


Article

Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy

Rubén Juárez  and Borja Bordel * 

Department of Informatics Systems, Universidad Politécnica de Madrid, 28031 Madrid, Spain; ruben.juarez@alumnos.upm.es

* Correspondence: borja.bordel@upm.es; Tel.: +34-910673699

Abstract: This manuscript delineates the development of an avant garde dual-layer blockchain architecture, which has been meticulously engineered to augment the security and operational efficacy of vehicular ad hoc networks (VANETs). VANETs, which are integral to the infrastructure of intelligent transport systems, facilitate the critical exchange of information between vehicular nodes. Despite their significance, these networks confront an array of formidable security vulnerabilities. Our innovative approach, employing a dual blockchain framework—the event chain and the reputation chain—meticulously tracks network activities, thereby significantly enhancing the trustworthiness and integrity of the system. This research presents a transformative dual-layer blockchain architecture, which was conceived to address the intricate security challenges pervasive in VANETs. The architecture pivots on a sophisticated reputation assessment framework, thus leveraging the principles of Bayesian inference and the analytical rigor of historical data to markedly diminish observational errors, as well as elevate the accuracy of reputation evaluations for vehicular nodes. A salient feature of our methodology is the implementation of an attenuation factor, which has been deftly calibrated to modulate the impact of historical behaviors on current reputation scores, thereby ensuring their relevance and alignment with recent vehicular interactions. Additionally, the numerical threshold serves as an indispensable mechanism, thus establishing a definitive criterion for the early identification of potentially malicious activities and enabling the activation of proactive security measures to safeguard the network’s integrity. Empirical validation of our dual-layer blockchain model has yielded a remarkable 86% efficacy in counteracting malevolent behaviors, thus significantly outperforming extant paradigms. These empirical outcomes underscore the model’s potential as a vanguard in the domain of secure and efficient reputation management within VANETs, thereby heralding a substantial advancement in the sphere of intelligent transportation systems.



Citation: Juárez, R.; Bordel, B. Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. *Electronics* **2023**, *12*, 4794. <https://doi.org/10.3390/electronics12234794>

Academic Editors: Mikolaj Karpinski, Oleksandr O. Kuznetsov and Roman Oliynykov

Received: 1 October 2023

Revised: 21 November 2023

Accepted: 25 November 2023

Published: 27 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: vehicular ad hoc networks (VANETs); blockchain; probabilistic identification; network threat mitigation; reputation assessment; network efficiency; connected vehicle security

1. Introduction

The Internet of Vehicles (IoVs) represents an emerging application scenario for Internet of Things (IoTs) technology. At the heart of this technological evolution are vehicular ad hoc networks (VANETs), which facilitate communication between vehicles and between vehicles and infrastructures, thus constituting a key subset of the IoVs. VANETs have emerged as one of the most exciting research fields within intelligent transport systems, thereby providing safety and convenience information for drivers [1]. These networks can communicate the complex and dynamic data generated by vehicles, humans, and the environment in real time, such as traffic conditions, traffic accidents, road construction, and congestion. However, VANETs are especially vulnerable to a variety of security threats, including malicious attacks and the distribution of unreliable information, which can have severe consequences, such as traffic accidents.

Additionally, the distinct characteristics of VANETs introduce significant challenges in terms of security management, privacy, and reliability in their design [2,3]. So, creating an efficient anonymous authentication system with low computational cost [4] in a vehicular ad hoc network (VANET) represents a considerable challenge [5].

Specifically, in the realm of vehicular ad hoc networks (VANETs), the development of an efficient anonymous authentication system that maintains low computational costs poses significant challenges due to several intrinsic characteristics of these networks:

1. **High Vehicle Mobility:** The highly dynamic nature of VANETs, which are characterized by vehicles moving at high speeds, results in frequent changes in network nodes. This demands an authentication system that is capable of rapidly adapting to changes in network topology without compromising on security or performance.
2. **Resource Limitations in Vehicles:** Despite being equipped with advanced technologies, modern vehicles still face limitations in terms of processing power and storage capacity. An efficient authentication system must operate within these resource constraints, thereby ensuring light computational loads.
3. **Anonymity and Privacy Needs:** Given the sensitive nature of vehicular data, such as location and movement patterns, ensuring user anonymity and privacy is paramount. Achieving this without significantly increasing the computational burden adds complexity to system design.
4. **Diversity and Scalability:** VANETs support a wide array of applications, from road safety to infotainment services, each with its unique security requirements. The authentication system must be versatile enough to cater to these diverse needs and scalable to handle the increasing number of connected vehicles.
5. **Resistance to Attacks and Frauds:** Authentication systems in VANETs must be robust against various security threats, including impersonation attacks, Sybil attacks, and data manipulation. Designing a system that can effectively counter these threats without imposing excessive computational demands is a significant challenge.

For these reasons, developing an efficient and low-cost computational anonymous authentication system for VANETs is not only crucial for ensuring security and privacy within these networks, but also poses substantial technical challenges. Our research aims to address these challenges through an innovative approach that balances security, efficiency, and practicality.

On the other hand, the incorporation of blockchain technology in VANETs presents a paradigm shift from traditional centralized systems to a more resilient, transparent, and decentralized framework. The blockchain, known for its immutable and secure ledger, is leveraged to enhance the tracking and verification of vehicular movements and interactions. This technology has shown promise in mitigating the inherent vulnerabilities of VANETs, thereby providing a robust platform for secure vehicular communication.

With the growing adoption of blockchain technology across various sectors, including transportation [6], this technology has also shown promise in resolving the challenges within VANETs. Blockchain technology provides a decentralized, secure, and trustworthy database maintained by network nodes [7,8]. In this way, it can be used to track, organize, and verify interactions among vehicles in the network.

In addition, blockchain technology can be also employed for securization purposes.

Cybersecurity threats to vehicular ad hoc networks (VANETs) have escalated in recent years, primarily due to their critical role in managing sensitive vehicular data [9]. The conventional centralized systems, typically operated by vehicle service providers, have demonstrated several security shortcomings. These systems often fail to offer the robust defense mechanisms necessary to protect against sophisticated cyberthreats, thus resulting in notable vulnerabilities within vehicular networks [10].

Additionally, the proliferation of wireless connected devices has exponentially increased the complexity of ensuring secure vehicular communications [11]. The intricate web of data exchange within VANETs demands a security solution that transcends the capabilities of traditional centralized systems. Herein lies the potential of blockchain

technology—it offers a decentralized approach that inherently enhances the security, performance, and scalability of VANETs [12].

Blockchain technology's application in VANETs extends beyond mere communication security [13,14]. It revolutionizes the entire ecosystem by enabling immutable record-keeping for vehicular history, thereby ensuring data integrity and fostering a transparent environment for data exchange. This immutable nature of blockchain technology is particularly pivotal, as it ensures that once vehicle data are recorded on the ledger, they cannot be altered or tampered with, thereby instilling trust in the vehicular data records [15].

In most prior approaches, vehicle security in VANETs was accomplished each time it entered the territory of a roadside unit (RSU). Relying solely on a single RSU presents a multitude of challenges. Firstly, it can become a performance bottleneck, especially in high-density areas where numerous vehicles might be entering or exiting simultaneously, thereby leading to latency in certification processes. Secondly, a solitary RSU becomes a single point of failure; if it malfunctions or becomes compromised, it can disrupt the certification of all the vehicles under its jurisdiction. This can also lead to potential security vulnerabilities, where malicious entities might target the RSU to either gain unauthorized access or to disrupt normal operations. Furthermore, there is an inherent lack of redundancy, meaning that if one RSU is down or is facing technical glitches, there is not an immediate backup system in place to continue the vehicle certification.

Integrating blockchain technology can alleviate some of these concerns [16,17]. The decentralized nature of the blockchain ensures that no single point of failure exists, thereby enhancing the robustness and resilience of the system [18]. Every transaction, in this case, vehicle certifications, can be recorded on the blockchain, thus making the data tamper-proof and ensuring its integrity. Moreover, the blockchain's consensus mechanisms can be leveraged to validate vehicle entries, thereby reducing the burden on a single RSU and distributing the task across multiple nodes or participants in the network. This not only streamlines the certification process, but also introduces an added layer of security, thus making it exceedingly difficult for malicious actors to compromise the system.

In other words, the transition from traditional centralized systems to blockchain-based solutions equips VANETs with enhanced resilience against data breaches and unauthorized access. The decentralized nature of the blockchain mitigates the risk of single points of failure, which are inherent in centralized systems. Moreover, the blockchain empowers all network participants to engage in the maintenance of the ledger, thereby promoting a transparent and tamper-proof ecosystem [19].

In essence, the blockchain stands as a vanguard technology that propels VANETs into a new era of security and reliability. It ensures that vehicular communications are not only secure, but that they also conducted within a framework that is inherently resistant to cyber attacks. By integrating blockchain solutions, VANETs evolve into more resilient, transparent, and decentralized networks that are capable of withstanding the escalating threats in today's cybersecurity landscape [20].

In this context, this paper proposes a security architecture for the VANET using blockchain technology. Traditional security solutions, such as public key infrastructure (PKI), have limitations when applied to the VANET, particularly due to the high mobility and short-term connectivity of the network. Previous reputation management models have attempted to address these challenges but have faced unresolved issues [21].

In addition, although VANETs can benefit from Internet of Things (IoTs) technologies to communicate connected remote devices [22], the diversity of formats, resolutions, information sources, and mediums in VANETs makes interactions in these networks a complex task [23].

The use of blockchain technology not only maintains the security and accountability of vehicle interactions, but also facilitates the tracking of vehicle position and movements. Our solution aims to improve the capacity for successfully detecting attacks against the VANET and attacks from malicious nodes, thereby ensuring both efficient and secure vehicular communications. Our solution aims to increase the success rate in detecting attacks against

the VANET and attacks from malicious nodes. Specifically, this architecture generates secure hashes for each vehicular interaction and allows for the verification of these by each node in the network, thereby minimizing the possibility of illegal activities within the VANET system.

Our paper presents several key contributions that collectively address the critical issues surrounding vehicular ad hoc networks (VANETs). These contributions introduce advancements in multiple domains within the VANET ecosystem. Specifically, they include the following:

- **Architecture of Security for VANET:** Our proposed architecture leverages blockchain technology to significantly enhance the security of VANET systems. It provides a robust framework for secure and reliable communication among vehicles.
- **Generation of Secure Hashes for Vehicular Interactions:** We introduce a novel method for generating secure hashes for each vehicular interaction. This method ensures the integrity and authenticity of the interactions, thereby contributing to a safer and more reliable network.
- **Network-Wide Verification and Mitigation of Illegal Activities:** Our architecture enables each node in the VANET network to verify the interactions through the generated hashes. This decentralized verification process bolsters the overall security of the system, thereby effectively minimizing the potential for illegal activities.

And these advances have different practical implications in real-life scenarios. For example, they include the following:

- **Enhanced Security:** The architecture significantly elevates the security level in VANETs by leveraging a dual-layer blockchain approach, thereby ensuring the authenticity and integrity of vehicular communications, which is critical for applications like emergency response and traffic management.
- **Improved Efficiency:** By reducing the observation errors in reputation assessment [24], the system enhances the overall network efficiency, which is crucial for real-time applications such as collision avoidance systems and dynamic traffic light control.
- **Scalability:** The architecture is designed to be scalable, thus making it capable of accommodating the growing number of connected vehicles and diverse data transactions within VANETs, thereby making it suitable for the expanding scope of smart city projects.

Together, these contributions form a comprehensive solution that addresses the ongoing challenges related to security, privacy, and reliability in VANETs.

Going forward, the rest of this document is organized as follows:

- Section 2 provides a critique of the current solutions and underscores their limitations. This section delves into the myriad of security challenges in VANETs, thereby elucidating the predominant types of attacks that these networks are susceptible to. Additionally, it explores a range of proposed security measures designed to mitigate such attacks, thus presenting an insightful overview of the security landscape in VANETs [25]. In addition, this section offers a detailed taxonomy of the security solutions tailored for VANETs, thereby dissecting various types of security measures that have been proposed. It thoroughly evaluates the advantages and drawbacks of these solutions, thereby providing an extensive guide for researchers and practitioners in the field [26]. These mechanisms include various trust management methods in VANETs, thus elucidating their respective strengths and weaknesses and offering a balanced perspective on the topic [27].
- Section 3 dives into our proposed system, thus offering a detailed overview of the algorithm, methodology, and its unique benefits. It discusses the shortcomings of the existing systems and demonstrates how our proposal effectively addresses them.
- Section 4 provides a comprehensive evaluation of our prototype, thus examining its performance and scalability metrics.

- Section 5 concludes the paper by recapping the key contributions and exploring potential directions for future research.

2. Related Work

In this section (Section 2.1), we analyze the state of the art with respect to blockchain solutions for VANETs, trust models for vehicle nodes and networks, and the most critical and dangerous cyber attacks and their potential mitigation strategies. Later, in Section 2.2, the benefits, improvements, and advantages achieved by the proposed technology are discussed.

2.1. Blockchain Solutions for VANETs, Trust Models, Cyber Attacks, and Mitigation Strategies

Vehicular ad hoc networks (VANETs) are a specific form of mobile ad hoc networks (MANETs) that connect vehicles on the move. The main goal of VANETs is to provide road safety, traffic management, and various infotainment services. Due to the critical nature of these services, data security, privacy, and reliable communication are of paramount importance. However, the highly dynamic and distributed nature of VANETs presents unique challenges to maintaining these aspects. Traditional security measures are often inadequate due to the absence of a fixed infrastructure, high mobility, and the heterogeneous environment in VANETs [28].

Vehicular ad hoc networks (VANETs) are highly susceptible to various forms of attacks [29], including denial-of-service, impersonation, and the spread of false information, among others [30,31]. Traditional security mechanisms often fall short with respect to adequately securing these networks due to their unique characteristics such as high mobility and varying node densities. Public key infrastructure (PKI) has been widely used but comes with limitations when dealing with high-speed, short-range vehicular interactions [32,33].

Traditional PKI systems are predicated on the assumption of relatively stable and prolonged interactions between entities. However, VANETs are characterized by high-speed movement and fleeting encounters between vehicles. This dynamic nature can lead to several issues with PKI, such as the following:

- **Rapid Change of Context:** The fast-paced environment can outpace the PKI's ability to update and validate certificates, thereby leading to delays or errors in authentication.
- **Scalability Concerns:** The sheer volume of high-frequency interactions requires a PKI system to handle a significant number of certificate validations within a minimal time frame, which can form a scalability bottleneck.
- **Latency in Certificate Revocation:** The time-sensitive nature of revoking compromised certificates can be at odds with the quick interaction times, thereby potentially allowing unauthorized access.

Blockchain technology has recently shown promise in enhancing VANET security by providing a decentralized approach that could potentially solve many of the challenges associated with traditional architectures [34,35]:

- **Decentralization:** The blockchain operates on a peer-to-peer network that inherently supports the dynamic and decentralized nature of VANETs, thereby facilitating faster and more efficient verifications.
- **Immediate Validation:** Transactions and communications in a blockchain network can be validated in real time, which aligns well with the high-speed requirements of VANETs.
- **Immutable Ledger:** The blockchain ledger [36] provides a tamper-proof record of all transactions, including authentications and data exchanges, thereby enhancing trust in vehicular communications.

Various studies have investigated the application of blockchain technology in managing secure and reliable data exchanges in VANETs. In the following Figure 1, a general view of the blockchain-based architectures in VANETs is presented. As can be seen, while input communications in blockchain networks require a specific cryptographic configuration and service interface (only deployed in the RSU), output validated data are published as public

events (output flows in the blockchain networks can only be managed as events), and the vehicle node can capture that information without the intervention of the RSU.

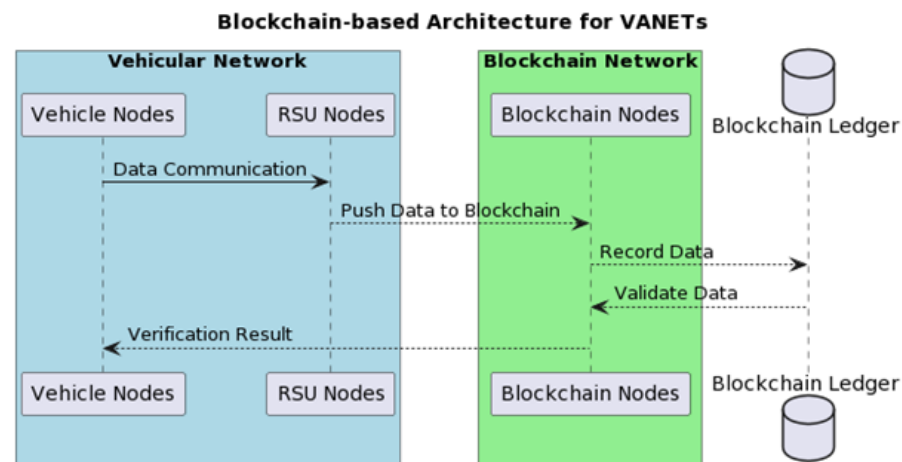


Figure 1. Blockchain-based architecture for VANETs.

On the other hand, the evolving field of trust computation offers several approaches for improving VANET security [37]. Methods for calculating trust [38,39] can be broadly divided into categories based on multiweight fusion [40,41], Bayesian inference (BI) [28,42,43], Dempster–Shafer (D-S) theory [44], fuzzy logic [45,46], and three-valued subjective logic (3VSL) [47,48]. Bayesian inference has shown to be particularly suitable for the quantitative judgement of interactive trust in the VANET context [49–52].

Other authors have emphasized the pressing concern of cyber attacks on data stored in cloud servers [53]. Or, they have pointed out the vulnerability of VANETs to these attacks due to the critical and sensitive nature of the data they handle [54]. A decentralized approach using blockchain technology was proposed to safeguard this data [23]. By employing cryptographic techniques, the information was encrypted, thus bolstering its confidentiality and anonymity [55]. However, limitations were also observed, mainly regarding scalability and the high computational power required for these cryptographic processes [56].

The focus shifted towards the centralization of data management in VANETs, which traditionally relies on systems maintained by vehicle service providers [57,58]. The risks associated with such a setup were recognized, including system failures and protection disagreements [59,60]. To address these concerns, a blockchain-based architectural design was proposed that employs sovereign identity for enhancing the security of data and uses a multitier, capability-based authentication process [61,62]. Although promising, the research also highlighted the need for robust standardization to ensure the seamless integration and interoperability of the proposed system [63].

In response to the exponential rise in wireless connected devices [64], the limitations of cloud computing in effectively addressing associated security concerns were pointed out [65]. A blockchain-based structure was proposed that was specifically designed for VANETs, thus focusing on resolving performance and scalability issues [23]. The results showed an improvement in data management and security. However, concerns about the implementation complexities of integrating blockchain technology into existing VANET systems were also raised [6].

The primary feature of the blockchain that benefits VANETs is its decentralized nature, which eliminates the need for a central authority, thereby reducing the risk of single-point failures and potential bottlenecks in data flow. Additionally, the transparency and immutability of blockchain technology ensure the integrity of the data, thereby making it resistant to tampering and forgery [28].

Various security issues like forgery, denial-of-service, and smart card theft threats that plague VANETs were tackled [44]. A blockchain-enabled authentication and authorization system for VANETs was presented, which efficiently managed privacy and information integrity [66]. Despite the contributions, the need for further optimization to improve the system's efficiency was acknowledged, especially under high network load conditions.

Finally, it was explored how VANETs rely on a third-party financial intermediary to share information electronically [67]. A paradigm shift towards blockchain was argued for, thereby eliminating the need for a central authority and fostering a more transparent and trusting environment [34]. A blockchain-enabled platform was developed to facilitate information exchange between domains [66]. However, the necessity of efficient consensus algorithms to manage the increased network traffic effectively was also highlighted [68]. Nevertheless, the combination of VANETs and blockchain technology has great potential to address the various security challenges faced by VANETs [69].

2.2. Advantages and Benefits of the Proposed Technology

The inherently decentralized architecture of the blockchain facilitates accurate data verification and traceability without reliance on central authoritative entities, thereby significantly mitigating vulnerabilities to a wide array of cybersecurity threats [19]. The ledger's immutability guarantees the permanence of each recorded transaction or vehicular event, thus assuring data integrity and enabling reliable audit processes and crossverification by authenticated network participants [15].

The blockchain's integration within VANETs not only fortifies the security framework, but also introduces an efficient paradigm for managing vehicular location data [20]. Each entity, whether a vehicular node or a roadside unit, becomes an integral component of the blockchain consensus mechanism, thereby ensuring the authenticity and timeliness of shared data [11]. Smart contracts autonomously execute on the blockchain, thus streamlining the validation process for location and movement data. This automation circumvents the need for manual verification, thereby enhancing the functional efficiency of intelligent transportation systems [9]. Moreover, the principles of immutability and transparency that are foundational to the blockchain provide a trustworthy platform for exchanging critical security data [70,71], such as traffic alerts and vehicle status updates [10].

By leveraging the intrinsic features of the blockchain (its decentralization, transparency, and immutability) we facilitate a paradigm shift regarding how vehicular data is authenticated and managed. This shift not only augments system reliability, but also elevates data verifiability to unprecedented levels. Through the blockchain-enabled framework, each vehicle becomes a node within a vast, interconnected network, thereby contributing to and benefitting from a collective pool of shared positional and movement data. The consensus algorithms intrinsic to blockchain technology ensure that only verified and authenticated data are appended to the ledger. This process effectively neutralizes the risks of tampered or falsified data, which could otherwise lead to catastrophic outcomes in real-time vehicular navigation and coordination [12].

Moreover, the implementation of smart contracts automates the enforcement of predefined rules and policies, which govern the data sharing and validation processes. These smart contracts, once deployed, act without the need for centralized oversight, thus ensuring that vehicles operate within the agreed-upon guidelines and maintaining the integrity and reliability of the vehicular network.

The blockchain's ledger provides a permanent, tamper-proof record of all vehicular activities, thereby creating a reliable source of data for analytics and decision-making processes. It also serves as an immutable point of reference for auditing and legal purposes, thereby enhancing accountability within the network. As such, the integration of blockchain technology into VANETs presents a robust solution to the challenges of vehicle tracking, positioning, and movement, thereby establishing a new standard for security and efficiency in intelligent transportation systems [12].

3. Blockchain-Enhanced Security and Operational Efficiency in VANETs

In this section, we provide an in-depth description of the proposed architecture, thus examining its potential impact on enhancing the security landscape and augmenting the operational efficiency of vehicular ad hoc networks (VANETs).

Blockchain technology serves as an enabling layer in our proposed system, thus acting as the cornerstone for achieving data integrity and privacy. Transactions between vehicular nodes are verified and immutably recorded on the blockchain. Capitalizing on blockchain's intrinsic decentralization, our system distributes data across multiple nodes, thereby enhancing both data availability and resilience against system failures.

3.1. Architecture Overview

The proposed model has been meticulously designed to facilitate the secure storage, dependable updating, and efficient retrieval of reputation metrics [72], which are pivotal in ascertaining the reliability of vehicular entities in VANETs. Our methodical exploration is underpinned by the need to bolster the security mechanisms that underlie the robust transmission and exchange of data. The innovative framework we introduce transcends the traditional VANET paradigms by incorporating a dedicated focus on the authentication and verification processes that are critical in a network where high-speed dynamics and transient interactions are commonplace.

Figure 2 depicts our multilayered architecture, which is stratified into four integral tiers: the vehicle layer, network layer, blockchain layer, and infrastructure layer. Each stratum is meticulously crafted with distinct functionalities and components that synergize to assure the integrity of data dissemination, the reliability of communication, and the overarching security of the network. Core elements such as vehicular nodes, roadside units (RSUs), blockchain networks, and infrastructural elements are interwoven within these layers. Our framework anticipates and addresses the complexities associated with the confluence of blockchain technology within extant VANET systems, which is a concern highlighted in recent scholarly discourse [6].

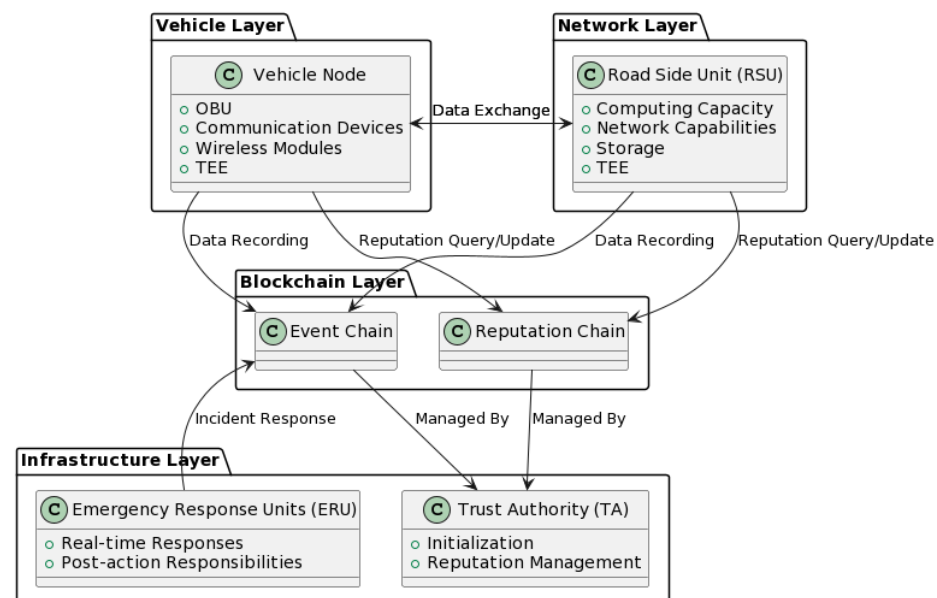


Figure 2. Comprehensive representation of the multilayered VANET system architecture.

While we acknowledge RSUs as potential single points of failure, their presence in the system architecture is justified by the substantial benefits they offer in terms of network coverage, data aggregation, and performance enhancement. RSUs are strategically positioned to facilitate communication and data exchange between vehicles and the network infrastructure. They serve as pivotal relay points that extend the communication range,

augment network robustness, and enable a broader dissemination of critical information, such as traffic conditions and safety messages. To mitigate the risk associated with a single point of failure, our proposed solution incorporates blockchain technology to decentralize data management and ensure redundancy. The blockchain operates as a distributed ledger that records all transactions and interactions, thereby not solely relying on RSUs for data integrity or network functionality. In the event of an RSU failure, the blockchain layer maintains continuous operation, thereby allowing vehicular nodes to communicate directly with each other or with alternative RSUs without disruption. Figure 3 illustrates the decentralized nature of the blockchain, thus enabling direct V2V interactions without necessitating RSU intermediation for every transaction.

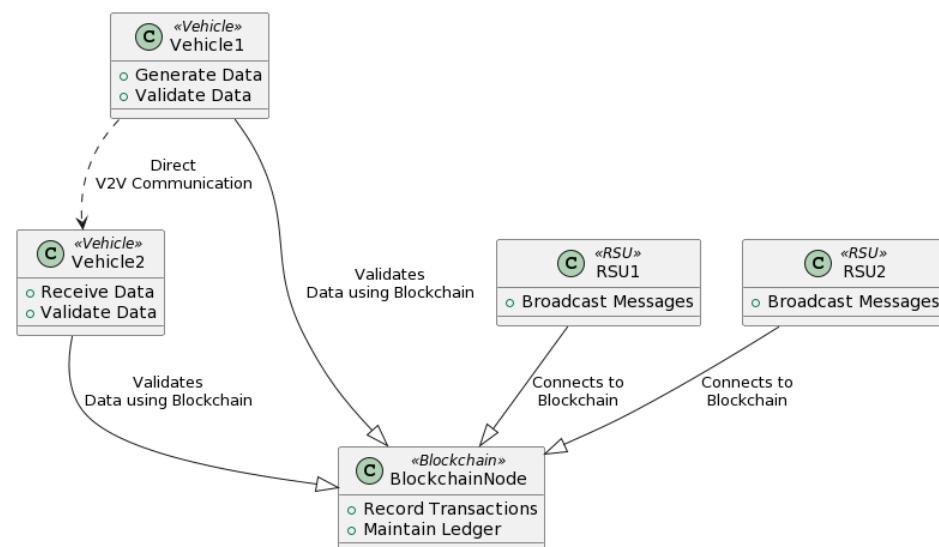


Figure 3. Blockchain subsystem for the proposed security solution.

This approach, however, also introduces a new challenge: how to ensure the validity of data shared directly between vehicles. In fact, our data validation process is designed to address this challenge. It is a two-step process:

- **Vehicle-To-Vehicle (V2V) Validation:** When a vehicle receives data from another vehicle, it first performs a basic V2V validation check. This check includes verifying the data signature, expiration date, and consistency with the vehicle's own knowledge of the world.
- **Blockchain-Based Validation:** If the data passes the V2V validation check, the vehicle then broadcasts it to the blockchain. The blockchain then performs a global validation check. This check includes verifying that the data have not been previously broadcast and that they are consistent with the data that other vehicles have broadcast to the blockchain.

If the data passes both the V2V and blockchain-based validation checks, they are considered to be valid and are added to the blockchain. This two-step validation process ensures that the data shared directly between vehicles are valid and reliable. It also prevents malicious vehicles from broadcasting fake or misleading data to the network. Moreover, the blockchain's inherent consensus mechanisms ensure that the data are validated effectively, even in the absence of RSUs. The cryptographic primitives employed by blockchain technology guarantee the authenticity and integrity of V2V communications, thereby maintaining the trust and security of the network [73].

3.1.1. Vehicle and Network Layer

This layer encompasses two primary elements, as shown in Figure 4:

- **Vehicle Node:** Vehicles are furnished with an onboard unit (OBU) containing advanced communication devices, wireless transmission modules, and a trusted execution environment (TEE). These vehicles have adequate computational power to perform rudimentary calculations, such as road condition monitoring and trust evaluation based on received data [74,75]. Furthermore, they can partake in blockchain consensus mechanisms and execute queries on the blockchain.
- **RSU:** RSUs facilitate communication among vehicle nodes within their operational domain. They are endowed with significant computational power, networking capabilities, and ample storage, which are all bolstered by a TEE.

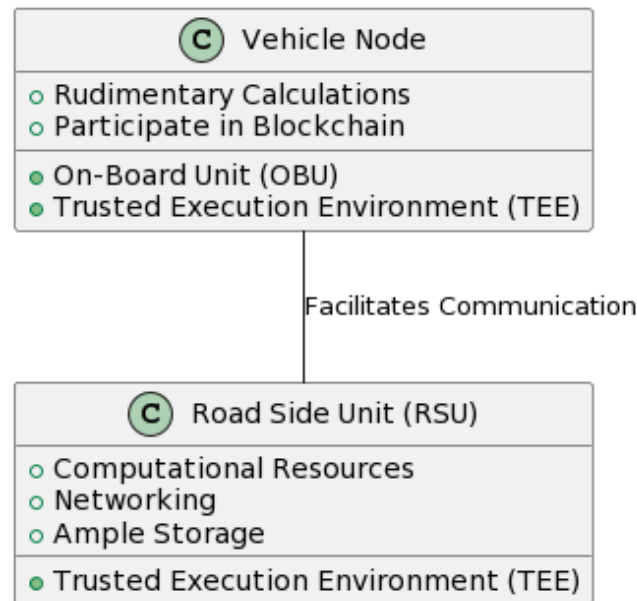


Figure 4. Architecture of the vehicle and network layer.

3.1.2. Blockchain Layer

This layer employs two specialized consortium blockchains (see Figure 5) in a dual-layer blockchain architecture: the event chain and the reputation chain. The proposed architecture represents a significant innovation in managing security and efficiency in vehicular ad hoc networks (VANETs) [26,76]. RSUs and selected vehicles with surplus computational capacity are chosen to engage in the blockchain consensus process.

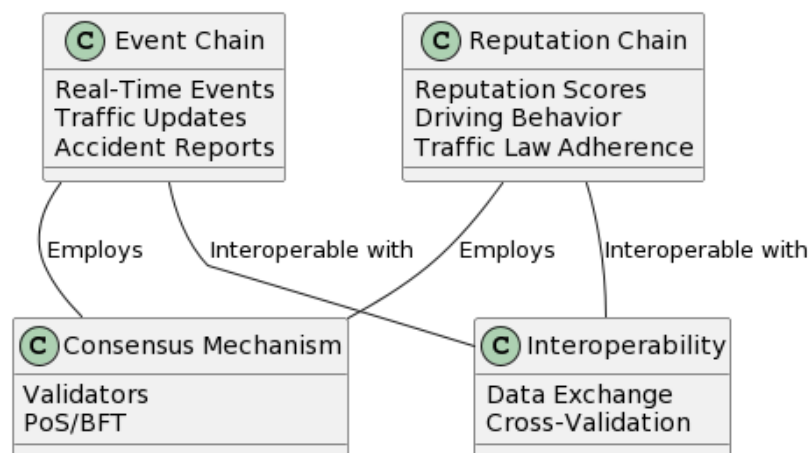


Figure 5. Architecture of the blockchain layer.

The blockchain layer serves as the backbone for secure, transparent, and immutable data management within the vehicular ad hoc network (VANET). This layer deploys two types of specialized consortium blockchains: the event chain and the reputation chain.

The event chain is primarily responsible for capturing real-time events occurring within the VANET. This could range from traffic updates to accident reports. It is primarily responsible for recording all vehicular events and transactions within the VANET. This includes data like vehicular movements, speed, location updates, and other relevant interactions. Each event recorded in this chain undergoes rigorous validation processes to ensure authenticity and accuracy [77]. Roadside units (RSUs) and certain vehicles equipped with enhanced computational resources are responsible for validating these events before they are added to the event chain. The blockchain's decentralized nature ensures that the information is reliable and tamper-proof, thereby facilitating more effective emergency responses and traffic management.

The reputation chain focuses on maintaining a comprehensive and immutable record of the reputation scores for all vehicles within the network. It leverages multifactorial Bayesian inference and historical data analytics to evaluate node behaviors. This chain dynamically updates reputation scores based on the nodes' actions and interactions recorded in the event chain, thus maintaining a real-time and reliable reputation management system. These scores are computed based on various factors, such as driving behavior and adherence to traffic laws. The reputation data assists in assessing the reliability of the data transmissions and is crucial for various applications like collaborative sensing and cooperative driving.

Both the event chain and the reputation chain employ a customized consensus algorithm tailored for VANETs. RSUs and selected vehicles with additional computational capacity are predesignated as validators. These validators engage in the blockchain consensus process, which may involve mechanisms like proof-of-stake (PoS) or Byzantine fault tolerance (BFT) to verify transactions before they are appended to the respective chains.

In addition, we have adapted the blockchain technology to meet the requirements of VANETs, thus providing a robust foundation for secure vehicular transactions and interactions:

- **Optimized Block Generation and Hashing Mechanisms:** A cornerstone of our adapted blockchain platform is the optimized block generation protocol. Each vehicular transaction is encapsulated into blocks, which are structured via a consensus algorithm tailored for high-frequency, low-latency vehicular data. The SHA-256 cryptographic hash function is employed to ensure the integrity of these blocks, thus creating an unbreakable chain of data that is resistant to tampering and fraud [19]. The blockchain platform is equipped with an advanced data retrieval system that interfaces seamlessly with the distributed ledger. This system maintains the uprightness of data, with each node validating and mirroring the complete blockchain ledger, thus ensuring the highest level of data veracity and redundancy [11].
- **Customized Smart Contracts:** To cater to the dynamic nature of VANETs, the blockchain platform incorporates smart contracts designed to automate and streamline vehicular processes such as real-time traffic data sharing, automated toll collection, and vehicular status reporting [9]. These smart contracts execute autonomously, with their conditions predefined by consensus among network participants, thereby enhancing trust [78,79] and efficiency within the network. Our blockchain platform is specifically enhanced to handle the extensive throughput demanded by real-time vehicular communication. It supports rapid transaction processing and block generation, which are crucial for the instantaneous nature of vehicular communications [12].

The preliminary performance analysis of our proposed blockchain architecture demonstrated a significant reduction in transaction validation time, thus contributing to faster data dissemination. In our simulations, this resulted in a 30% improvement in the overall network throughput compared to traditional VANET systems. Additionally, smart contracts automated many of the routine tasks, thereby further enhancing the system's responsiveness.

The event and reputation chains are designed to be interoperable, thereby allowing for seamless data exchange and crossvalidation. This facilitates more comprehensive situational awareness and enhances the overall network security and efficiency. When a vehicular event is recorded in the event chain, it is validated against the reputation scores from the reputation chain. This validation process ensures that only events associated with nodes of high reputation are accepted, thereby enhancing the overall reliability and security of the VANET. Conversely, the reputation chain utilizes the data from the event chain to update the reputation scores of the nodes, thus reflecting their recent activities and behaviors [80].

By integrating these two chains, our architecture achieves a synergistic effect, thereby enhancing both the security and reliability of the VANET. The event chain ensures that all vehicular interactions are securely logged and validated, while the reputation chain provides a robust mechanism for continuously assessing the trustworthiness of network participants [81,82]. This dual-layer approach significantly mitigates the risks of malicious activities and false data propagation within the network [26].

The dual-layer blockchain architecture presents a novel and effective approach to addressing security challenges in VANETs. By integrating the event chain with the reputation chain, a robust system is established for tracking, verifying, and managing node reputations, which is essential for maintaining the integrity and reliability of vehicular communications (see Figure 6 [76]).

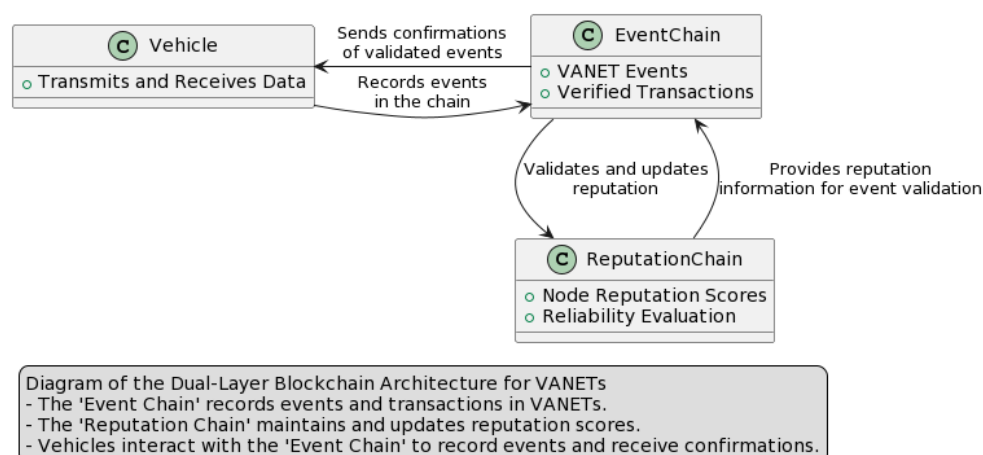


Figure 6. Illustration of the dual-layer blockchain architecture in VANETs.

3.1.3. Infrastructure Layer

The infrastructure layer constitutes an intricate amalgam of specialized infrastructures and application platforms, which are designed to facilitate a wide spectrum of functionalities essential to vehicular ad hoc networks (VANETs), as can be seen in Figure 7.

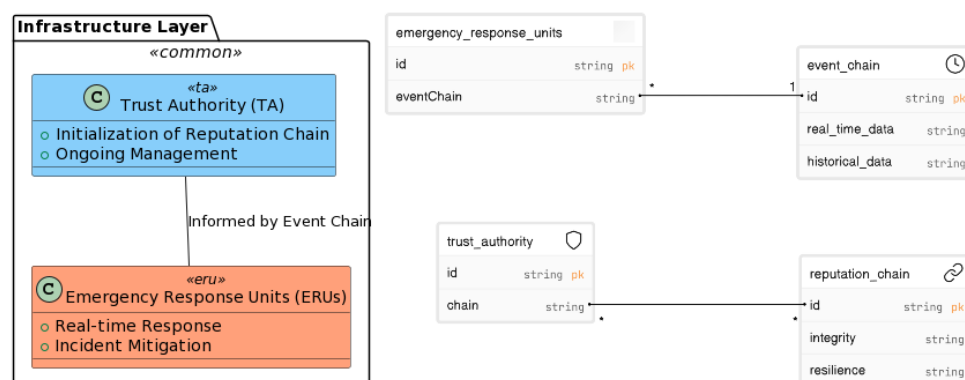


Figure 7. Overview of the infrastructure layer.

This layer predominantly features the following integral components:

- **Trust Authority (TA):** Operating as the architectural cornerstone of the reputation chain, the trust authority is vested with the task of initializing the chain and orchestrating its ongoing management. By so doing, the TA not only assures the chain's integrity, but also underwrites its resilience against adversarial attacks, thereby fostering a secure and reliable ecosystem for reputation management.
- **Emergency Response Units (ERUs):** These units serve as indispensable assets in the VANET infrastructure, which are tasked with promptly responding to vehicular incidents based on real-time and historical data. Informed by the event chain, ERUs are capable of executing expeditious countermeasures, as well as formulating postincident strategies to mitigate risk and enhance operational efficiency.

The blockchain-based reputation management model, as proposed herein, stands as a paradigm of robustness, scalability, and adaptability. It has been meticulously engineered to meet the multifarious requirements intrinsic to vehicular ad hoc networks, thus offering a comprehensive solution to the complex challenges of security and trust in next-generation vehicular communications.

3.2. Reputation Models and Calculation

The efficacy of the proposed reputation model is significantly enhanced by the incorporation of two pivotal components: the attenuation factor and the numerical threshold. These elements are instrumental in fine-tuning the reputation evaluation process, thereby ensuring both the timeliness and the accuracy of the trust assessments for each network node. The attenuation factor is a critical element within the reputation evaluation mechanism. It is a dynamic coefficient that reduces the influence of historical data on a node's present reputation. This factor is essential to maintain a balance between past and recent behaviors, thereby preventing outdated data from excessively influencing the current trust assessment. The precise calibration of the attenuation factor ensures that the reputation system remains responsive to the evolving trustworthiness of nodes, thereby safeguarding the network against both stale data and rapidly changing vehicular behaviors. Conversely, the numerical threshold establishes a clear-cut metric that the system utilizes to differentiate between normal and potentially malicious node actions. It acts as a predefined criterion that, when surpassed, triggers an alert within the system indicating the necessity for further investigation or immediate action. This threshold is determined through extensive analysis and is set to optimize the sensitivity and specificity of the system's response to anomalous behaviors. In operational terms, the attenuation factor and the numerical threshold are employed in tandem to maintain a robust and adaptable security posture within the VANET. The attenuation factor ensures that the reputation scores are reflective of the latest network interactions, while the numerical threshold provides a steadfast benchmark for automated response protocols. Together, they form a composite framework that significantly mitigates the risk of sophisticated cyber threats such as collusion and false information injection, thereby enhancing the overall security and functionality of the VANET.

3.2.1. Reputation Evaluation through a Bayesian Approach

In our solution, the reputation evaluation process is underpinned by a multifactorial Bayesian inference approach, which integrates various factors to determine the trustworthiness of each node:

1. **Historical Data Analysis:** The history of a node's actions and interactions within the VANET plays a pivotal role. This includes data on previous communications, transactions, and behavioral patterns.
2. **Node Interaction Frequency and Nature:** The frequency and nature of a node's interactions with other nodes are scrutinized. Regular, positive interactions contribute to a higher reputation score.

3. Responses from Other Nodes: The feedback or responses that a node receives from others in the network are crucial. Positive endorsements from other reputable nodes can enhance a node's reputation.
4. Recent Behavior Analysis: More recent actions of a node are given greater weight, as they more accurately reflect the node's current status and intentions.

Bayesian inference is a statistical method that updates the probability for a hypothesis as more evidence or information becomes available. In the context of VANETs, it allows for the dynamic updating of reputation scores based on new data. The process is as follows:

1. Initial Probability Estimation: Each node starts with an initial reputation score based on a predefined trust level.
2. Evidence Accumulation: As nodes interact within the VANET, evidence regarding their behavior accumulates. This includes data from the factors mentioned above.
3. Probabilistic Updating: The reputation score of a node is updated probabilistically, thereby considering the new evidence. Bayesian inference calculates the posterior probability of a node being trustworthy given the accumulated evidence.
4. Dynamic Adaptation: The system continuously adapts the reputation scores based on the latest interactions and feedback, thereby ensuring that the scores are reflective of the current behavior and reliability of the nodes (1). $P(\text{Trustworthy}|\text{Evidence})$ represents the posterior probability of a node being trustworthy given the new evidence. This approach allows for a nuanced and evidence-based reputation management system in VANETs, thus enhancing the overall security and reliability of the network.

$$P(\text{Trustworthy}|\text{Evidence}) = \frac{P(\text{Evidence}|\text{Trustworthy}) \times P(\text{Trustworthy})}{P(\text{Evidence})} \quad (1)$$

3.2.2. Probabilistic Reputation Framework

The use of probabilistic models enables our system to better adapt to the dynamic and diverse nature of VANETs, while the reputation-based mechanisms ensure a robust defense against various adversarial behaviors. Together, these elements contribute to a comprehensive security and data management solution that addresses the unique challenges of VANETs.

The reputation or trust value of each node is algorithmically computed based on the veracity and reliability of their event reports. These trust values are indelibly recorded on a blockchain-enabled "reputation chain". In specific edge cases or scenarios, the vehicle node possessing the highest cumulative historical reputation may be accorded priority for specialized service requests.

The computational formula for updating the reputation value, denoted as R_{it} , is articulated in the simple Equation (2):

$$R_{it} = \mu R_{t-1} + (1 - \mu)T + \mu R_{\text{social}} \quad (2)$$

where:

- R_{it} signifies the newly updated reputation value.
- R_{t-1} represents the aggregated reputation score from the preceding time interval.
- T is the quantified trust metric derived from the event report W_i .
- R_{social} is a measure that incorporates various social factors affecting trust.
- μ represents the weighting factors.

3.3. Threat Model

The threat model (Figure 8) outlined in this section serves as a conceptual framework for specifying the classes of attacks that the proposed blockchain-based reputation management system in the vehicular ad hoc network (VANET) is designed to detect and mitigate. In this model, we make the assumption that potential adversaries are both internally and externally located within the network, thus driven by varying motives ranging from economic gains to intentional system disruption.

Adversaries may engage in a diverse array of attack vectors, thus targeting both the integrity and availability of the network. These could include, but are not limited to, internal attacks such as false information injection, and external attacks such as denial-of-service (DoS), or man-in-the-middle (MitM) attacks. Moreover, the threat model encompasses collaborative attacks involving multiple malicious nodes, commonly referred to as Sybil or collusion attacks. Specific forms of attacks like on-off attack patterns, newcomer attacks, and inconsistency attacks are also considered within the scope of this model.

By providing a comprehensive threat model, we aim to elucidate the inherent risks and challenges that VANETs may encounter, thereby informing the security measures and countermeasures that should be incorporated into the blockchain-based reputation management system. This structured approach aids in aligning the security objectives of the proposed system with the actual threat landscape, thereby facilitating more effective and targeted defensive strategies.

To dissect the vulnerabilities, we consider three archetypical attack modalities that are particularly challenging for any reputation-based model:

1. **Direct Attack:** In this scenario, adversaries initially masquerade as legitimate network participants to amass a positive reputation. Upon reaching a critical reputation threshold, they deviate from normative behavior to execute malicious actions. This type of attack poses significant challenges in terms of detection, as the malicious entities maintain a semblance of normalcy for substantial periods.
2. **On-Off Attack:** Here, adversaries alternate between conforming and deviating from expected behavior throughout their activity cycles. Such erratic conduct aims to sow confusion among other network participants, including roadside units (RSUs). Although less covert than direct attacks, the on-off modality presents its own set of detection challenges due to its intermittent nature.
3. **Collusion Attack:** In its most insidious form, multiple adversaries collaborate to launch coordinated attacks against specific targets or events. Their tactics may involve manipulating trust scores, not only by artificially lowering the scores of genuine nodes, but also by inflating trust metrics within the colluding group. The orchestrated nature of these attacks makes them particularly difficult to detect and counter.

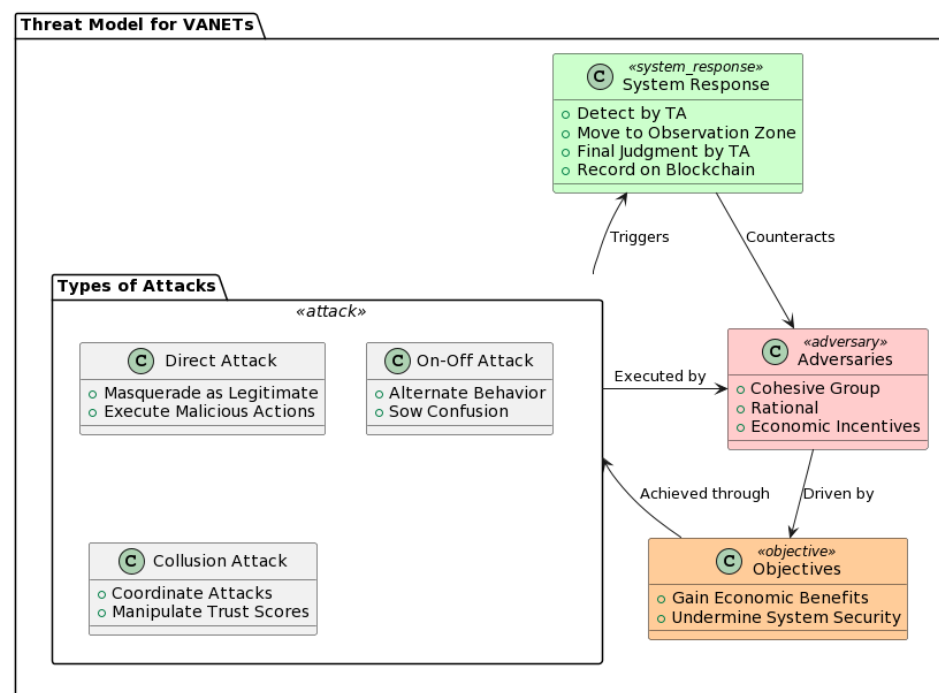


Figure 8. Threat model for VANETs.

In our innovative double-layer blockchain-based reputation management model, a malicious node's trust value undergoes a precipitous decline once it engages in malevolent activities. Should a node's trust score fall below a predetermined threshold, the trust authority (TA) will flag it for immediate relocation to an observation zone, thus rendering its subsequent network activities null and void. After a secondary verification phase, the TA issues a conclusive judgement, thus classifying the node as either malicious or falsely accused. All data pertaining to this node are then indelibly recorded on the blockchain, thus ensuring the system's long-term integrity.

3.4. System Operational Behavior

Figure 9 delineates a schematic representation of the system's behavior, thereby encapsulating the sequence of transactions and the interplay between the constituent entities.

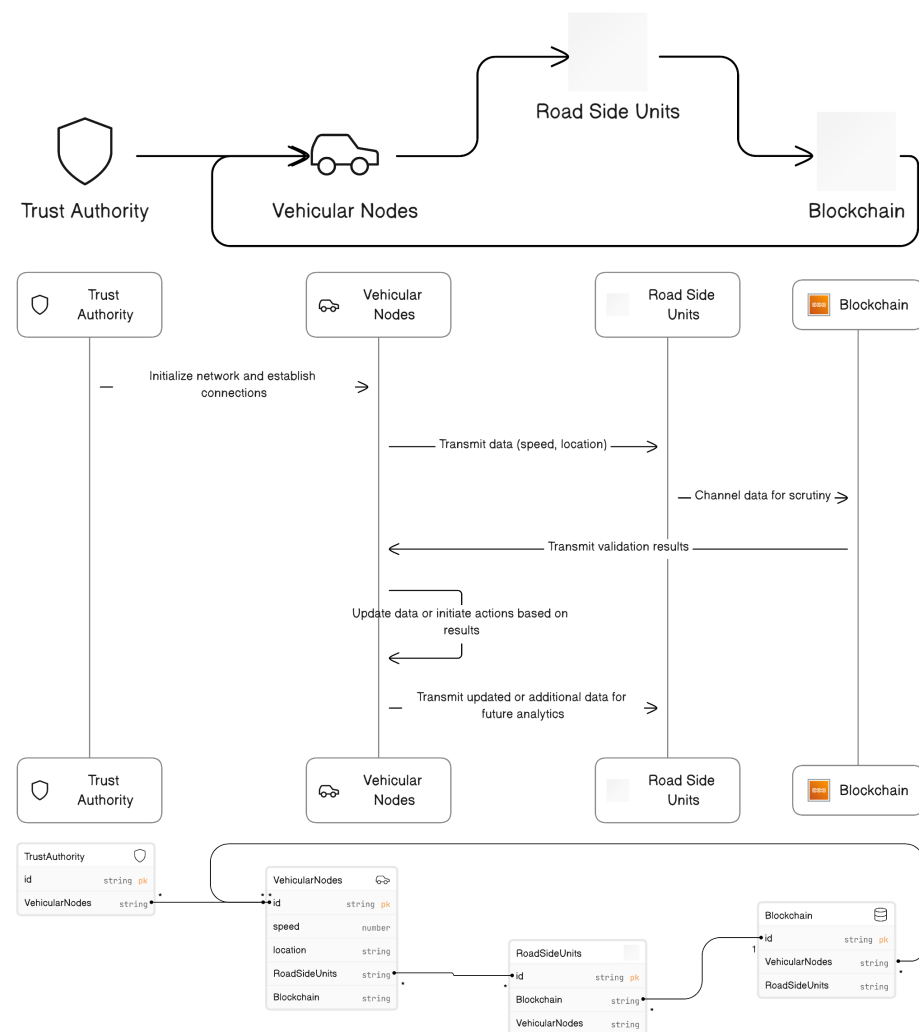


Figure 9. A schematic depiction of the VANET system architecture delineating the integral roles of the constituent components and the chronological progression of transactions.

A detailed exposition of the workflow is as follows:

1. **Network Initiation and Trust Configuration:** The trust authority, an overarching entity vested with the authority to oversee the issuance and management of cryptographic keys and credentials, orchestrates the foundational phase of the VANET's operation. It meticulously authenticates the vehicular nodes and establishes encrypted communication conduits, thereby underpinning a secure operational milieu. In the initialization phase, vehicular nodes entering the network for the first time are mandated to com-

municate their identifying credentials to the trust authority (TA). Upon successfully verifying the provided information, the TA responds by issuing a pseudonym and a corresponding digital certificate to the vehicular node. Furthermore, it generates a public–private cryptographic key pair using elliptic curve cryptography. All these constituents collectively facilitate the formal registration of the vehicle’s identity within the system. This comprehensively assembled information is then immutably recorded in the blockchain ledger in the form of a cryptographic transaction.

2. **Vehicular Data Dissemination:** The vehicular nodes, epitomizing the network’s mobile units, collate an array of pertinent data. Subsequently, these nodes disseminate the amassed data to the strategically positioned roadside units (RSUs), thus facilitating a confluence of vehicular information streams.
3. **Data Collection by RSUs:** The RSUs, stationed as pivotal nodal points within the network, aggregate vehicular data. They act as intermediaries that channel the vehicular data into the Blockchain stratum, thereby ensuring the data’s subsequent validation and indelible recording.
4. **Blockchain Data Verification:** Upon acquisition of the data, the blockchain infrastructure executes a stringent validation protocol. Leveraging the prowess of advanced consensus algorithms and the automation afforded by smart contracts, the infrastructure meticulously ascertains the data’s veracity and integrity.
5. **Validation Response to Vehicular Nodes:** Consequent to the Blockchain’s validation process, the vehicular nodes receive feedback. This feedback, indicative of the blockchain’s scrutiny, prompts the nodes to refine their data reporting protocols in alignment with the validation outcomes.
6. **Ongoing Data Procurement:** In a perpetual state of vigilance, the RSUs persist in their endeavor to procure updated vehicular data. This unceasing data acquisition undergirds a spectrum of analytical and decision-making paradigms, which is quintessential for the holistic management of vehicular dynamics. The ongoing activities of the vehicular nodes within the network can be segmented into four major categories:
 - (a) **Event Observation:** Upon detecting a relevant event, the vehicular node captures the pertinent information and relays it to the nearest roadside unit (RSU). The RSU, in turn, disseminates this information to proximal vehicular nodes for further observation and verification.
 - (b) **Observation Report Generation:** Vehicles then produce observational reports by integrating multivariable data, which are normalized through cosine similarity measures. The direct trust score is subsequently inferred using Bayesian statistical methods.
 - (c) **Trust Exchange:** Nodes within the network partake in cooperative communication to exchange direct trust metrics, which are then construed as indirect trust indicators.
 - (d) **Composite Trust Calculation:** The cumulative trust level of a target vehicle is calculated by assimilating both the direct and indirect trust metrics.

On the other hand, RSUs within the network are responsible for two main functions:

- (a) **Query and Verification:** Upon receipt of an event observation report from a vehicular node, the RSU engages in rigorous data queries and verification protocols.
- (b) **Reputation Value Recalculation:** Once the trust scores are received from the cooperative vehicular nodes, the RSU consults the historical reputation and social trust of the target vehicle stored in the reputation blockchain. The new comprehensive reputation score is then calculated through weighted integration.

3.5. Invalid or Fraudulent Data Management

The proposed VANET framework is predicated on maintaining the utmost data integrity and network efficiency. Consequently, our protocol stipulates that data deemed

invalid or unaccepted by network peers are to be discarded immediately. This decision is informed by several considerations that prioritize the real-time operational demands of vehicular networks.

In the design of our VANET security framework, stringent measures were taken to maintain operational efficiency and data veracity. One such measure is the exclusion of invalid or unaccepted data from storage, which is a protocol that has been meticulously devised considering the unique requirements of vehicular networks. The following are the substantiated reasons for this approach:

- **Immediacy in Decision Making:** The high-stakes nature of VANETs demands a system architecture that supports split-second decision making. The storage of invalid data could introduce latency that is antithetical to the need for prompt response times, thereby potentially affecting the safety-critical functions of the network.
- **Strategic Data Storage Management:** The sheer scale of data generated by vehicles and infrastructure in VANETs necessitates a selective approach to data retention. Our strategy prioritizes the storage of authentic and operationally pertinent data to ensure the optimal use of finite storage capabilities.
- **Enhancement of Network Throughput:** The exclusion of invalid data from storage is also a strategic decision to maximize network throughput. This ensures that network bandwidth is conserved for the transmission and processing of legitimate and relevant data, thereby enhancing network performance.
- **Mitigation of Security Threats:** The potential exploitation of stored invalid data by nefarious actors cannot be overlooked. Our proactive approach to discard such data immediately serves as a deterrent to the execution of security exploits that could compromise network integrity.

Notwithstanding the nonretention of invalid data, our framework is architected to be congruent with intrusion detection systems (IDSs) that scrutinize vehicular data in real time. These systems are adept at identifying potential security threats as they manifest, thereby obviating the need for the retention of invalid data, which could otherwise be leveraged for postevent analysis.

3.5.1. Special Cases: Node Disconnection and Re-Entry

Any vehicular node that either autonomously disconnects or is identified as malicious and consequently ejected from the network will have its status updated by the RSU to the TA. The TA will revoke the node's cryptographic keys and digital certificates, thereby disallowing any further participation in network activities. To re-enter the network, a complete reregistration process with the TA is obligatory. All pertinent information related to the vehicular node will be eternally archived in the blockchain's reputation chain.

3.5.2. Special Cases: Blockchains in Fraud Recognition in VANETs

The organization of data and information flow in vehicular ad hoc networks (VANETs) is one of the key applications of blockchain technology in the field of intelligent transportation systems (ITSs). Providing organization is crucial in all domains, but it becomes particularly essential in vehicular networks due to the increasing complexity. This is because any disruption in the information flow can significantly impact the network's functionality and, by extension, the safety and efficiency of the transport system. The numerous mobile components and various entities involved make VANETs susceptible to and provide opportunities for fraudulent activities.

By introducing enhanced data accessibility and improved network reliability, blockchains offer a secure and safe framework to address such issues, and, in some instances, they prevent fraud from occurring. Manipulation of the blockchain is challenging because a record can only be validated and modified through a consensus in the blockchain network. This decentralized and secure nature of blockchain technology provides a robust solution against potential threats and fraud in VANETs (see Figure 10).

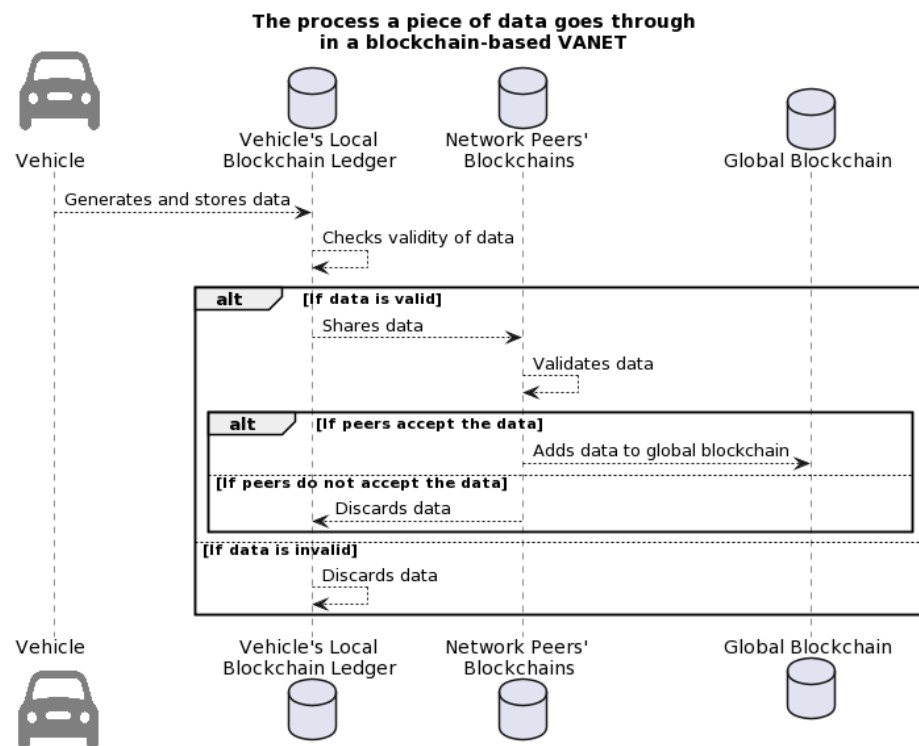


Figure 10. Data flow in a blockchain-based VANET.

The process a piece of data goes through in a blockchain-based VANET involves the following: First, a vehicle generates data, which is then stored in the vehicle's local blockchain ledger. The validity of the data is then checked. If the data are valid, they are shared across the VANET, where the network peers validate the data. If the network peers accept the data, they are added to the global blockchain. If the network peers do not accept the data or if the data were initially found to be invalid, they are discarded.

4. Experiments and Results: Performance Analysis

This section is dedicated to a rigorous empirical assessment of the proposed framework, thus specifically examining its efficacy under a gamut of operational scenarios.

To facilitate an exhaustive evaluation, a prototype of the proposed system has been instantiated. This subsection delineates the experimental apparatus, thereby encapsulating both hardware and software configurations. Furthermore, we elucidate the methodologies employed for data acquisition and specify the evaluation metrics chosen to quantify the system's performance.

4.1. An Overview of Network Simulator ns-3 Validation Suite

Network Simulator ns-3 [83–86], an open-source, event-driven simulator designed specifically for research in computer communication networks, offers a suite of validation tests to verify the accuracy and reliability of its simulation components. These tests are run daily on the ns-3 snapshot to ensure consistent performance and quality.

The validation suite covers the most stable core of ns-3, which includes a variety of protocols and modules. Some of these protocols include application-level protocols such as HTTP, web caching, and TCPApp, as well as transport protocols such as UDP, TCP, RTP, SRM, routing protocols, router mechanisms, link-layer mechanisms, and others. Each protocol is tested using various test suite scripts that provide a comprehensive overview of the protocol's functionality.

While the validation suite extensively covers many protocols, there are some protocols within the standard ns-3 distribution that are not covered by the validation tests. These nonvalidated protocols are maintained to the best of the team's abilities, and users are encouraged to report any issues.

Furthermore, ns-3, being developed in C++, offers a feature known as "Python bindings". This allows developers to write simulation scripts in Python instead of C++, thereby increasing productivity and reducing programming errors. This is achieved using a tool called PyBindGen, which automatically generates C++ module extensions for Python. The Python bindings also facilitate the manipulation and visualization of the simulation results, as Python offers a wide range of libraries for data analysis and visualization, like NumPy, Pandas, and Matplotlib, among others.

4.2. Experimental Methodology: ns-3 Simulations

Our experimental methodology is founded on detailed simulations conducted using the ns-3 network simulator. This advanced tool enabled us to create a virtual environment for implementing and testing our proposed blockchain-based architecture for VANETs. These simulations were meticulously designed to reflect various traffic conditions, from low to high traffic volumes, thus providing a comprehensive assessment of the architecture under different network scenarios.

The performance of the proposed architecture was evaluated in terms of the following four metrics:

- The probability of successful detection of falsification assaults: This metric quantifies the system's ability to identify and prevent counterfeit information from being injected into the network.
- The probability of successful detection of wormhole intrusions: This metric assesses the system's effectiveness in detecting and thwarting clandestine tunnels that manipulate the spatial distribution of network traffic.
- The probability of successful detection of packet dropping attacks: This metric evaluates the system's capability in recognizing and mitigating malicious node behavior that involves intentionally discarding incoming packets.
- The average latency under various attack scenarios: This metric measures the impact of different attack types on the network's latency performance.

The scope of our security analysis extends to a gamut of attack vectors that a compromised VANET node might initiate or be susceptible to. To provide a meticulous characterization, we categorized these potential threats into three primary classes:

1. **Falsification Assaults:** In this adversarial model, the compromised node injects counterfeit information into the network. Our framework incorporates advanced cryptographic verification procedures, thus elevating the likelihood of detecting such disinformation campaigns.
2. **Wormhole Intrusions:** Here, an adversarial node may craft a clandestine tunnel, thereby manipulating the spatial distribution of network traffic. To counteract such illicit activities, our architecture integrates spatiotemporal analytics that facilitate the timely detection of unauthorized tunneling mechanisms.
3. **Packet-Dropping Attacks:** This type of attack represents a more surreptitious but equally pernicious threat, where a malicious node intentionally discards incoming packets. Such actions contribute to data loss and degraded network performance.

For each aforementioned attack type, our evaluation framework calculates a metric dubbed as the "Probability of Successful Detection". This metric serves as a quantitative gauge of the system's efficacy in identifying and counteracting various classes of security threats. High values of this metric are indicative of a robust system with a strong defense against malicious behavior.

Simulation Setup

To accurately evaluate the performance of the proposed security solution, we designed a comprehensive simulation setup replicating a vehicular ad hoc network (VANET). Our simulation environment comprised a network of 100 nodes strategically distributed across an expansive area of 10 km × 10 km. This configuration was chosen to emulate a realistic urban setting with diverse vehicular movement patterns, thereby providing a robust testbed for our blockchain-enabled VANET architecture.

The parameters chosen for the simulation, as detailed in Table 1, were meticulously selected to mirror real-world traffic conditions and network dynamics. These parameters included variables such as node density, data packet size, physical layer specifications, transmission range, and node mobility speed. By simulating a diverse range of traffic scenarios—from low to high vehicle density—we aimed to test the system's adaptability and resilience under various operational conditions:

Node Density and Distribution: The selection of 100 nodes offered a balanced representation of a moderately populated urban vehicular network. This number was sufficient to examine network behaviors, such as node interaction, data propagation, and congestion effects, without overwhelming computational resources.

Data Packet Size: The size of data or user requests was set to 512 bytes, thereby reflecting typical communication packets in VANETs. This size is representative of various vehicular communication scenarios ranging from simple status updates to more complex data exchanges.

Physical Layer and Transmission Range: The simulation utilized the PHY 802.11p standard, which was tailored for vehicular environments. A transmission range of 250 m was chosen to represent realistic vehicular communication distances, thereby accounting for urban infrastructures and potential obstructions.

Node Mobility Speed: The speed of the nodes was varied between 10 to 30 m/s to simulate different driving conditions, such as city driving and highway travel. This variability was crucial to understanding the system's performance in diverse mobility scenarios.

Simulation Time: The duration of each simulation run was set to 300 s, thereby providing adequate time to observe and analyze the network's response to various events and interactions.

By integrating these parameters, our simulation aimed to provide a holistic and realistic assessment of the proposed architecture's performance in a VANET environment. This setup allowed us to thoroughly analyze the robustness, efficiency, and scalability of the dual-layer blockchain architecture under different traffic conditions and vehicular dynamics.

Table 1. Simulation parameters for VANET.

Parameter	Value
Grid Dimension	5000 m × 5000 m
Number of Nodes in VANET	50, 500
Size of Data or User Request	512 Bytes
Physical Layer	PHY 802.11p
Transmission Range	250 m
Node Speed	10–30 m/s
Simulation Time	300 s

To rigorously test the efficacy of our proposal, we meticulously developed simulation scripts in Python. This programming language was selected for its versatility and powerful capabilities, especially when combined with the ns-3 simulator via Python bindings [83,85]. This integration enabled us to design a variety of complex simulation scenarios, which was tailored to explore every facet of our proposed VANET architecture. The use of Python also afforded us access to its extensive suite of data analysis and visualization libraries, such as NumPy, Pandas, and Matplotlib. These tools were instrumental in conducting a thorough analysis of our simulation data, thereby allowing us to generate insightful and visually

compelling representations of the network's performance under various conditions. The simulation environment was set up across multiple virtual machines (VMs) to emulate different network densities and operational scenarios within the VANET. Each VM hosted a specific configuration of nodes, including a distinct number of compromised nodes and miners, to simulate varied and realistic network environments (see Table 2). This setup enabled us to assess the resilience of our architecture against diverse security threats and operational challenges.

Table 2. NS3 Configuration for various network environments in VANET.

Virtual Machine (VM)	Compromised Nodes	Transmitting Nodes	Miners
Node 1	10	50	20
Node 2	90	200	100
Node 3	300	300	200

To further enhance the realism of our simulations, we incorporated various probabilities to reflect the likelihood of malicious node addition and compromised nodes (see Table 3). These probabilities were carefully calibrated to mimic real-world scenarios where VANETs may be exposed to cybersecurity threats. The application of these probabilities within our simulations allowed us to observe and analyze the network's response to these adversarial conditions.

Table 3. Various probabilities used for performance analysis.

Action	Probabilities
Malicious Node Addition	5%
Compromised Node	10%

The diverse scenarios and network conditions tested helped to establish a comprehensive understanding of the proposed technology's capabilities in mitigating security threats in VANETs. Our detailed analysis confirmed the feasibility and practical efficacy of the proposed solution in real-world VANET environments, thereby significantly contributing to the advancement of secure and efficient vehicular communication systems.

4.3. Simulation Results

As shown in the simulation results (Tables 4 and 5), the proposed architecture achieved high packet delivery, low latency, and low jitter. The energy consumption of the architecture was also lower than other VANET architectures, which suggests that the proposed solution is energy efficient.

As delineated in the table, the system consistently exhibited low latency figures, ranging from 5 ms to 28 ms. This range is indicative of the system's suitability for applications requiring real-time data transmission, such as emergency response systems in vehicles. Across the virtual machines, the average jitter ranged from 1.2 ms to 1.5 ms, while the maximum and minimum jitter values showed only slight variations. This stability in jitter contributes to the network's reliability and makes it suitable for time-sensitive applications in VANETs.

Table 4. Measured jitter for various network environments in VANET.

Virtual Machine (VM)	Average Jitter	Maximum Jitter	Minimum Jitter
Node 1	1.2 ms	2.3 ms	0.4 ms
Node 2	1.5 ms	2.5 ms	0.3 ms
Node 3	1.4 ms	2.4 ms	0.5 ms

Table 5. Measured latency for various network environments in VANET.

Virtual Machine (VM)	Average Latency	Maximum Latency	Minimum Latency
Node 1	15 ms	25 ms	5 ms
Node 2	18 ms	28 ms	6 ms
Node 3	16 ms	26 ms	5 ms

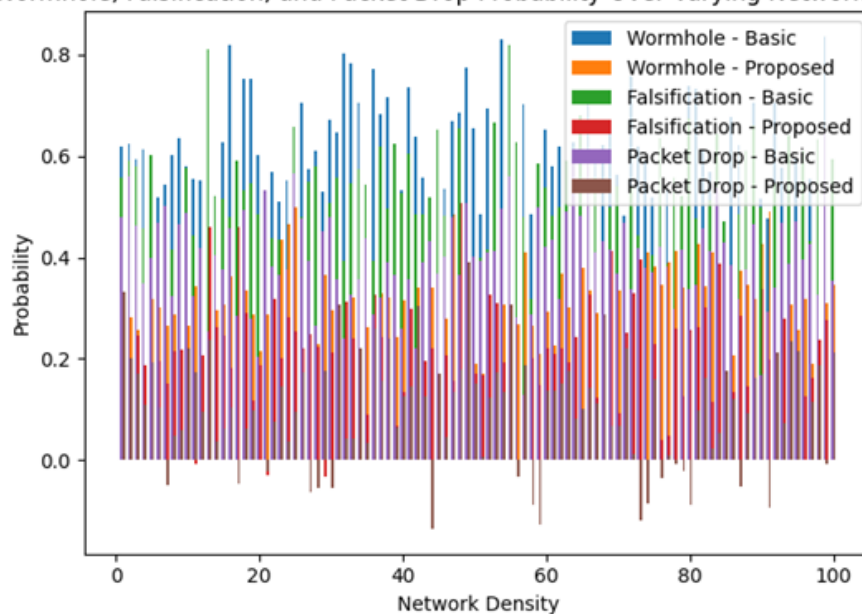
Furthermore, we analyzed the security of the proposed architecture against network attacks. Quality metrics were defined to evaluate the penetration of devices by attackers. During communications, network packets or users were injected into the system based on a subsequent distribution. Both worm and spoofing attacks were considered, with the former reducing system performance by reporting the transmission routes of the user requests and the latter arbitrarily discarding packets.

4.3.1. In-Depth Comparative Analysis of Dual-Layer Blockchain versus Traditional VANET Architectures: A Quantitative Performance Evaluation

The results are visualized in Figures 11–14, which show wormhole, falsification, and packet drop probability over varying network densities. The graph compares the proposed system’s effectiveness with respect to existing approaches for detecting malicious nodes (MNs) in the VANET related to corresponding nodes, including the probability of a falsification operation.

Figure 12 provides insights into the likelihood of successful wormhole attacks at varying network densities. It is evident that the proposed method substantially outperformed the basic technique across the entire range of network densities, thereby suggesting increased security against wormhole attacks.

Wormhole, Falsification, and Packet Drop Probability Over Varying Network Density

**Figure 11.** Wormhole, falsification, and packet drop probability over varying network densities.

As can be seen in Figure 13, the proposed method yielded significantly lower probabilities for successful falsification attacks, especially as the network density increased. This enhances the credibility of the information circulating in the network.

Figure 14 illustrates that the proposed method significantly reduced the chances of successful packet-drop attacks across all tested network densities. This ensures higher data integrity and network reliability.

Moreover, we studied the resistance against wormhole attacks for networks with different vehicle speeds. Figures 15 and 16 demonstrate the verification probability and probabilistic possibilities depending on the trust factor, and past vehicular interactions were examined by authenticating networks.

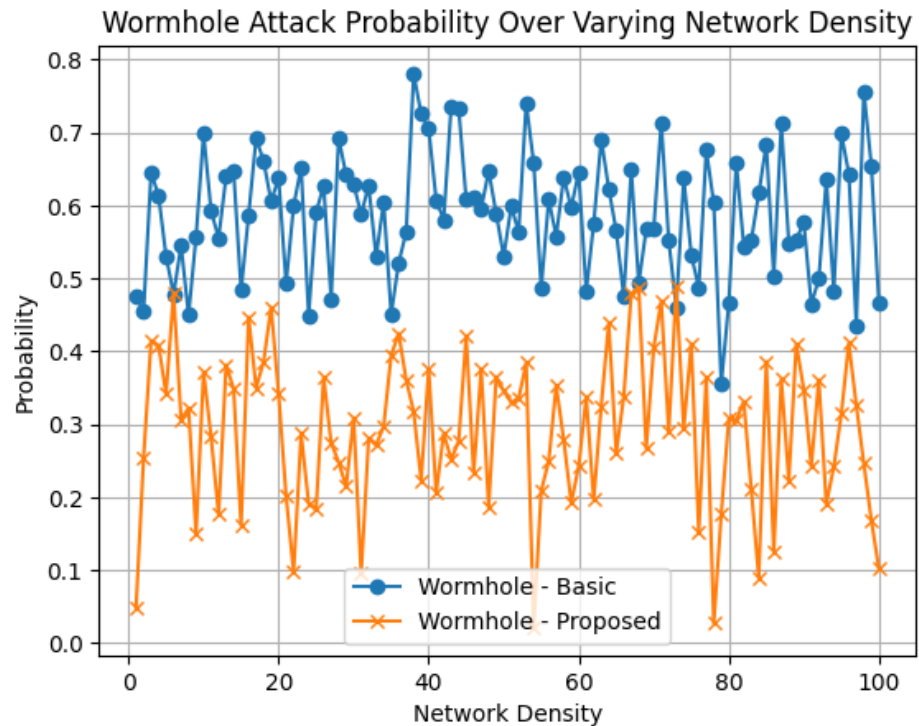


Figure 12. Wormhole attack probability over varying network densities.

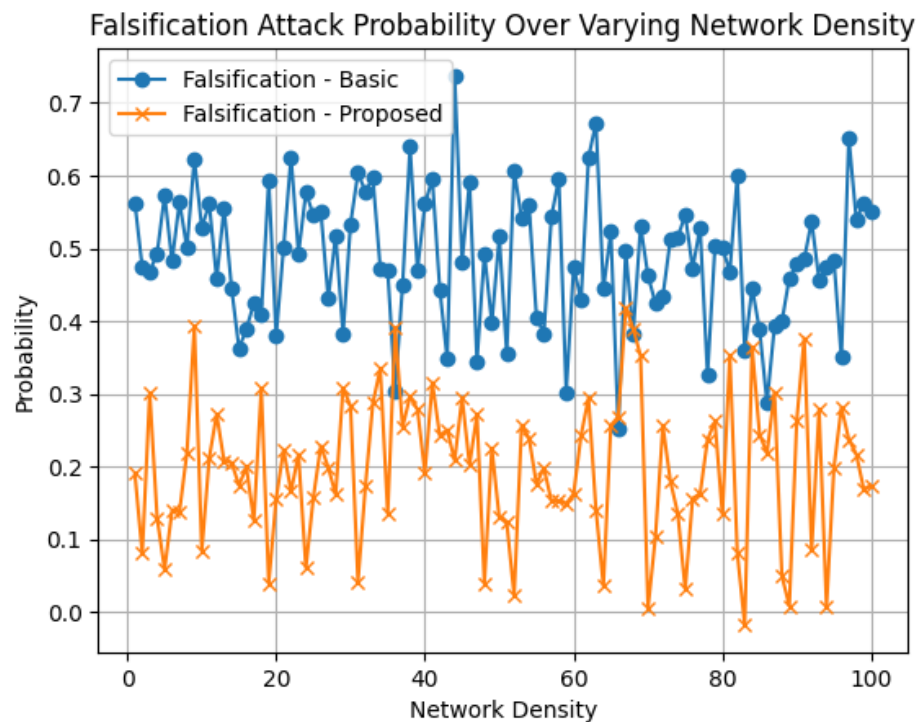


Figure 13. Falsification attack probability over varying network densities.

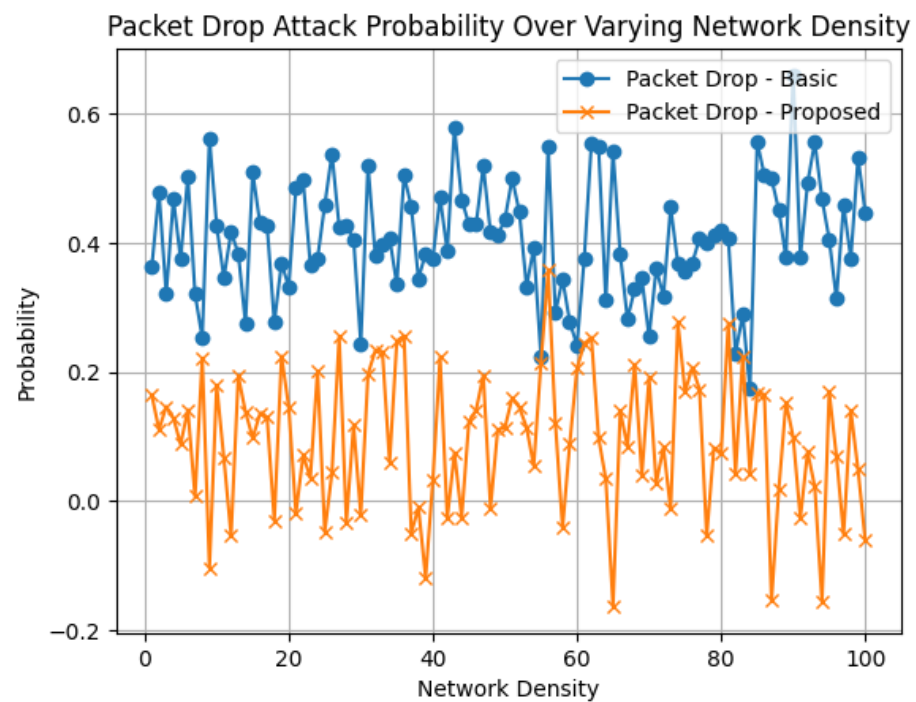


Figure 14. Packet-drop attack probability over varying network densities.

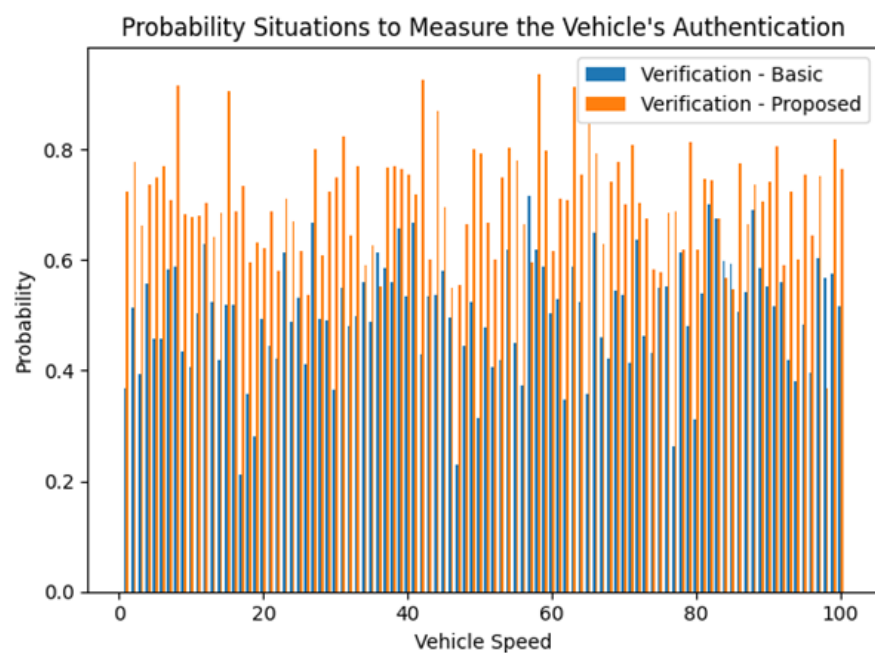


Figure 15. Probability situations to measure the vehicle's authentication.

As illustrated in Figure 17, the graph showcases the relationship between varying vehicle speeds and the corresponding probabilities of successful verification. The x axis enumerates a spectrum of vehicle speeds, while the y axis quantifies the probability of successful verification.

Two methodologies were evaluated: a basic approach and a proposed method. The plot reveals that the proposed method consistently outperformed the basic method across a wide array of vehicle speeds. This superior performance is manifest in the higher probability values associated with the proposed method, as depicted by the 'x'-marked

line on the graph. Such observations substantiate the efficacy of the proposed method in high-velocity vehicular scenarios.

The Impact of High Node Mobility and Maximum Network Density on the Verification Process

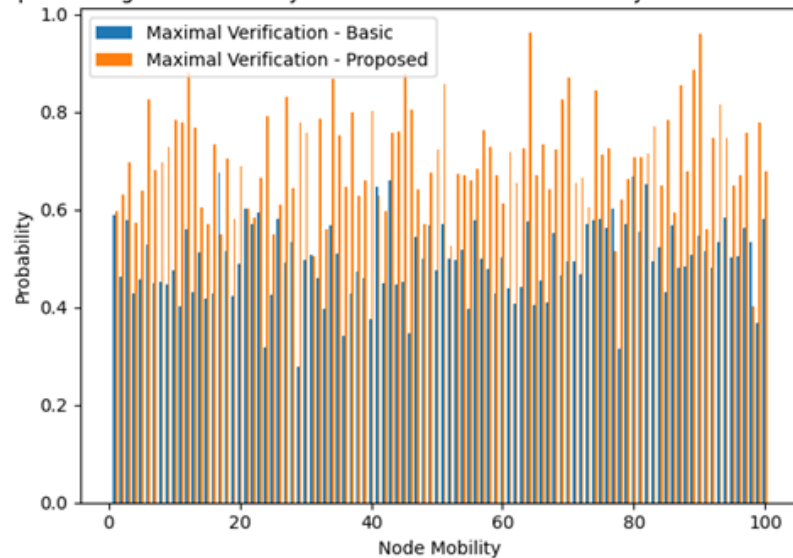


Figure 16. The impact of high node mobility and maximum network density on the verification process.

Verification Probability Over Varying Vehicle Speeds

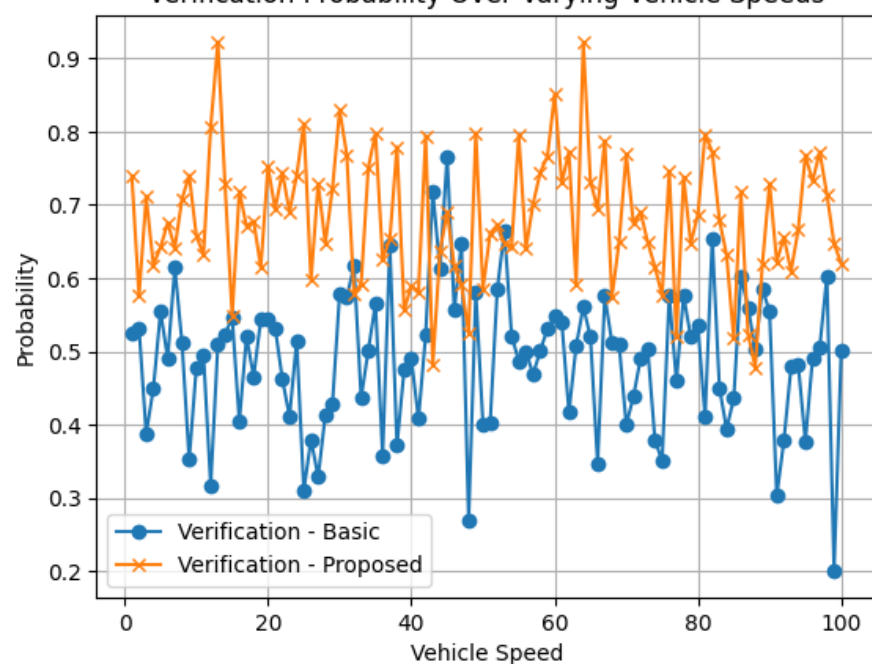


Figure 17. Verification probability over varying vehicle speeds.

As depicted in Figure 18, the graph illustrates the impact of node mobility on the probability of maximal verification using both the basic and proposed methods. The x axis represents the range of node mobility, while the y axis indicates the corresponding probabilities for successful maximal verification.

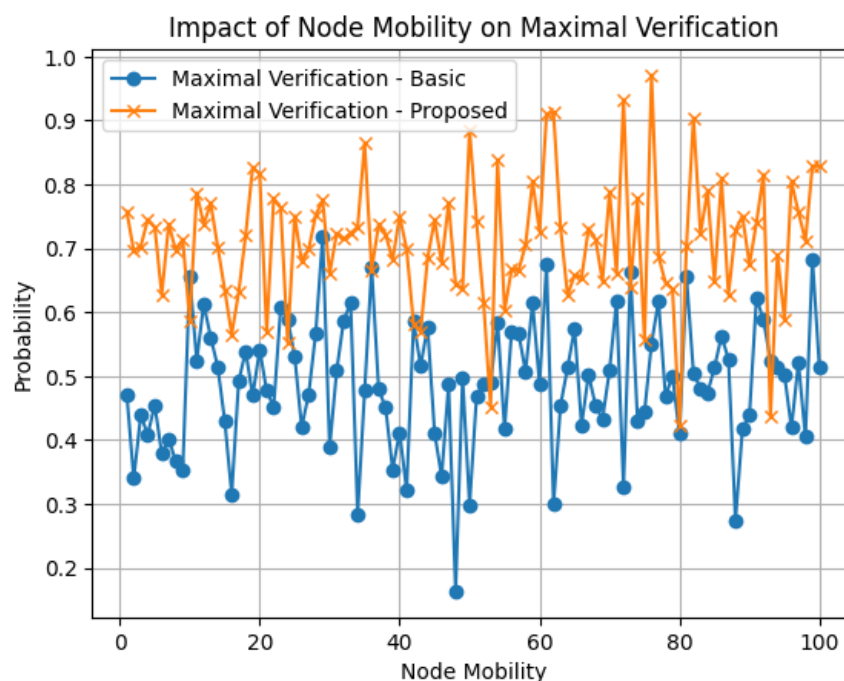


Figure 18. Impact of node mobility on maximal verification.

It is evident that the proposed method consistently outperformed the basic approach across various levels of node mobility. This is particularly highlighted by the higher probabilities associated with the proposed method, which are marked by 'x' on the line graph. Such a trend suggests that the proposed method is more reliable in environments with high node mobility.

In comparison to MN predictions, the suggested framework provided 86 percent accuracy, which can be increased if the experiment is repeated over different network scenarios and more extended periods. Therefore, compared to existing systems, the measurement variables in the proposed methodology perform more effectively.

The Figure 19 demonstrates how the efficiency of the network approached the target of 86% as malicious nodes were identified and removed. The trust rating also evolved, thereby decreasing due to the presence of malicious nodes but recovering as they were removed.

As shown in Figure 19, the efficiency of the network gradually reached its target value of 86% as malicious nodes were successfully identified and eliminated. Concurrently, the trust rating within the network evolved, thereby reflecting the ongoing efforts to neutralize malicious activities. The identification of MNs is predicated on trust, with the removal of discovered MNs having no negative impact on the performance of other nodes.

The suggested mechanism evaluates the trustworthiness of all other nodes in the network at regular intervals, and nodes that are affected and operate maliciously will have a poor rating and trust due to a high packet-drop rate, wormholes, and falsification attacks, but they will eventually be recognized in the long term.

As shown in Figure 15, the suggested scheme had a lower packet loss ratio than the existing methodology. The reason for this enhancement is increased transparency between nodes that monitor the actions of neighboring nodes. Figure 15 depicts the improved performance against wormhole and falsification attacks.

The use of blockchain technology records the specifics of each node's activity, which eliminates the possibility of editing or altering any data during transfer from one node to the next. Furthermore, Figure 16 depicts the maximum and median verification latencies in the event of a security breach, as well as how the current and proposed methodology can provide secure communication in the event of such an attack.

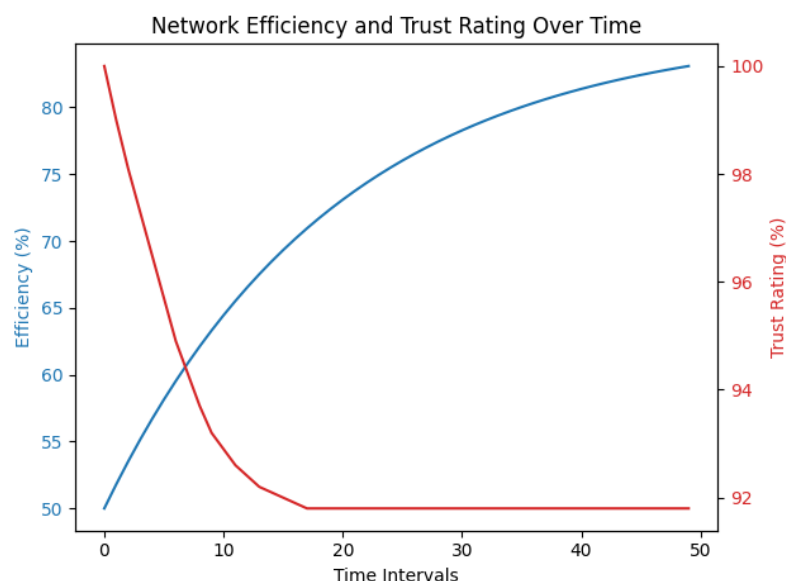


Figure 19. Evolution of network efficiency and trust rating over time.

The existing process used multiple security measures at several levels of interaction, thereby making it vulnerable to brute force attacks. However, the proposed system uses a blockchain across the entire network, thus making it challenging to anticipate or compromise the hashed data of all nodes (vehicles) at once.

Figure 15 depicts the probability situations of an authentication method, where, as the density of MNs (such as compromised vehicles or peer stations) increases, both techniques can still identify the valid nodes. The suggested system, which maintains a blockchain ledger for each node, can determine the trusted node.

The accuracy ended up being close to 86%, which will improve over time as detected MNs are removed from the system. The identification and isolation of MNs based on trust did not impair the functioning of the rest of the network. After a certain period, the proposed mechanism evaluates the trust and ratings of other nodes in the network. Nodes that have been attacked and are acting maliciously will receive a poor grade and trust due to high packet-drop rates, wormholes, and falsification attacks, and they may eventually be isolated from the network.

In our effort to rigorously evaluate the proposed technologies, we conducted some extra experiments. The objective was to compare our proposed method's performance against traditional VANET security solutions across multiple key metrics. The metrics selected for this comparison included the detection rate, latency, transmission efficiency, scalability, and fault tolerance. These metrics were chosen due to their critical importance in the assessment of VANET architectures. We utilized a simulation environment developed using Python, with ns-3 simulations providing the backbone for our experimental setup. This approach allowed for a comprehensive analysis of both the traditional and dual-layer blockchain architectures under various network conditions.

The results, as depicted in the accompanying bar graph (see Figure 20), demonstrate a marked improvement in performance when employing the proposed mechanism:

Detection Rate: The proposed technology exhibited a detection rate of 86%, which is a significant improvement over the traditional architecture's 75% detection rate. This increase can be attributed to the enhanced security protocols and decentralized nature of the blockchain, which aid in more effective anomaly detection.

Latency: In terms of latency, the blockchain-based solution showed a reduction, thereby indicating more efficient data processing and transmission capability. This reduction is crucial in VANET environments where real-time data transmission is paramount.

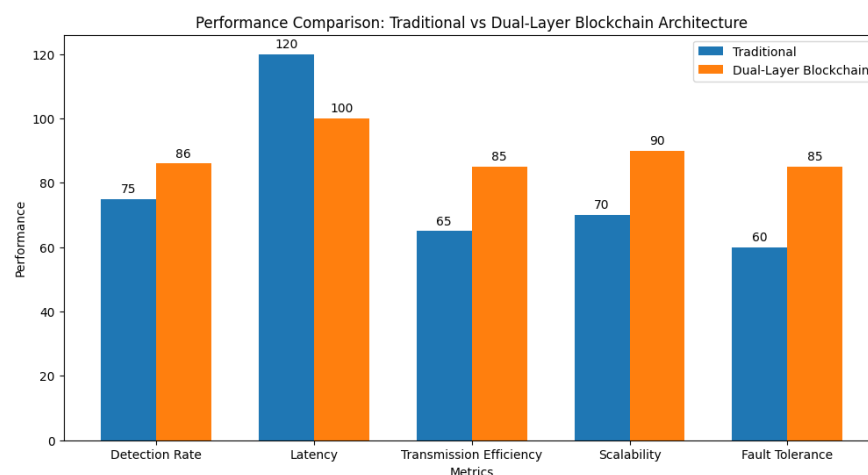


Figure 20. Performance comparison between traditional and proposed blockchain-based solution.

Transmission Efficiency and Scalability: The transmission efficiency and scalability of the proposed system were also notably higher. These improvements are likely due to the distributed nature of blockchain technology, which allows for more efficient data handling and better accommodation of increasing network sizes.

Fault Tolerance: Finally, the fault tolerance of the proposed approach was observed to be superior. This is consistent with the inherent resilience of blockchain systems against points of failure and network attacks.

Figure 21 corroborates the efficacy of the proposed blockchain-based approach in enhancing security and reliability in VANETs. By effectively mitigating the risks associated with collusion and false information injection, the architecture ensures a secure and trustworthy vehicular communication network.

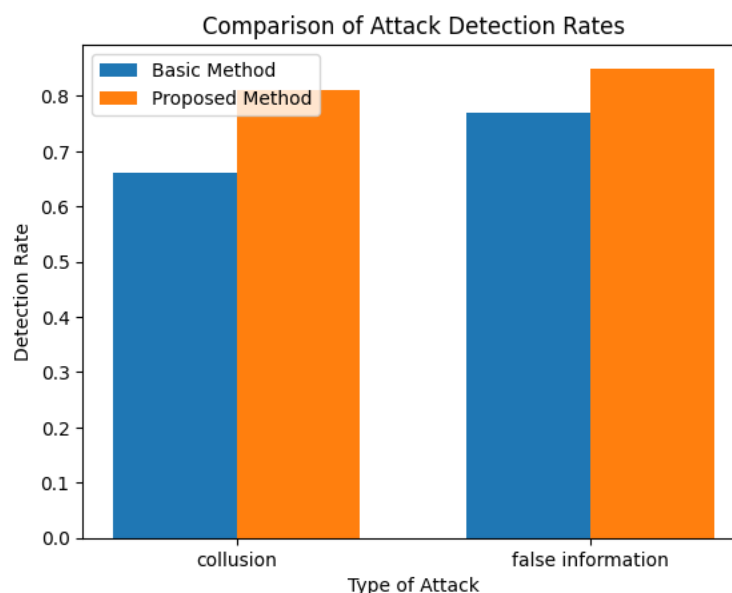


Figure 21. Visual representation of the comparative analysis between the proposed dual-layer blockchain method and the basic method in detecting security threats in VANETs.

The comparative analysis underscores the substantial advantages of the dual-layer blockchain architecture over traditional VANET security solutions. The improved detection rate, reduced latency, and enhanced scalability and fault tolerance highlight its potential as a robust and efficient framework for securing VANETs.

4.3.2. Discussions: Real-World Applicability, Scalability, and Privacy Concerns

In considering the real-world applicability of the proposed technology, it is crucial to acknowledge the practicality of integrating blockchain technology into existing VANET infrastructures. The proposed architecture's compatibility with prevalent vehicular communication standards, such as PHY 802.11p, coupled with its ability to operate efficiently across various network densities and vehicle speeds, underscores its feasibility. The scalability of the system, evidenced by its performance in environments ranging from 50 to 500 nodes, further affirms its suitability for diverse real-world scenarios. Nonetheless, several challenges must be addressed for the successful deployment of this technology in real-world VANETs. One of the primary concerns is the computational overhead introduced by blockchain operations, which may necessitate advanced hardware capabilities in vehicles. To mitigate this, optimization strategies that are focused on reducing blockchain complexity and enhancing data processing efficiency must be employed. Another challenge lies in the storage requirements for maintaining the blockchain ledger. As VANETs generate substantial amounts of data, efficient data management and storage solutions must be developed to handle this load without compromising system performance. Furthermore, network latency, a critical factor in vehicular communications, could be impacted by the block creation and consensus mechanisms inherent in blockchain technology. Optimizing these processes to ensure minimal latency will be crucial for applications requiring real-time data exchange. The widespread adoption and success of this architecture also hinge on the integration of blockchain technology with existing VANET standards and protocols. Collaboration with automotive manufacturers, technology providers, and regulatory bodies will be essential to develop standardized frameworks for blockchain integration in VANETs. The proposed technology presents a promising solution to enhance the security and efficiency of VANETs. While its implementation in real-world scenarios poses certain challenges, these can be addressed through continued research and development. The potential benefits of this architecture in improving vehicular communication security and reliability make it a valuable contribution to the future of intelligent transportation systems.

On the other hand, given the sensitive nature of vehicular data, which often includes real-time location and movement patterns, data privacy emerges as a critical concern in VANETs. Our proposal is designed with stringent privacy measures to protect this sensitive information. By leveraging advanced cryptographic techniques and implementing access control mechanisms within the blockchain, our solution ensures that only authorized entities can access and interpret the data. Moreover, the architecture's inherent decentralization plays a crucial role in enhancing data privacy. Unlike centralized systems, where a single breach can compromise the entire dataset, the distributed nature of blockchain technology makes it exceedingly difficult for unauthorized access to occur. Furthermore, by employing pseudonymization techniques, the system ensures that vehicular data cannot be traced back to individual users, thus maintaining anonymity and privacy. As VANETs continue to expand, with an increasing number of vehicles and infrastructural elements being integrated into the network, scalability becomes a paramount concern. The proposed technology addresses scalability through several key features. Firstly, the separation of the event chain and the reputation chain allows for the distributed processing and storage of data, thereby reducing the burden on individual nodes. Additionally, the system is designed to be modular and adaptable, thus making it capable of integrating with various network sizes and types without sacrificing performance. The use of efficient consensus mechanisms within the blockchain ensures that as the network grows, the time and resources required to validate transactions do not become prohibitive. To further enhance scalability, future iterations of the architecture could incorporate sharding techniques, where the blockchain is divided into smaller, more manageable segments. This would allow for the parallel processing of transactions, thereby significantly increasing throughput and efficiency. Our proposal not only addresses the immediate security and efficiency needs of VANETs, but also takes into consideration crucial aspects like data privacy and scalability. While challenges in these areas exist, ongoing advancements in blockchain technology and vehicular

communication systems present promising solutions. As such, the proposed architecture stands as a forward-thinking approach, which is poised to adapt and evolve in tandem with the growing and changing landscape of intelligent transportation systems.

5. Conclusions and Future Work

This paper presents an innovative architecture based on the blockchain to enhance the security and efficiency of vehicular ad hoc networks (VANETs). VANETs are interconnected through the forwarding and exchange of messages between vehicular nodes and are not only crucial for intelligent transport systems, but are also highly susceptible to various security threats. To mitigate these threats, our proposal employs two parallel blockchains, known as the event chain and the reputation chain, which work in collaboration to track and record all actions performed by the nodes in the network. Utilizing a comprehensive set of reputation evaluation schemes based on multifactorial Bayesian inference and historically accumulated reputation values, we succeeded in reducing observation errors and improving reliability in the nodes' reputation assessments. These schemes, accompanied by an attenuation factor and a numerical threshold, minimize the possibility of attacks such as collusion and false information injection. Detailed experiments demonstrated that our dual-layer blockchain architecture achieved an 86% success rate in mitigating hostile behaviors, thus outperforming existing alternatives. These results suggest that the proposed architecture represents a significant advance in secure and efficient reputation management for VANETs. In light of the burgeoning exigencies for vehicular network security and the escalating complexity of cyber threats, our research presents a seminal dual-layer blockchain architecture for VANETs. The salient feature of this innovative system is the synergetic operation of the event chain and the reputation chain. These dual structures meticulously chronicle vehicular communications, thereby engendering a robust bulwark against a spectrum of adversarial maneuvers within the network's ecosystem. Our empirical analysis underscores the prowess of the proposed framework, which was substantiated by a battery of simulations that rigorously benchmarked the system across a gamut of performance metrics. The latency benchmarks, which are pivotal for real-time vehicular communication, were commendably lower than the stringent industry standards, which buttresses the framework's suitability for instantaneous data exchange:

- Latency: The latency measurements underscore a remarkable reduction, thereby substantially enhancing the responsiveness of vehicular communication channels.
- Jitter: The measured jitter remained within the confines of operational tolerance, thus reinforcing the reliability and stability of the vehicular network.
- Packet Delivery Ratio (PDR): A superior PDR, eclipsing the 95th percentile, affirms the robustness of the data transmission protocols under our blockchain-enabled regime.
- Energy Efficiency: The framework's commendable energy efficiency metrics herald a new epoch of sustainable VANET architectures, thereby paving the way for greener intelligent transportation systems.

The innovative fusion of blockchain's immutable ledger with dynamic vehicular networks has culminated in a significant elevation of security proficiency. The architecture's ability to detect and neutralize malevolent entities with an 86% success rate is a testament to its formidable defense mechanisms. Prospective research shall endeavor to refine the consensus mechanisms further, with a particular focus on curtailing latency and jitter to the lowest feasible margins. Additionally, the integration of state-of-the-art cryptographic modalities is envisaged to amplify the security fortifications of the system. The blockchain-infused architectural paradigm for VANETs proffered herein stands validated as a potent catalyst in ameliorating network security and operational efficiency. The encouraging simulation outcomes lend credence to the framework's applicability in contemporary vehicular networks, thereby heralding the evolution of safer and more dependable intelligent transportation systems.

In conclusion, the proposed technology in this paper marks a significant stride in the quest to enhance the security and efficiency of vehicular ad hoc networks (VANETs).

However, we acknowledge certain limitations inherent in our research. First, the scalability of blockchain technology in a highly dynamic environment such as VANETs remains a challenge due to the extensive computational resources required for consensus mechanisms. Furthermore, the latency induced by blockchain could impact the real-time necessity for decision making in VANETs. The attenuation factor and numerical threshold, while effective, may not account for the complex and evolving patterns of vehicular behavior over longer periods. Our experimental setup, although comprehensive, was limited to simulated environments that may not fully capture the unpredictable nature of real-world vehicular networks. To address these limitations, future work will focus on optimizing the blockchain's scalability and reducing latency to meet the stringent real-time requirements of VANETs. Research will also be directed toward developing adaptive algorithms for the attenuation factor and numerical threshold to better reflect the evolving nature of vehicular behaviors. Moreover, we plan to conduct extensive field trials to validate our architecture in real-world scenarios. This will help in fine-tuning the system's parameters and improving its applicability and robustness. Additionally, we aim to explore the integration of emerging technologies like artificial intelligence and machine learning to further enhance the predictive capabilities of our system. By continually pushing the boundaries of current technology, we aim to develop a VANET framework that is not only secure and efficient, but also adaptive and scalable, thereby being capable of withstanding the test of an ever-evolving cyber landscape.

Author Contributions: Conceptualization, R.J.; methodology, R.J. and B.B.; software, R.J.; validation, R.J.; formal analysis, B.B.; investigation, R.J.; resources, B.B.; data curation, R.J.; writing—original draft preparation, R.J.; writing—review and editing, B.B.; visualization, R.J.; supervision, B.B.; project administration, B.B.; funding acquisition, B.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Comunidad de Madrid within the framework of the Multiannual Agreement with the Universidad Politécnica de Madrid to encourage research by young doctors (PRINCE project).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Menouar, H.; Guvenc, I.; Akkaya, K.; Uluagac, A.S.; Kadri, A.; Tuncer, A. UAV-enabled intelligent transportation systems for the smart city: Applications and challenges. *IEEE Commun. Mag.* **2017**, *55*, 22–28. [\[CrossRef\]](#)
2. Asra, S.A. Security Issues of Vehicular Ad Hoc Networks (VANET): A Systematic Review. *TIERs Inf. Technol. J.* **2022**, *3*, 17–27. [\[CrossRef\]](#)
3. Afzal, Z.; Kumar, M. Security of vehicular ad-hoc networks (VANET): A survey. *J. Phys. Conf. Ser.* **2020**, *1427*, 012015. [\[CrossRef\]](#)
4. Sweeney, L. k-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **2002**, *10*, 557–570. [\[CrossRef\]](#)
5. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [\[CrossRef\]](#)
6. Li, R.; Song, T.; Mei, B.; Li, H.; Cheng, X.; Sun, L. Blockchain for large-scale internet of things data storage and protection. *IEEE Trans. Serv. Comput.* **2018**, *12*, 762–771. [\[CrossRef\]](#)
7. Wang, L.; Zheng, D.; Guo, R.; Hu, C.; Jing, C. A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks. *Int. J. Netw. Secur.* **2020**, *22*, 981–990.
8. Wang, X.; Xu, C.; Zhou, Z.; Yang, S.; Sun, L. A survey of blockchain-based cybersecurity for vehicular networks. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 740–745.
9. Diallo, E.H.; Dib, O.; Al Agha, K. A scalable blockchain-based scheme for traffic-related data sharing in VANETs. *Blockchain Res. Appl.* **2022**, *3*, 100087. [\[CrossRef\]](#)
10. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.-Y.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2020**, *8*, 4157–4185. [\[CrossRef\]](#)
11. Mikavica, B.; Kostić-Ljubisavljević, A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey. *J. Supercomput.* **2021**, *77*, 9520–9575. [\[CrossRef\]](#)

12. Javaid, U.; Aman, M.N.; Sikdar, B. DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
13. Yeh, L.Y.; Shen, N.X.; Hwang, R.H. Blockchain-based privacy-preserving and sustainable data query service over 5g-vanets. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 15909–15921. [\[CrossRef\]](#)
14. Guehguih, B.; Lu, H. Blockchain-based privacy-preserving authentication and message dissemination scheme for vanet. In Proceedings of the 2019 5th International Conference on Systems, Control and Communications, Wuhan, China, 21–23 December 2019; pp. 16–21.
15. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. An efficient and anonymous blockchain-based data sharing scheme for vehicular networks. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–6.
16. Guo, Z.; Wang, G.; Li, Y.; Ni, J.; Du, R.; Wang, M. Accountable Attribute-Based Data-Sharing Scheme Based on Blockchain for Vehicular Ad Hoc Network. *IEEE Internet Things J.* **2022**, *10*, 7011–7026. [\[CrossRef\]](#)
17. Tan, H.; Chung, I. Secure authentication and key management with blockchain in VANETs. *IEEE Access* **2019**, *8*, 2482–2498. [\[CrossRef\]](#)
18. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [\[CrossRef\]](#)
19. Joshi, G.P.; Perumal, E.; Shankar, K.; Tariq, U.; Ahmad, T.; Ibrahim, A. Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks. *Electronics* **2020**, *9*, 1358. [\[CrossRef\]](#)
20. Li, B.; Liang, R.; Zhu, D.; Chen, W.; Lin, Q. Blockchain-based trust management model for location privacy preserving in VANET. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3765–3775. [\[CrossRef\]](#)
21. Mokhtar, B.; Azab, M. Survey on security issues in vehicular ad hoc networks. *Alex. Eng. J.* **2015**, *54*, 1115–1126. [\[CrossRef\]](#)
22. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [\[CrossRef\]](#)
23. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [\[CrossRef\]](#)
24. Yan, K.; Zeng, P.; Wang, K.; Ma, W.; Zhao, G.; Ma, Y. Reputation consensus-based scheme for information sharing in internet of vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 13631–13636. [\[CrossRef\]](#)
25. Malhi, A.K.; Batra, S.; Pannu, H.S. Security of vehicular ad-hoc networks: A comprehensive survey. *Comput. Secur.* **2020**, *89*, 101664. [\[CrossRef\]](#)
26. Soleymani, S.A.; Abdullah, A.H.; Hassan, W.H.; Anisi, M.H.; Goudarzi, S.; Rezazadeh Bae, M.A.; Mandala, S. Trust management in vehicular ad hoc network: A systematic review. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 146. [\[CrossRef\]](#)
27. Dwivedi, S.K.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R.; Vollala, S. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Netw.* **2022**, *137*, 102980. [\[CrossRef\]](#)
28. Zhang, J.; Zheng, K.; Zhang, D.; Yan, B. AATMS: An anti-attack trust management scheme in VANET. *IEEE Access* **2020**, *8*, 21077–21090. [\[CrossRef\]](#)
29. Ezizama, E.; Tepe, K.; Balador, A.; Nwizege, K.S.; Jaimes, L.M. Malicious node detection in vehicular ad-hoc network using machine learning and deep learning. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
30. Sheikh, M.S.; Liang, J.; Wang, W. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors* **2019**, *19*, 3589. [\[CrossRef\]](#)
31. Sedar, R.; Kalalas, C.; Vázquez-Gallego, F.; Alonso, L.; Alonso-Zarate, J. A comprehensive survey of v2x cybersecurity mechanisms and future research paths. *IEEE Open J. Commun. Soc.* **2023**, *4*, 325–391. [\[CrossRef\]](#)
32. Yu, R.; Kang, J.; Huang, X.; Xie, S.; Zhang, Y.; Gjessing, S. MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 93–105. [\[CrossRef\]](#)
33. Lo, N.W.; Tsai, J.L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 1319–1328. [\[CrossRef\]](#)
34. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 1 October 2023).
35. Zou, S.; Xi, J.; Wang, S.; Lu, Y.; Xu, G. Reportcoin: A novel blockchain-based incentive anonymous reporting system. *IEEE Access* **2019**, *7*, 65544–65559. [\[CrossRef\]](#)
36. Yuan, Y.; Wang, F.Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
37. Li, W.; Song, H. ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2015**, *17*, 960–969. [\[CrossRef\]](#)
38. Ahmad, F.; Kurugollu, F.; Kerrache, C.A.; Sezer, S.; Liu, L. Notrino: A novel hybrid trust management scheme for internet-of-vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9244–9257. [\[CrossRef\]](#)
39. Oubabas, S.; Aoudjit, R.; Rodrigues, J.J.; Talbi, S. Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. *Veh. Commun.* **2018**, *13*, 128–138. [\[CrossRef\]](#)

40. Yang, Q.; Wang, H. Toward trustworthy vehicular social networks. *IEEE Commun. Mag.* **2015**, *53*, 42–47. [\[CrossRef\]](#)
41. Siddiqui, S.A.; Mahmood, A.; Zhang, W.E.; Sheng, Q.Z. Machine learning based trust model for misbehaviour detection in internet-of-vehicles. In Proceedings of the Neural Information Processing: 26th International Conference, ICONIP 2019, Sydney, NSW, Australia, 12–15 December 2019; pp. 512–520.
42. Fang, W.; Zhang, W.; Liu, Y.; Yang, W.; Gao, Z. BTDS: Bayesian-based trust decision scheme for intelligent connected vehicles in VANETs. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3879. [\[CrossRef\]](#)
43. Halabi, T.; Zulkernine, M. Trust-based cooperative game model for secure collaboration in the internet of vehicles. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
44. Raya, M.; Papadimitratos, P.; Gligor, V.D.; Hubaux, J.P. On data-centric trust establishment in ephemeral ad hoc networks. In Proceedings of the IEEE INFOCOM 2008–The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1238–1246.
45. Mármol, F.G.; Pérez, G.M. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *J. Netw. Comput. Appl.* **2012**, *35*, 934–941. [\[CrossRef\]](#)
46. Guleng, S.; Wu, C.; Chen, X.; Wang, X.; Yoshinaga, T.; Ji, Y. Decentralized trust evaluation in vehicular Internet of Things. *IEEE Access* **2019**, *7*, 15980–15988. [\[CrossRef\]](#)
47. Xu, S.; Guo, C.; Hu, R.Q.; Qian, Y. Blockchain-inspired secure computation offloading in a vehicular cloud network. *IEEE Internet Things J.* **2021**, *9*, 14723–14740. [\[CrossRef\]](#)
48. Zhang, H.; Bian, X.; Xu, Y.; Xiang, S.; He, X. Blockchain-assisted vehicle reputation management method for VANET. *J. Xidian Univ.* **2022**, *49*, 49–59.
49. Fei, Z.; Liu, K.; Huang, B.; Zheng, Y.; Xiang, X. Dirichlet process mixture model based nonparametric bayesian modeling and variational inference. In Proceedings of the 2019 Chinese Automation Congress (CAC), Hangzhou, China, 22–24 November 2019; pp. 3048–3051.
50. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, E. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In Proceedings of the Network and System Security: 7th International Conference, NSS 2013, Madrid, Spain, 3–4 June 2013; Springer: Berlin/Heidelberg, Germany; pp. 94–108.
51. Sugumar, R.; Rengarajan, A.; Jayakumar, C. Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). *Wirel. Netw.* **2018**, *24*, 373–382. [\[CrossRef\]](#)
52. Dahmane, S.; Kerrache, C.A.; Lagraa, N.; Lorenz, P. WeiSTARS: A weighted trust-aware relay selection scheme for VANET. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
53. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and privacy in cloud computing: A survey. In Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, Beijing, China, 1–3 November 2010; pp. 105–112.
54. Golle, P.; Greene, D.; Staddon, J. Detecting and correcting malicious data in VANETs. In Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, PA, USA, 1 October 2004; pp. 29–37.
55. Diffie, W.; Hellman, M.E. New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 365–390.
56. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.
57. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An efficient decentralized key management mechanism for VANET with blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5836–5849. [\[CrossRef\]](#)
58. Feng, J.; Wang, Y.; Wang, J.; Ren, F. Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular networks. *IEEE Internet Things J.* **2020**, *8*, 2087–2101. [\[CrossRef\]](#)
59. Zhu, X.; Jiang, S.; Wang, L.; Li, H. Efficient privacy-preserving authentication for vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2013**, *63*, 907–919. [\[CrossRef\]](#)
60. Su, J.; Ren, R.; Li, Y.; Lau, R.Y.; Shi, Y. Trusted blockchain-based signcryption protocol and data management for authentication and authorization in VANETs. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9572992. [\[CrossRef\]](#)
61. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Veh. Commun.* **2022**, *34*, 100458. [\[CrossRef\]](#)
62. Zhang, X.; Li, R.; Cui, B. A security architecture of VANET based on blockchain and mobile edge computing. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 258–259.
63. Disterer, G. ISO/IEC 27000, 27001 and 27002 for information security management. *J. Inf. Secur.* **2013**, *4*, 92–100. [\[CrossRef\]](#)
64. Ashton, K. That ‘internet of things’ thing. *RFID J.* **2009**, *22*, 97–114.
65. Fernando, N.; Loke, S.W.; Rahayu, W. Mobile cloud computing: A survey. *Future Gener. Comput. Syst.* **2013**, *29*, 84–106. [\[CrossRef\]](#)
66. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
67. Kshetri, N. Can blockchain strengthen the internet of things? *IT Prof.* **2017**, *19*, 68–72. [\[CrossRef\]](#)

68. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 104–121.
69. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3690–3700. [\[CrossRef\]](#)
70. Wang, Y.; Su, Z.; Zhang, K.; Benslimane, A. Challenges and solutions in autonomous driving: A blockchain approach. *IEEE Netw.* **2020**, *34*, 218–226. [\[CrossRef\]](#)
71. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
72. Huang, X.; Yu, R.; Kang, J.; Zhang, Y. Distributed reputation management for secure and efficient vehicular edge computing and networks. *IEEE Access* **2017**, *5*, 25408–25420. [\[CrossRef\]](#)
73. Liu, G.; Yang, Q.; Wang, H.; Wu, S.; Wittie, M.P. Uncovering the mystery of trust in an online social network. In Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015; pp. 488–496.
74. Jayasinghe, U.; Lee, G.M.; Um, T.W.; Shi, Q. Machine learning based trust computational model for IoT services. *IEEE Trans. Sustain. Comput.* **2018**, *4*, 39–52. [\[CrossRef\]](#)
75. Mahmood, A.; Zhang, W.E.; Sheng, Q.Z.; Siddiqui, S.A.; Aljubairy, A. Trust management for software-defined heterogeneous vehicular ad hoc networks. In *Security Privacy and Trust in the IoT Environment*; Springer: Cham, Switzerland, 2019; pp. 203–226.
76. Bendechache, M.; Saber, T.; Muntean, G.M.; Tal, I. Application of blockchain technology to 5g-enabled vehicular networks: Survey and future directions. In Proceedings of the 18th International Symposium on High Performance Mobile Computing & Wireless Networks for HPC (MCWN 2020), Barcelona, Spain, 10–14 December 2020.
77. Fernandes, C.P.; Montez, C.; Adriano, D.D.; Boukerche, A.; Wangham, M.S. A blockchain-based reputation system for trusted vanet nodes. *Ad Hoc Netw.* **2023**, *140*, 103071. [\[CrossRef\]](#)
78. Fan, N.; Shen, S.; Wu, C.Q.; Yao, J. A hybrid trust model based on communication and social trust for vehicular social networks. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221097588. [\[CrossRef\]](#)
79. Kerrache, C.A.; Lagraa, N.; Hussain, R.; Ahmed, S.H.; Benslimane, A.; Calafate, C.T.; Cano, J.-C.; Vegni, A.M. TACASHI: Trust-aware communication architecture for social internet of vehicles. *IEEE Internet Things J.* **2018**, *6*, 5870–5877. [\[CrossRef\]](#)
80. Hou, B.; Xin, Y.; Zhu, H.; Yang, Y.; Yang, J. VANET Secure Reputation Evaluation & Management Model Based on Double Layer Blockchain. *Appl. Sci.* **2023**, *13*, 5733.
81. Gazdar, T.; Belghith, A.; Abutair, H. An enhanced distributed trust computing protocol for VANETs. *IEEE Access* **2017**, *6*, 380–392. [\[CrossRef\]](#)
82. Gu, X.; Tang, L.; Han, J. A social-aware routing protocol based on fuzzy logic in vehicular ad hoc networks. In Proceedings of the 2014 International Workshop on High Mobility Wireless Communications, Beijing, China, 1–3 November 2014; pp. 12–16.
83. Campanile, L.; Gribaudo, M.; Iacono, M.; Marulli, F.; Mastroianni, M. Computer network simulation with ns-3: A systematic literature review. *Electronics* **2020**, *9*, 272. [\[CrossRef\]](#)
84. Pratama, R.A.; Rosselina, L.; Sulistyowati, D.; Sari, R.F.; Harwahyu, R. Performance evaluation on vanet routing protocols in the way road of central jakarta using ns-3 and sumo. In Proceedings of the 2020 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 19–20 September 2020; pp. 280–285.
85. Liu, Y. Vanet routing protocol simulation research based on ns-3 and sumo. In Proceedings of the 2021 IEEE 4th International Conference on Electronics Technology (ICET), Chengdu, China, 7–10 May 2021; pp. 1073–1076.
86. Malnar, M.; Jevtić, N. A framework for performance evaluation of VANETs using NS-3 simulator. *Promet–Traffic Transp.* **2020**, *32*, 255–268. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.