular direction, measuring each of the states to convert them into single values by collecting the photons and hashing the bit values to get the SHA-256 value.

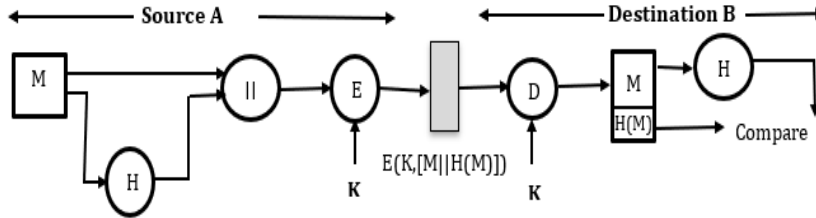


Figure 4. The architecture of Hash Function

Algorithm 1. (SHA-3) Hash Functions

```

keccak [448] (m||01,224)  $\mapsto$  SHA3- 224 (m)
keccak [512] (m||01,256)  $\mapsto$  SHA3- 256 (m)
keccak [768] (m||01,384)  $\mapsto$  SHA3- 384 (m)
keccak [1024] (m||01,1024)  $\mapsto$  SHA3- 512 (m)
keccak [c](N,d)  $\leftarrow$  Sponge [keccak - p[1600,24],pad10*1,r](N,d)
Function SHA-256 (m)
Initialize hash values:  $H_0, H_1, H_2, \dots, H_7$ 
Initialize round constant:  $R_0, R_1, R_2, \dots, R_{63}$ 
Preprocessing the message m:
SPONGE: Input m: input message Output H: hash value
 $Y \leftarrow (-m-2) \bmod r$ 
Add padding
 $\text{Pad} \leftarrow 1 || \text{Zeros}(Y) || 1$ 
Divide the message into (512- bits) blocks
 $P \leftarrow m || 01 || \text{pad}$ 
 $n \leftarrow \text{Len}(P) / r$ 
For all 512 - bits message blocks ( $m_x$ ), do
Divided  $M_x$  into sixteen (32-bit) words:  $w_0, w_1, \dots, w_{15}$ 
For t=16 to 63

$$w_t = w_{t-16} + \sigma_0(w_{t-15}) + w_{t-7} + \sigma_1(w_{t-2})$$

End for
Absorbing:
For I  $\leftarrow$  0 to n-1 do
 $S = S \oplus (P[x * r : (x + 1) * r - 1 || \text{zeros}(c)])$ 
For x  $\leftarrow$  0 to 23 do
Round Function:
Theta

```

```

For I ← 0 to 4, K ← 0 to 63 do
    C[I, K] ← A[I, 0, K] ⊕ A[I, 1, K] ⊕ A[I, 2, K] ⊕ A[I, 3, K] ⊕ A[I, 4, K]
End for
For I ← 0 to 4, K ← 0 to 63 do
    D[I, K] ← C[(I - 1) mod 5, K] ⊕ C[(I + 1) mod 5, (K - 1) mod w]
End for
For I ← 0 to 4, K ← 0 to 63 do
    A1[I, J, K] ← A[I, J, K] ⊕ D[I, K]
End for

```

Rho

```

For t ← 0 to 23, do
    For K ← 0 to 63 do
        A2[I, J, K] ← A1[I, J, (K - ((t + 1) * (t + 2))/2) mod w]
        (I, J) ← (J, (2I + 3J) mod 5)
    End for
End for

```

Pi

```

For I ← 0 to 4, J ← 0 to 4, K ← 0 to 63 do
    A3[I, J, K] ← A2[(I + 3J) mod 5, I, K]
End for

```

chi

```

For I ← 0 to 4, J ← 0 to 4, K ← 0 to 63 do
    A4[I, J, K] ← A3[I, J, K] ⊕ ((A3[(I + 1) mod 5, J, K] ⊕ 1) ∧ A3[(I + 2) mod 5, J, K])
End for

```

Iota

```

For K ← 0 to 63 do
    A5[0, 0, K] ← A4[0, 0, K] ⊕ RC(K)
End for
End for

```

End for**Squeezing:**

```

K ← Truncr(S)

```

Hash value

```

H ← K

```

3.2.3. Mathematical Model of SHA3-256

SHA3-256 is based on the Keccak algorithm, which uses a sponge construction to create a mathematical model for SHA3-256 in the context of a blockchain; the key components of this model include:

A. Input Space

In Figure 5, input the information to the hash function, then calculate the hash message vi eq. (1)

$$S[I][J][K] = S[I][J][K] \oplus (\oplus_{x=0}^4 S[I-1][x][K] \oplus S[I+1][x][K-1]) \quad (1)$$

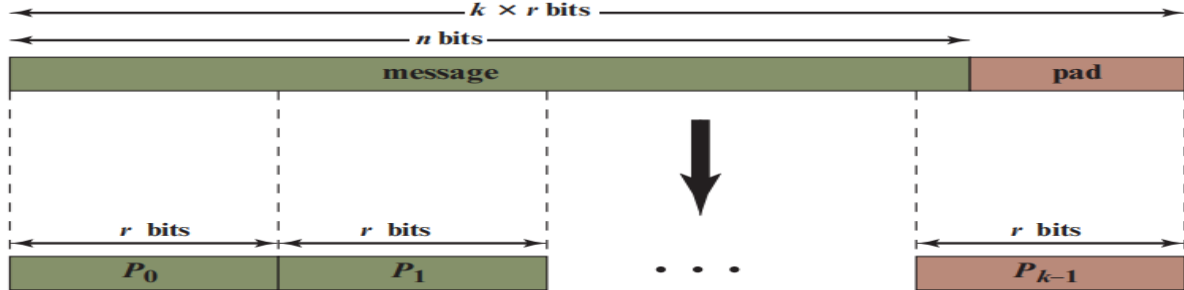


Figure 5. Input Space of SHA3-256

B. Padding and Preprocessing

The padded message is then segmented into fixed-sized sections [47, 48]. For SHA3-256, the block size for the sponge construction's absorption phase is 1088 bits, as shown in Figure 6.

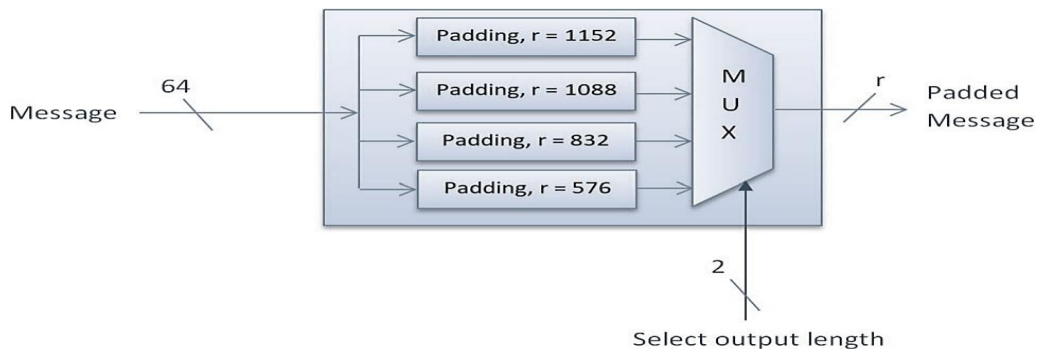


Figure 6. Padding Unit of the SHA-3

C. Sponge Construction

SHA-3 uses a sponge construction, which involves two phases: absorption and squeezing, as shown in Figure 7 [49].

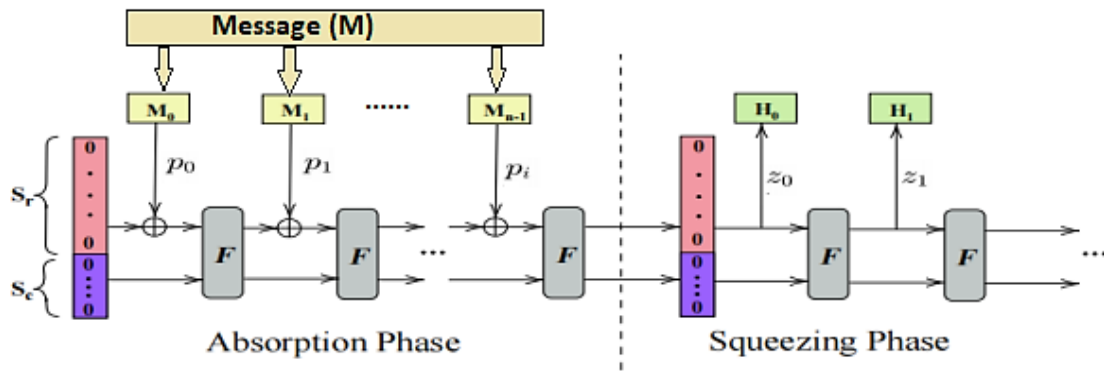


Figure 7. Spongy Construction of SHA-3

D. Permutation Function (Keccak-f)

Theta Step Function, u function is defined in the Keccak reference as depicted in Figure (8), for the bit z in the position (I, J) [50, 51] the following:

θ (Theta): The Theta (θ) function is defined as shown in eq. (2):

$$\theta: a[I, J, K] \leftarrow a[I, J, K] \oplus \sum_{j=0}^4 a[(I-1) \cdot J, K] \oplus \sum_{j=0}^4 a[(I+1) \cdot J, (K-1)] \quad (2)$$

ρ (Rho) and π (Pi): The Rho (ρ) function is defined as follows in eq. (3):

$$\rho: a[I, J, K] \leftarrow a[I, J, K] \text{ if } I = J = 0$$

Otherwise

$$\rho: a[I, J, K] \leftarrow a[I, J, (K - \frac{(t+1)(t+2)}{2})]$$

for which (t) is satisfactory , $0 \leq t \leq 24$ and

$$\left(\frac{0}{2} \frac{1}{3}\right)^t \left(\frac{1}{0}\right) = \left(\frac{1}{J}\right) \text{ in } GF(5)^{2 \times 2} \quad (3)$$

The pi (π) function is defined as shown in eq. (4):

$$\pi: a[I, J] \leftarrow a[I', J'], \text{ with } \begin{pmatrix} I' \\ J' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} I \\ J \end{pmatrix} \quad (4)$$

χ (Chi): The Chi (χ) function is defined in eq. (5):

$$\chi: a[I] \leftarrow a[I] \oplus ((a[I+1] \oplus 1) \text{ AND } A[I+2]) \quad (5)$$

ι (Iota): The Iota (ι) function is defined as follows in eq. (6):

$$\iota: a \leftarrow a \oplus RC[X_r] \quad (6)$$

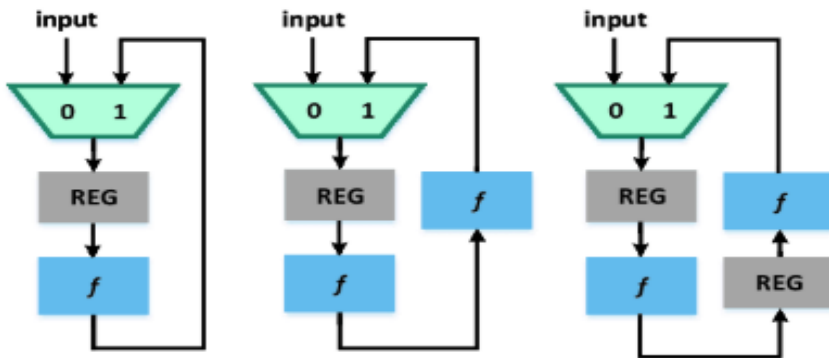


Figure 8. Interval Architecture in SHA-3 Quantum Circuit with Keccak 3- round

E. Output Space

The final output is a fixed-length 256-bit hash value (HHH), representing the digest of the input data (MMM), as illustrated in (9) [52].

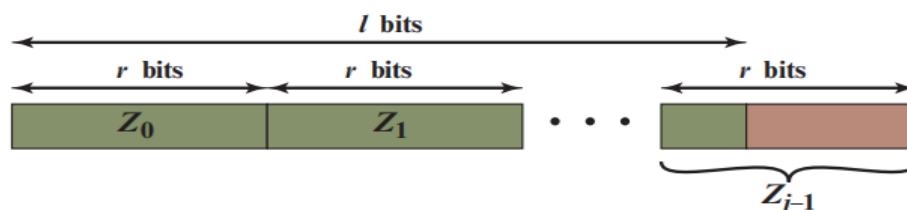


Figure 9. Output space of SHA3-256

3.2.3.1. Properties and Advantages of SHA3-256

The following is the list of properties of SHA3-256:

1. Pre-image resistance: Pre-image resistance is a solid cryptographic property, meaning you cannot compile the corresponding message if the hash code is given.
2. Second pre-image resistance: This property ensures that distinct messages do not produce the same hash code. Similar to property 1, it is practically impossible for technical professionals to create two messages possessing equivalent hash codes [52].
3. Collision resistance: Collision resistance is another fundamental property of cryptographic hash functions, which operate on a data block to generate a fixed-size hash code. As the hash function accepts variable-size messages as the input, the output hash code is treated as a unique digital fingerprint representing the data entered. An ideal hash function should give an exclusive fingerprint for all the file formats [53]. When two independent blocks of input data give the same hash output, it is said to produce a collision. In ideal cases, the hash function should distribute its messages uniformly into varied hash values, and it should not matter whether the changes to the message are small or large.
4. High capacity: SHA-3 utilizes the Merkle-Damgård construction, which has a capacity twice that of the hash length [54].
5. Provides 256 bits of security against pre-image on the function and 128 bits of resistance for collision resistance. Since this is a quantum-safe algorithm, the 256-bit security level is equivalent to that of the AES-128 algorithm [55].
6. Bit-length of 32: 4 bytes * 8 bits/byte, referred to as the word-on-processor for 32-bit processors [56].
7. Contains different logic operations: The algorithm of the SHA-3 hash function is defined based on the cyclic array of 64 bytes and logical operations AND, OR, and XOR; the negation function is involved.
8. Deterministic: The function provides the identical hash output for the identical input message, so Hash (M, X) would continuously deliver the same output for the same M.
9. Speed purpose: The enhanced version of SHA, achieved through sponge construction, offers a higher

speed of operation due to the increased parallelism of the platforms [57]. Overall, the SHA3-256 algorithm was selected primarily based on its security and potential impact on travel time on this digital streaming data service platform.

10. Object: It operates as an array of bytes during the execution of the specified operation.
11. Non-linearity: All the input bits interact with one another, involving the s-box and the same three basic calculations involving the binary OR, the summation, and the exclusive-OR functions[58].
12. Confidence: The strength is based on the non-linear interactions and the non-cooperative calculations used throughout the rounds [59].
13. Collision analysis: The model has not reported a collision to date and provides security against pre and second-image attacks.
14. Strength: Quantum combat-ready cryptographic capabilities are expected to serve a long term and offer the highest available security level [60].

SHA3-256 is fundamentally different from SHA-2 and offers a distinct level of security. While there is nothing wrong with the SHA2 hash functions, using something that offers a lower collision susceptibility is always better. Choosing SHA-3 now will future-proof the applications and services for many years.

3.3. Python Programming Language Overview

Python programming language is widely used all over the world. Python is a highly versatile and easy programming language [61]. Python syntax can be complex, but it supports numerous advanced methods. Python has many features that make it worthwhile. It is considered one of the world's best and most recommended programming languages. It is ideal for machine learning, artificial intelligence, and data analysis for statistics using data frames [19]. Python requires libraries such as Django, Flask, and web2py, among others, to create web applications. It provides new frameworks for developing suitable applications, supporting libraries, and users, as well as developing secure applications such as image processing to ensure quality. These days, Python is the most widely used programming language in software development. It provides straightforward syntax, extensive libraries, and frameworks for users to develop secure applications. This language is used in cybersecurity to develop secure applications through the use of cryptography. There is a vast Python community; as a result of these communities, there are several forums where you can find everything you need to develop an application and enhance your skills with many other experts. This means that many documentation sites help learners and experts increase their knowledge of Python. It is used in cryptography to develop cryptographic algorithms. In the blockchain, we have used the SHA3-256 cryptographic algorithm of the Python programming language [58]. One of the most advanced and

sophisticated Python features is that it provides better solutions for developing complex blockchain projects, such as car and node interactions, Electrum, and RPC tools, which require handling intricate data and processes.

Several programming languages were used to develop the blockchain and secure hash algorithm applications. Java and Python were used to develop the blockchain and cryptographic solutions [62]. However, many developers prefer Java due to its built-in SHA library. Conversely, Python is a popular object-oriented language with a rich set of libraries; it was the programming language of choice for this research. The final Python implementation of the blockchain, which incorporates solid features while keeping it as simple as possible, is presented in this section to assist the reader in configuring the presented prototype. Consequently, the Python implementation of our Blockchain and SHA3-256 blockchain will reduce complexity, facilitating user manipulation and support.

3.3.1. Introduction and Features

Introduction In VANET, an intelligent transportation system has been implemented to reduce traffic accidents, casualties, and inconvenience. However, various security threats exist in VANET; therefore, it is necessary to enhance VANET security. This work proposes methods to enhance the security of VANET by utilizing blockchain and SHA-3-256 in Python [63]. The blockchain utilizes hash pointers and Merkle trees to secure the message consensus algorithm. It separately calculates several hash values of a message using the trust value and the hash of a public key. The proposed method calculates several hash values and appends them to the message in the blockchain network. The appended hash values are derived from the database, and unauthorized users cannot access or tamper with the values of original transactions.

The trust value decides the reward of the consensus node. The SHA-3-256 algorithm encrypts and decrypts the message, storing it in an array within a block folder. The proposed work aims to apply Blockchain to VANET using a decentralized network, a distributed database, transparent record history, a consensus node group, intelligent contracts, and a high level of privacy, considering the VANET environment. In this paper, we describe the theories of Blockchain, SHA-3-256, and proposed methods in VANET security and then explain how to develop an implemented prototype program in Python. In the conclusion, we evaluate the proposed methods.

3.3.2. Implementing SHA3-256 Algorithm in Python

The SHA3-256 hashing algorithm creates a unique hash value based on binary or text data. In many security protocols, hashing is used to check data integrity, as it is generally challenging to invert the function and identify the initial input from a hash [64]. It is not impossible, however, which is why large hash sizes and well-implemented algorithms are essential in security. For this project, I will be creating a Python implementation of SHA3-256. Also, I will use this algorithm to create the hash value for strings, text, and

binary data. We will also implement some simple code to utilize essential collision detection, demonstrating the unique nature of the hashing algorithm. Let us start by creating a Python function using variables and the SHA3-256 algorithm to process a string. I will take the input and run it through padding, message block creation, and permutation processing in the for loop to find the unique hash, as shown in Figure 10.

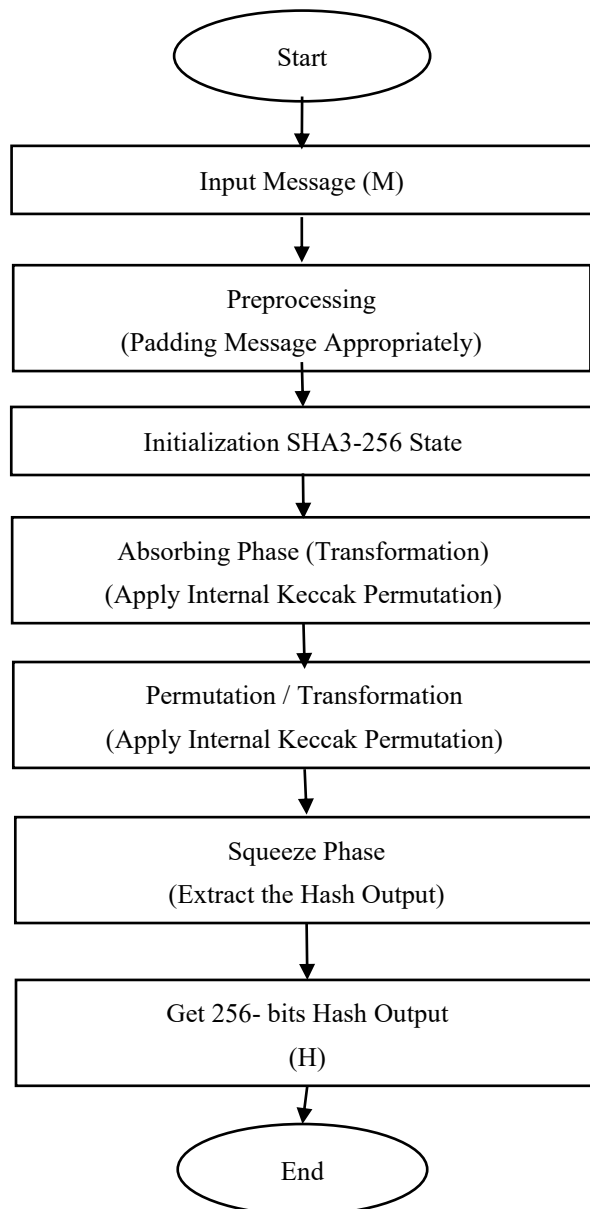


Figure 10. Flowchart of SHA3-256 Algorithm

Performance testing can be conducted by measuring the time required for the program to hash data, thereby assessing the efficiency of the SHA3-256 algorithm implementation. Additionally, the implementation of SHA3-256 can be further optimized through data preprocessing techniques. The hash structure can also be organized into blocks to enhance data transmission speed and efficiency. In the context of VANET security, GroupSHA3-256 can be employed to hash the data or messages transmitted across the network.

3.3.3. Integrating SHA3-256 and Blockchain in Python for VANET Security

Managing trust and security in a VANET is a challenging task. Although authentication is challenging due to the large number of vehicles and limited infrastructure, clever methods for obtaining, representing, and understanding credentials can be implemented. The Blockchain and intelligent contract firewall solution provides authentication for V2V communications in VANETs because the decentralized smart contract stores a continuously updated ledger list. Each ledger member submits credentials that describe its presence, thereby facilitating privacy. Such solutions should be developed to support an ever-increasing number of ledgers [65].

A combination of decentralized technologies using blockchain with the integration of a secure hash algorithm version 3 – 256-bit can enhance the security of VANETs. SHA3-256 ensures data integrity is recorded on the Blockchain [66]. Moreover, it offers a sufficiently long and deterministic string utilized for proof of work within solid blocks. Hence, the role of SHA3-256 is to increase the overall security in VANETs and provide more reliable transportation applications. Several crucial security challenges and solutions for VANETs are identified. In VANETs, blockchain technology facilitates secure, transparent, and non-repudiable transactions in vehicular communications, as shown in Figure 11.

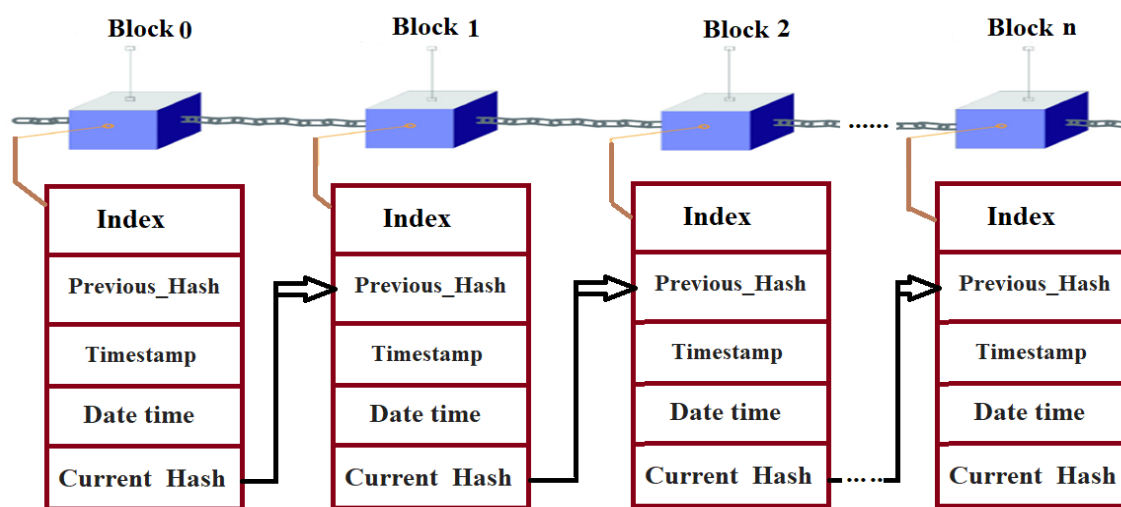


Figure 11. Diagram of SHA3-256 in blockchain

A new direction or research gap may be exploring how VANET services could use cryptographic techniques to enhance the data authentication provided by the anonymous communication service [67]. For instance, practical applications include cryptographic algorithms, such as those used in network protocols, where data are encrypted and other parties possess corresponding decryption keys. The integration of SHA3-256 and Blockchain is unique in addressing some VANET challenges. SHA3-256, a product of an algorithm competition by a cryptographic voting process for a 'crypto-hash' design based on a sponge function, is used in this paper as a methodology for securely hashing data on a blockchain. The synergy of VANETs and blockchain technologies can be realized through decentralized data management and robust hashing of VANET data [68]. Therefore, a practical use case of these decentralized technologies is proposed

in this study as an idea for an advanced VANET mechanism, which guarantees higher integrity, security, privacy, and scalability [69]. The flowchart for implementing a security system using SHA3-256 and Blockchain is represented in Figure 12 [70].

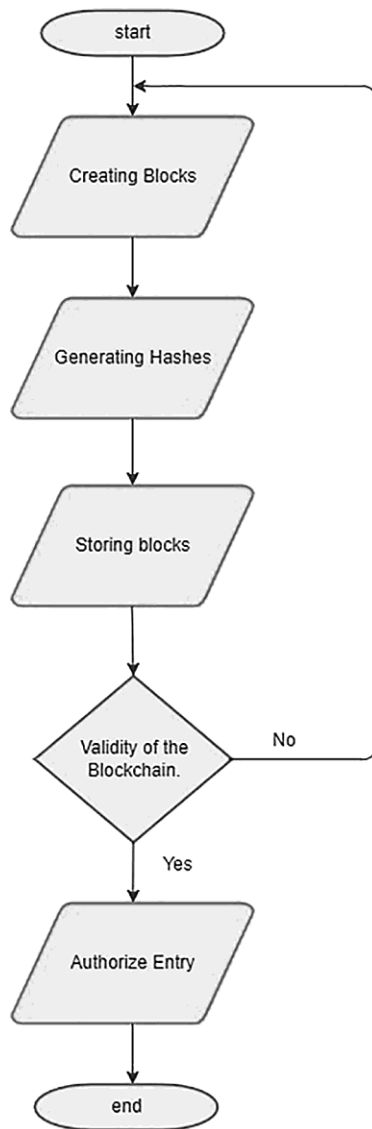


Figure 12. Flowchart of security using SHA3-256 through blockchain technology

3.4. Test Environments Setup

3.4.1. Hardware Configuration

Operating System: Windows 10 (64-bit) A widely used and stable operating system that ensures compatibility with various software tools; CPU: Intel Core (TM- I5, 1.60GHz) - Provides sufficient processing power for running simulations and computations required by the testing tools, and RAM: 4.00 GB - A modest amount of memory, indicating the resource efficiency of the testing tools.

3.4.2. Software Tools

Integrating these tools (Netedit, Sumo, Python) creates a cohesive environment for simulating and

analyzing mobility scenarios: Road networks were designed or modified using Netedit to match real-world scenarios or hypothetical layouts. The edited networks were exported to formats compatible with SUMO for seamless simulation. SUMO was used to simulate vehicle movements, traffic signals, and mobility patterns based on the network created in Netedit. SUMO's flexibility allowed for the addition of traffic demand, routes, and environmental constraints. Python (v3.13) was employed to automate simulation runs, configure parameters, and process the output data from SUMO. Libraries like Traci (Traffic Control Interface) facilitated real-time communication between Python scripts and SUMO for dynamic simulations.

Strengthening the paper's practical contribution resource efficiency: Modest hardware (4GB RAM and Core(TM) i5-8250U CPU) highlights the tools' efficiency and accessibility for researchers or practitioners with limited computational resources. Using standard tools (Netedit, SUMO, Python) ensures that other researchers can replicate the experiments, enhancing the reliability and credibility of the research.

4. Findings and Results

In this case study, 1000 vehicles were used using the Python 3.12 program. All vehicles send messages to each other. The message is entered as input to the hash function, and privacy is applied to it using Sponge construction. The hash value is calculated and extracted with a size of 256 bits after performing a 3- 3 round. The result will be a fixed capacity of 256 bits, regardless of the input message's length. This number will be in one direction only and have a unique value.

The first block of the blockchain is a gene block (zero), after which the previous hash value is combined with the current values in the first block. This process continues consecutively until the last block, as illustrated in Table 2.

Output

Message = Enhancing VANET Security using Blockchain and SHA3-256 in Python

SHA3-256 = 245057b32583dae1699cf414c3eaa08ed10dd97df8c466eb8b622ae4caa7d514

QSKA = b'jUUZil1utpzyP7LIRcT-iL-k_NtPyBpH7VOeNEVFCUk='

Encrypted message using QSKA =

b'gAAAAABngPiGRD-

hoi0WFlx0gZGcZz5zM4vqBcpEFO70uPaXVRmg12p_Xy_1lTefzPB6wdpObP0p4-

ydO7CyBQjVcNrp90Ax8BKFLfHnWrfNw24cyld72scn-65b1JHvPCsYMiGklC5Blk8ckAds-

KVIRirQdc1MU5iT9XWX4HLmquD2oYaIz0UQ='

Decrypted message using QSKA = Enhancing VANET Security using Blockchain and SHA3-256 in Python

Vehicle V1 sends a message to Vehicle V2. Vehicle V2 receives the message: Vehicle Ad Hoc Networks

Security Using SHA3-256.

Table 2. Blockchain using SHA3-256

Index	Message	Previous Hash	Current Hash	Timestamp	Date time
0	Genesis Block	0	4d9fd18cfefc3a9b22c8ec2 97f907f938ee169ad89a6e 9	2025, 1, 10, 270349	3, 12, 11
1	Vehicle V1 sent a message to Ve- hicle V2	4d9fd18cfefc3a9b22c8ec2 97f907f938ee169ad89a6e9	91211525a42c9b12b8371 0f188e68a2e9daf3ccea2b 464	2025, 1, 10, 270420	3, 12, 11
2	Vehicle V2 sent a message to Ve- hicle V3	91211525a42c9b12b83710 f188e68a2e9daf3ccea2b46 4	430a52543fefaf473482d4 838e1aa1a6d84b2ca9eeb9 f4	2025, 1, 10, 270435	3, 12, 11
3	Vehicle V3 sent a message to Ve- hicle V4	430a52543fefaf473482d48 38e1aa1a6d84b2ca9eeb9f4	45d0691017f36058de328 857f8f618b01a8801b8b4e 7a7	2025, 1, 10, 270443	3, 12, 11
4	Vehicle V4 sent a message to Ve- hicle V5	45d0691017f36058de3288 57f8f618b01a8801b8b4e7 a7	696cffe0267aa16a3ba296 361c35a0e22930dde11f0c 82	2025, 1, 10, 270448	3, 12, 11
....					
994	Vehicle V994 sent a message to Vehicle V995	3dbaa2ee93f4e4af7a70245 48429fcaed26deeb749b7d b	791d3d1e2b426b12882df d00106c90030d5b96ba19 12f9	2025, 1, 10, 270543	3, 12, 11
995	Vehicle V995 sent a message to Vehicle V996	791d3d1e2b426b12882dfd 00106c90030d5b96ba1912 f9	50d0b5d19d358b07dd693 82ebfe79f0de5cc168b541 b25	2025, 1, 10, 270553	3, 12, 11
996	Vehicle V966 sent a message to Vehicle V997	50d0b5d19d358b07dd693 82ebfe79f0de5cc168b541b 25	5d9e704ddbba366eb2087 4b442d6b5c5ee1f32ce32d 3eb	2025, 1, 10, 270582	3, 12, 11
997	Vehicle V997 sent a message to Vehicle V998	5d9e704ddbba366eb20874 b442d6b5c5ee1f32ce32d3 eb	ea2a4ae53f79c3c3ed8479 aefa5add89072f06a2db7d 33	2025, 1, 10, 270612	3, 12, 11
998	Vehicle V998 sent a message to Vehicle V999	ea2a4ae53f79c3c3ed8479a efa5add89072f06a2db7d3 3	87838e47b03261920a3b6 d940baac0ad9ab99d2fff4f 2f	2025, 1, 10, 270661	19, 10, 11

5. Discussions

Table 3 compares existing security solutions in VANETs. It is essential to understand their strengths and limitations, as well as how a proposed solution builds upon them.

Table 3. Comparative analysis of security solutions in VANETs

Ref.	Category	Security Technique	Strengths	Limitations	This Work
[2]	Privacy	Pseudonym-based Schemes	- Ensures anonymity - Balances privacy with accountability	- Overhead in pseudonym change - Key management challenges	Blockchain, SHA-3, and VANET technologies offer decentralized, self-verifying security mechanisms, reducing the need for frequent updates and ensuring cryptographic security without patching.
	Preservation	Group Signatures	- Provides anonymity within groups - Efficient for batch verification	- High computational cost - Complex key revocation	VANET with Blockchain & SHA3-256 provided transparent, decentralized key revocation, real-time updates, and smart contracts for dynamic security policy enforcement in compromised vehicles, overcoming cryptographic challenges.
[5]	Intrusion	Anomaly-Based Detection	- Effective for detecting novel attacks - Proactive threat mitigation	- High false-positive rates - Resource-intensive	Blockchain, SHA-3, and VANET technologies enhance data validation, reduce false positives, and improve intrusion detection accuracy through efficient security and distributed computing.
	Detection	Signature-Based Detection	- Reliable for known attack patterns - Low false-positive rates	- Ineffective for zero-day attacks - Requires frequent updates	Blockchain, SHA-3, and VANET technologies safeguard against zero-day threats, guarantee the integrity of software updates, and utilize AI-driven analytics for real-time anomaly detection.
[22, 38]	Cryptographic Solutions	Public Key Infrastructure (PKI)-based Systems	- Strong authentication - Ensures message integrity and non-repudiation	- High computational overhead - Delays in certificate distribution - Scalability issues	- SHA-3 optimization improves hardware efficiency. Lightweight blockchain solutions reduce overhead, and edge computing distributes computational load, - Blockchain-based PKI distributes certificates, - Sharing blockchain enhances scalability.
		Symmetric Key Cryptography	- Low computational overhead - Efficient for large-scale applications	- Key distribution and management challenges - Vulnerable to insider attacks	Blockchain and SHA-3 combine to form a trustless, decentralized, and tamper-proof key management system, ensuring secure distribution, tracing misuse, and enhanced cryptanalysis resistance.
		Hybrid Cryptographic Techniques	- Balances efficiency and security - Reduced key management complexity	- Complex implementation - Dependency on infrastructure	VANET, SHA3-256, and Blockchain technologies improved the security and decentralization of vehicle communication in intelligent transportation systems, utilizing DSRC or 5G for real-time communication and hashed messages for verification.

[23]	Blockchain Solutions	Blockchain-Based Security	- Decentralized authentication - Immutability and traceability	- High latency - Scalability and resource constraints	VANET improves vehicle-to-vehicle communication, reduces server dependency, optimizes blockchain with lightweight consensus mechanisms, and offers efficient cryptographic hashing with lower computational overhead.
[28]	Trust-Based Solutions	Trust Management Models	- Resilient to malicious nodes - Effective for detecting insider threats	- High communication overhead - Difficulty in trust initialization	VANET, SHA-3, and Blockchain are integrated into vehicular networks to enhance communication efficiency, data integrity, and lightweight cryptographic operations, resulting in a secure, efficient, and decentralized network.
		Reputation-Based Systems	- Builds reliability through historical interactions - Reduces reliance on central entities	- Susceptible to false feedback - Slow trust establishment	Integrating VANET, SHA-3, and Blockchain can reduce false feedback and improve communication overhead, trust initialization, and trust establishment in vehicular networks.

6. Conclusions

This research presents a blockchain-based security framework integrated with SHA3-256 encryption to address the vulnerabilities of VANETs. By leveraging blockchain's decentralized trust management and SHA3-256's data integrity features, the proposed solution enhances the security of VANET communications, safeguarding against threats like data tampering, eavesdropping, and unauthorized access. Python scripting for automating simulations further optimizes testing, making it more efficient and adaptable to real-world scenarios.

Integrating blockchain and SHA3-256 significantly improves the reliability of both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, mitigating security risks and fostering a secure environment for intelligent transportation systems. While the proposed framework is theoretically sound, it currently caters to moderately fast-moving entities. Real-world deployment would require more advanced systems capable of handling larger-scale problems, potentially supported by quantum computing in the future.

This research demonstrates a scalable and computationally efficient approach to securing VANETs. Future work could enhance security by integrating digital signatures for stronger authentication and exploring quantum-resistant algorithms to address evolving threats.

Funding: The authors declare that no funding was received for this research.

Declaration of Competing Interest: The authors declare they have no known competing interests.

Research Involving Human/Animal Participants: This article does not involve any studies conducted by authors on animals or human participants.

References

- [1] P. Garrad and S. Unnikrishnan, "Reinforcement learning in VANET penetration testing," *Results in Engineering*, vol. 17, p. 100970, 2023, doi: <http://dx.doi.org/10.1016/j.rineng.2023.100970>.
- [2] J. Ping, Z. Yan, and S. Chen, "A privacy-preserving blockchain-based method to optimize energy trading," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1148-1157, 2022, doi: <http://dx.doi.org/10.1109/TSG.2022.3198165>.
- [3] M. J. N. Mahi, S. Chaki, E. Humayun, H. Imran, A. Barros, and M. Whaiduzzaman, "A Review on VANET Security: Future Challenges and Open Issues," *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, vol. 11, no. 1, pp. 180-193, 2023, doi: <http://dx.doi.org/10.52549/ijeei.v11i1.4295>.
- [4] R. Singh and R. Ujjwal, "Feature Selection Using Bio-Inspired Optimization for IoT Intrusion Detection and Prevention System," *International Journal on Information Technologies & Security*, vol. 15, no. 3, pp. 87-96, 2023, doi: <http://dx.doi.org/10.59035/OEXI6498>.
- [5] M. M. Obaid and M. H. Saleh, "Efficient Intrusion Detection Through the Fusion of AI Algorithms and Feature Selection Methods," *Journal of Engineering*, vol. 30, no. 07, pp. 184-201, 2024.
- [6] S. D. Kotey *et al.*, "Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication," *IET Communications*, vol. 17, no. 8, pp. 891-914, 2023, doi: <http://dx.doi.org/10.1049/cmu2.12594>.
- [7] D. Jia, G. Yang, M. Huang, J. Xin, G. Wang, and G. Y. Yuan, "An efficient privacy-preserving blockchain storage method for internet of things environment," *World Wide Web*, vol. 26, no. 5, pp. 2709-2726, 2023, doi: <http://dx.doi.org/10.1007/s11280-023-01172-0>.
- [8] M. D. Abdul-Jabbar and Y. A. A. S. Aldeen, "State-of-the-art in data integrity and privacy-preserving in cloud computing," *Journal of Engineering*, vol. 29, no. 01, pp. 42-60, 2023, doi: <http://dx.doi.org/10.31026/j.eng.2023.01.03>.
- [9] J. K. Adeniyi *et al.*, "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system," *Egyptian Informatics Journal*, vol. 25, p. 100447, 2024, doi: <http://dx.doi.org/10.1016/j.eij.2024.100447>.
- [10] S. Gaba, S. Nagpal, A. Aggarwal, S. Kumar, and P. Singh, "A modified approach for accuracy enhancement in intruder detection with optimally certain features," in *Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022*: Springer, 2023, pp. 149-157.
- [11] K. Muthulakshmi, K. Kalirajan, J. Jean Justus, and P. Sivamalar, "QoS Aware Data Congestion Control Routing in Mobile Ad Hoc Networks for Intelligent Transportations Systems," *Tehnički vjesnik*, vol. 31, no. 1, pp. 240-246, 2024.
- [12] J. A. R. de Souza, E. R. Cavalcanti, T. de Sales Bezerra, and R. C. d. M. Gomes, "VANETs' research overview updated: past, present and future," *Journal of the Brazilian Computer Society*, vol. 30, no. 1, pp. 380-393, 2024, doi: <http://dx.doi.org/10.5753/jbcs.2024.3354>.
- [13] J. Wheeder, S. Ponnusamy, M. Muqem, and P. R. Bhaladhare, "A Careful Examination of the Security and Traffic Effects Associated with the Vehicle Ad-hoc Network (VANET)," *International Journal of Innovative Science and Research Technology (IJISRT)*, vol. 9, no. 6, pp. 724-728, 2024, doi: <http://dx.doi.org/10.38124/ijisrt/IJISRT24JUN210>.
- [14] Y. G. Khidhir and A. H. Morad, "Comparative Transfer Learning Models for End-to-End Self-Driving Car," *Al-Khwarizmi Engineering Journal*, vol. 18, no. 4, pp. 45-59, 2022, doi: <http://dx.doi.org/10.22153/kej.2022.09.003>.
- [15] S. Wasswa, M. Mojtaba, and S. Fawad, "Cybersecurity in unmanned aerial vehicles: A review," *Sciendo-International Journal on Smart Sensing and Intelligent Systems*, vol. 16, no. 1, pp. 1-16, 2023.
- [16] D. Rani, R. Kumar, and N. Chauhan, "A secure framework for IoT-based healthcare using blockchain and IPFS," *Security and Privacy*, vol. 7, no. 2, p. e348, 2024, doi: <http://dx.doi.org/10.1002/spy2.348>.
- [17] H. Zhang, M. You, T. Liu, Q. Zhang, and Y. Liu, "Variable Cluster Routing for Large-scale Human-Robot Collaboration Systems-A Top-Down Cluster Routing," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 6, pp. 8266-8280, 2024, doi: <http://dx.doi.org/10.1109/TVT.2024.3353799>.

- [18] D. Kandeepan and R. Durga, "An optimized secure dual authentication for VANETs," *Computer Software and Media Applications*, vol. 6, no. 1, p. 3061, 2024, doi: 10.24294/csma.v6i1.3061.
- [19] M. M. A. Muslam, "Enhancing security in vehicle-to-vehicle communication: a comprehensive review of protocols and techniques," *Vehicles*, vol. 6, no. 1, pp. 450-467, 2024, doi: <http://dx.doi.org/10.3390/vehicles6010020>.
- [20] A. A. Mehta *et al.*, "Securing the future: A comprehensive review of security challenges and solutions in advanced driver assistance systems," *IEEE Access*, vol. 12, pp. 643-678, 2023, doi: <http://dx.doi.org/10.1109/ACCESS.2023.3347200>.
- [21] N. S. Rajput *et al.*, "Amalgamating vehicular networks with vehicular clouds, AI, and big data for next-generation its services," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 1, pp. 869-883, 2023, doi: <http://dx.doi.org/10.1109/TITS.2023.3234559>.
- [22] S. Suegami, "Cryptographic obfuscation for smart contracts: Trustless bitcoin bridge and more," *Blockchain: Research and Applications*, vol. 4, no. 1, p. 100118, 2023, doi: <http://dx.doi.org/10.1016/j.bcr.2022.100118>.
- [23] T.-T. Kuo and P. Zhang, "Blockchain and distributed ledger technology—enabled architectures for improving healthcare," vol. 6, ed: Frontiers Media SA, 2023, p. 1275474.
- [24] J. P. Queralta, F. Keramat, S. Salimi, L. Fu, X. Yu, and T. Westerlund, "Blockchain and emerging distributed ledger technologies for decentralized multi-robot systems," *Current Robotics Reports*, vol. 4, no. 3, pp. 43-54, 2023, doi: <http://dx.doi.org/10.1007/s43154-023-00101-3>.
- [25] R. A. Falih, Y. Y. B. Jusoh, and D. J. Khadhim, "New Research Trends in Designing E-Government Architecture Based on Blockchain Technology," *Journal of Engineering*, vol. 29, no. 11, pp. 17-36, 2023, doi: <http://dx.doi.org/10.31026/j.eng.2023.11.02>.
- [26] P. Yao, B. Yan, T. Yang, Y. Wang, Q. Yang, and W. Wang, "Security Enhanced Operational Architecture for Decentralized Industrial Internet of Things: A Blockchain-based Approach," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 11073- 11086, 2024, doi: <http://dx.doi.org/10.1109/IIOT.2023.3329352>.
- [27] Y. Chen, Q. Yang, X. Zeng, D. Yang, and X. Li, "A New Identity Authentication and Key Agreement Protocol Based on Multi-Layer Blockchain in Edge Computing," *IEEE Access*, 2023, doi: <http://dx.doi.org/10.1109/ACCESS.2023.3347808>.
- [28] R. Huang, X. Yang, and P. Ajay, "Consensus mechanism for software-defined blockchain in internet of things," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 52-60, 2023, doi: <http://dx.doi.org/10.1016/j.iotcps.2022.12.004>.
- [29] S. Singh, N. K. Rajput, V. K. Rath, H. M. Pandey, A. K. Jaiswal, and P. Tiwari, "Securing blockchain transactions using quantum teleportation and quantum digital signature," *Neural Processing Letters*, pp. 1-16, 2023, doi: <http://dx.doi.org/10.1007/s11063-020-10272-1>.
- [30] K. Sutradhar, "A quantum cryptographic protocol for secure vehicular communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 5, pp. 3513-3522, 2023, doi: <http://dx.doi.org/10.1109/TITS.2023.3322728>.
- [31] M. Mastriani, "Quantum key secure communication protocol via enhanced superdense coding," *Optical and Quantum Electronics*, vol. 55, no. 1, p. 10, 2023, doi: <http://dx.doi.org/10.1007/s11082-022-04303-5>.
- [32] J. Miao, Z. Wang, Z. Wu, X. Ning, and P. Tiwari, "A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things," *Expert Systems with Applications*, vol. 237, p. 121329, 2024, doi: <http://dx.doi.org/10.1016/j.eswa.2023.121329>.
- [33] J. Lee *et al.*, "Blockchain-based data access control and key agreement system in iot environment," *Sensors*, vol. 23, no. 11, p. 5173, 2023, doi: <http://dx.doi.org/10.3390/s23115173>.
- [34] Z. Du, Y. Li, Y. Fu, and X. Zheng, "Blockchain-based access control architecture for multi-domain environments," *Pervasive and Mobile Computing*, vol. 98, p. 101878, 2024, doi: <http://dx.doi.org/10.1016/j.pmcj.2024.101878>.
- [35] Z. Su, "Evidentiary value and evidentiary status of blockchain evidence," *The International Journal of Evidence & Proof*, vol.58, no. 1, pp. 58-76, 2024, doi: <http://dx.doi.org/10.1177/13657127241238020>.
- [36] A. Y. Hassan and M. H. Saleh, "Intelligent Dust Monitoring System Based on IoT," *Journal of Engineering*, vol. 30, no.

- 06, pp. 39-56, 2024, doi: <http://dx.doi.org/10.31026/j.eng.2024.06.03>.
- [37] N. H. Hussein *et al.*, "SDN-Based VANET Routing: A Comprehensive Survey on Architectures, Protocols, Analysis, and Future Challenges," *IEEE Access*, pp. 1-1, 2024, doi: <http://dx.doi.org/10.1109/ACCESS.2024.3355313>.
- [38] S. A. Alahmari, S. Rajeyyagari, and F. Al-Turjman, "Davis Mayer Streebog Cryptographic Hash-Based Blockchain for Secure Transaction Management Using SDN in IIoT Applications," *Journal of Signal Processing Systems*, vol. 95, no. 2, pp. 241-252, 2023, doi: <http://dx.doi.org/10.1007/s11265-022-01825-9>.
- [39] U. Cali, M. Kuzlu, O. Elma, O. G. Gucluturk, A. Kilic, and F. O. Catak, "Cybersecurity and digital privacy aspects of V2X in the EV charging structure," in *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*, 2023, pp. 174-180, doi: <http://dx.doi.org/10.1145/3590777.3591406>.
- [40] G. A. Qadir and B. K. Hussan, "An Authentication and Access Control Model for Healthcare based Cloud Services," *Journal of Engineering*, vol. 29, no. 03, pp. 15-26, 2023, doi: <http://dx.doi.org/10.31026/j.eng.2023.03.02>.
- [41] A. A. Abdellatif, K. Shaban, and A. Massoud, "Blockchain-enabled distributed learning for enhanced smart grid security and efficiency," *Computers and Electrical Engineering*, vol. 123, p. 110012, 2025, doi: <http://dx.doi.org/10.1016/j.compeleceng.2024.110012>.
- [42] M. Jubur, P. Shrestha, and N. Saxena, "An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools," *ACM Computing Surveys*, 2025, doi: <http://dx.doi.org/10.1145/3711117>.
- [43] L. Noirie and R. Varloot, "Authentication through error estimation in qkd," in *GLOBECOM 2023-2023 IEEE Global Communications Conference*, 2023: IEEE, pp. 1369-1374, doi: <http://dx.doi.org/10.1109/GLOBECOM54140.2023.10437678>.
- [44] A. Sideris, T. Sanida, and M. Dasygenis, "Hardware acceleration design of the SHA-3 for high throughput and low area on FPGA," *Journal of Cryptographic Engineering*, vol. 14, no. 2, pp. 193-205, 2024, doi: <http://dx.doi.org/10.1007/s13389-023-00334-0>.
- [45] A. Sideris and M. Dasygenis, "Enhancing the hardware pipelining optimization technique of the sha-3 via fpga," *Computation*, vol. 11, no. 8, p. 152, 2023, doi: <http://dx.doi.org/10.3390/computation11080152>.
- [46] M. S. de Alencar, *Cryptography and Network Security*. River Publishers, 2022.
- [47] S. Hussain, S. Tahir, A. Masood, and H. Tahir, "Blockchain-enabled Secure Communication Framework for Enhancing Trust and Access Control in the Internet of Vehicles (IoV)," *IEEE Access*, 2024, doi: <http://dx.doi.org/10.1109/ACCESS.2024.3431279>.
- [48] M. S. Mohammed *et al.*, "Low-cost autonomous car level 2: Design and implementation for conventional vehicles," *Results in Engineering*, vol. 17, p. 100969, 2023, doi: <http://dx.doi.org/10.1016/j.rineng.2023.100969>.
- [49] A. H. Jasim and A. H. Kashmar, "An Evaluation of RSA and a Modified SHA-3 for a New Design of Blockchain Technology," in *Artificial Intelligence for Smart Healthcare*: Springer, 2023, pp. 477-489.
- [50] P. Natho, S. Somsuphaprunyos, S. Boonmee, and S. Boonying, "Comparative study of password storing using hash function with MD5, SHA1, SHA2, and SHA3 algorithm," *International Journal of Reconfigurable and Embedded Systems*, vol. 13, no. 2, pp. 502-511, 2024, doi: <http://dx.doi.org/10.11591/ijres.v13.i3.pp502-511>.
- [51] A. E. Putra, O. Natan, and J. E. Istiyanto, "Optimizing FPGA Resource Allocation for SHA-3 Using DSP48 and Pipelining Techniques," *IJUM Engineering Journal*, vol. 26, no. 1, pp. 240 - 253, 01/10 2025, doi: 10.31436/ijumej.v26i1.3328.
- [52] A. C. Chen, "Evaluation of Hash Algorithm Performance for Cryptocurrency Exchanges Based on Blockchain System," *arXiv preprint arXiv:2408.11950*, 2024.
- [53] L. Grassi, D. Khovratovich, R. Lüftenegger, C. Rechberger, M. Schafnegg, and R. Walch, "Hash Functions Monolith for ZK Applications: May the Speed of SHA-3 be With You," *IACR Cryptol. ePrint Arch.*, vol. 2023, p. 1025, 2023.
- [54] N. Mouha and C. Celi, "A vulnerability in implementations of SHA-3, SHAKE, EdDSA, and other NIST-approved algorithms," in *Cryptographers' Track at the RSA Conference*, 2023: Springer, pp. 3-28, doi: https://doi.org/10.1007/978-1-4939-9898-8_1.

- http://dx.doi.org/10.1007/978-3-031-30872-7_1.
- [55] K. Jang *et al.*, "Quantum Implementation and Analysis of SHA-2 and SHA-3," *Cryptology ePrint Archive*, 2024, doi: <http://dx.doi.org/10.1109/TETC.2025.3546648>.
 - [56] R. Vaughn and M. Borowczak, "Strict Avalanche Criterion of SHA-256 and Sub-Function-Removed Variants," *Cryptography*, vol. 8, no. 3, p. 40, 2024, doi: <http://dx.doi.org/10.3390/cryptography8030040>.
 - [57] A. Castro, "qoctrtools: A program for quantum optimal control calculations," *Computer Physics Communications*, vol. 295, p. 108983, 2024, doi: <http://dx.doi.org/10.1016/j.cpc.2023.108983>.
 - [58] M. Bashirov, R. Vildanov, A. Sabiryanova, D. Fokin, and E. Isaev, "Development and research of an intelligent control system and protection of electrical network equipment," in *E3S Web of Conferences*, 2024, vol. 494: EDP Sciences, p. 03008, doi: <http://dx.doi.org/10.1051/e3sconf/202449403008>.
 - [59] G. Archana, R. Goyal, and K. M. Kumar, "Blockchain-Driven Optimized Chaotic Encryption Scheme for Medical Image Transmission in IoT-Edge Environment," *International Journal of Computational Intelligence Systems*, vol. 18, no. 1, p. 11, 2025, doi: <http://dx.doi.org/10.1007/s44196-024-00731-1>.
 - [60] W. Li, W. Susilo, C. Xia, L. Huang, F. Guo, and T. Wang, "Secure data integrity check based on verified public key encryption with equality test for multi-cloud storage," *IEEE Transactions on Dependable and Secure Computing*, 2024, doi: <http://dx.doi.org/10.1109/TDSC.2024.3375369>.
 - [61] C. Deriu, "Vehicular Communication for Road Safety: Simulation and Analysis of Emergency Vehicles Preemption Using Traffic Light-Based V2I Technology," Politecnico di Torino, 2024.
 - [62] J. W. Lee *et al.*, "Traffic control via connected and automated vehicles: An open-road field experiment with 100 cavs," *arXiv preprint arXiv:2402.17043*, 2024, doi: <http://dx.doi.org/10.1109/MCS.2024.3498552>.
 - [63] V. Regener, G. Römmelt, A. Zeiselmaier, L. Wasmeier, and A. Bogensperger, "Design choices in peer-to-peer energy markets with active network management," *IET Smart Grid*, vol. 5, no. 4, pp. 281-296, 2022, doi: <http://dx.doi.org/10.1049/stg2.12067>.
 - [64] M. Juma, F. Alattar, and B. Touqan, "Securing big data integrity for industrial IoT in smart manufacturing based on the trusted consortium blockchain (TCB)," *IoT*, vol. 4, no. 1, pp. 27-55, 2023, doi: <http://dx.doi.org/10.3390/iot4010002>.
 - [65] A. Petcu, B. Pahontu, M. Frunzete, and D. A. Stoichescu, "A secure and decentralized authentication mechanism based on web 3.0 and ethereum blockchain technology," *Applied Sciences*, vol. 13, no. 4, p. 2231, 2023, doi: <http://dx.doi.org/10.3390/app13042231>.
 - [66] Z. Amine, H.-S. Naima, and A. Ali-Pacha, "A secure hash function based on sponge construction and chaos-maps," *International Journal of Computational Science and Engineering*, vol. 25, no. 3, pp. 285-297, 2022, doi: <http://dx.doi.org/10.1504/IJCSE.2022.123116>.
 - [67] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1-39, 2024, doi: <http://dx.doi.org/10.1145/3656166>.
 - [68] O. I. Kadhm and A. H. Hamad, "High Transaction Rates Performance Evaluation for Secure E-government Based on Private Blockchain Scheme," *Al-Khwarizmi Engineering Journal*, vol. 19, no. 3, pp. 44-55, 2023, doi: <http://dx.doi.org/10.22153/kej.2023.06.002>.
 - [69] N. Alturki *et al.*, "Efficient and Secure IoT Based Smart Home Automation Using Multi-Model Learning and Blockchain Technology," *CMES-Computer Modeling in Engineering & Sciences*, vol. 139, no. 3, 2024.
 - [70] I. Darmawan, F. Maulana, A. Rahmatulloh, and R. Gunawan, "Beccak: Combination of Blockchain and Keccak Algorithm for Improved Digital Signature Performance," in *2024 7th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 11-11 Dec. 2024, pp. 173-179, doi: [10.1109/ISRITI64779.2024.10963467](https://doi.org/10.1109/ISRITI64779.2024.10963467)