electronics

Article

Enhancing Privacy Preservation in Vehicular Trust Management Systems through Blockchain Technology

Nian Jin [1], Kun Meng [2], Jie Ding [1,*], Lijun Sun [2], Haiqin Wu [3] and Xiao Chen [4]

[1] School of Computer, Jiangsu University of Science and Technology, Zhenjiang 212100, China; nian.jin5@outlook.com
[2] College of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China; kunmeng@mails.qust.edu.cn (K.M.); lijunsun@qust.edu.cn (L.S.)
[3] Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, Shanghai 200062, China; hqwu@sei.ecnu.edu.cn
[4] School of Computing and Mathematical Sciences, University of Leicester, Leicester LE1 7RH, UK; xiao.chen@leicester.ac.uk
* Correspondence: jieding@just.edu.cn

Abstract: The advent of the Internet of Vehicles (IoV) has led to a significant surge in data generation from vehicles, prompting the innovative utilization of data transactions within the IoV environment. However, due to the inherent trustless nature of data transactions in IoV, concerns have arisen regarding the lack of trust between involved parties and the potential compromise of user privacy. To address these issues, blockchain technology emerges as a suitable decentralized distributed storage and security management solution, offering transparency and security in data transactions. In this study, we leverage blockchain to integrate with the IoV, devising a robust trust management framework, and devising a privacy protection scheme to safeguard user privacy concerns. Additionally, we employ the performance evaluation process algebra (PEPA) method for system modeling and performance analysis to assess the efficacy of our proposed solution. Empirical findings demonstrate that our approach effectively enhances the performance of data transactions within the IoV while ensuring that the privacy of users remains intact.

Keywords: vehicular trust management; privacy protection; blockchain; homomorphic encryption; pseudonym; PEPA modeling

Citation: Jin, N.; Meng, K.; Ding, J.; Sun, L.; Wu, H.; Chen, X. Enhancing Privacy Preservation in Vehicular Trust Management Systems through Blockchain Technology. *Electronics* **2023**, *12*, 4949. https://doi.org/10.3390/electronics12244949

Academic Editor: Dongkyun Kim

Received: 2 November 2023
Revised: 5 December 2023
Accepted: 6 December 2023
Published: 9 December 2023

1. Introduction

The Internet of Vehicles (IoV) represents a novel generation of information and communication technology that seamlessly integrates the intra-vehicle network, inter-vehicle network, and in-vehicle mobile Internet, thus achieving a comprehensive level of connectivity and integration among vehicles, road infrastructure, individuals, and digital platforms [1]. At its core, IoV establishes a sophisticated and intricate mobile network system that enables efficient data interaction [2]. This amalgamation of networks facilitates seamless communication between vehicles, traffic facilities, and participants, collectively forming a robust and dynamic information network. The strength of IoV lies in its capacity for information synchronization, informed decision-making, and heightened operational efficiency.

A significant outcome of the IoV implementation is its positive impact on traffic management. Through real-time data exchange, the IoV empowers authorities to guide individuals away from congested areas, thereby alleviating traffic bottlenecks [3]. Moreover, the timely sharing of critical information regarding traffic accidents becomes possible, leading to the prompt deployment of emergency services and mitigating potential secondary injuries [4]. Overall, the data transactions within the IoV play a pivotal role in enhancing the safety and efficiency of the transportation ecosystem. As the IoV continues to evolve,

its potential to revolutionize the future of transportation and urban mobility becomes increasingly evident.

However, the very nature of the IoV environment presents security challenges that must be addressed to ensure the integrity, privacy, and trustworthiness of data transactions. One of the primary security challenges in IoV-based data transaction systems is the lack of trust between participants. The IoV operates in a trustless environment, meaning that complete trust between all involved parties cannot be assumed. As a result, conflicts and issues related to data transactions frequently arise among these entities, hindering the seamless exchange of data and compromising the overall system's functionality. Another significant concern is the limited transparency of transaction handling within the IoV. The traditional centralized IoV transaction management solutions, while offering control and availability advantages, often fall short in terms of transparency, information sharing, and evaluation requirements. This lack of transparency can lead to uncertainties and disputes during data transactions, further exacerbating the trust issue between the parties involved. Furthermore, data privacy protection is a critical aspect that requires immediate attention in IoV-based data transactions. As vehicle nodes interact and exchange information, ensuring message security during transmission becomes vital. The compromise of data privacy and identity privacy during these interactions poses a severe risk to vehicle safety and the confidentiality of user information.

Addressing these security challenges is of utmost importance to ensure the seamless and secure functioning of data transaction systems within the Internet of Vehicles. Innovative solutions and robust schemes need to be developed to foster trust, enhance transparency, and safeguard data privacy, ultimately promoting the widespread adoption and success of IoV-based technologies.

To tackle the trust and transparency challenges inherent in IoV data transaction systems while ensuring user privacy protection, the integration of blockchain technology has emerged as a promising approach. Blockchain, pioneered by Nakamoto in 2008 [5], represents a decentralized, distributed, and transparent digital ledger designed to record transactions in peer-to-peer networks. Its unique architecture, where each device holds equal authority [6], makes it a powerful solution for the trustless IoV environment, offering essential security features such as decentralization, transparency, and tamper resistance.

By incorporating blockchains like Ethereum [7] and Hyperledger Fabric [8] into IoV data transactions, trust management can be decentralized, enabling secure and reliable interactions among participating entities. The immutable nature of the blockchain ensures transparency, as all transaction records are visible to authorized parties, mitigating conflicts and enhancing data transaction handling [9]. However, while blockchains offer significant advantages in addressing trust and transparency challenges, they also present certain limitations concerning privacy protection for user identity and transaction data. The pseudonymous nature of blockchain addresses raises concerns about user identity exposure, potentially compromising privacy. Additionally, as data transactions are permanently recorded on the blockchain, there is a risk of sensitive information being exposed, if not adequately safeguarded. Moreover, despite the potential benefits, the performance of using blockchains to support a privacy-preserved vehicular trust system lacks comprehensive formal analysis. Understanding the efficiency and scalability implications of blockchain implementation in the IoV context is crucial to ensure the seamless and privacy-preserving operation of the system.

The primary objective of this paper is to address the crucial challenges of user distrust and privacy concerns in existing IoV transaction management schemes. To achieve this, we propose a novel and robust trust management framework based on blockchain technology to secure data transaction services within the IoV environment. Our framework aims to decentralize trust computation while restricting node behaviors, providing a more secure and reliable environment for trust evaluation. Additionally, we emphasize the importance of user privacy protection and propose two key schemes to safeguard data privacy and identity privacy. The first scheme utilizes homomorphic encryption to ensure

the integrity and confidentiality of evaluation messages while enabling smooth trust value computation. This approach is seamlessly integrated into the transaction management framework, enabling Hyperledger Fabric-based trust value updates and ensuring secure trust value storage. Furthermore, we introduce an identity privacy protection scheme based on pseudonym technology. This scheme incorporates a hybrid time-based and traffic variable-based pseudonym update trigger mechanism, automatically generating new pseudonyms at vehicle nodes in collaboration with Road Side Units (RSUs). Integrating this scheme with our designed trust management framework, pseudonym updates based on Hyperledger Fabric [8] are effectively implemented to preserve identity privacy.

To validate the effectiveness and performance of our proposed scheme, we employ Performance Evaluation Process Algebra (PEPA) [10], a formal language and high-level modeling approach. PEPA allows us to conduct formal modeling and performance analysis of our blockchain-based vehicular trust management scheme. By leveraging PEPA's composition, formalization, and abstraction capabilities, we gain valuable insights into the scheme's functionality and efficiency. In summary, the key contributions of this paper are:

- Designing a trust management framework based on the consortium chain to provide a decentralized, secure, and reliable environment for trust computation in IoV data transactions.
- Proposing data privacy protection and identity privacy protection schemes based on homomorphic encryption and pseudonym technology, respectively, to ensure the integrity, confidentiality, and anonymity of user data and identities.
- Utilizing PEPA to conduct formal modeling and performance analysis, validating the effectiveness and efficiency of our privacy-preserved blockchain-based vehicular trust management scheme.

The rest of this paper is organized as follows. Section 2 reviews the related literature. Section 3 introduces the preliminary knowledge used in this research. The transaction management framework based on the consortium chain is described in Section 4. Data Privacy and Identity Privacy Protection Scheme are designed in Section 5. Section 6 uses PEPA to model the program and perform performance evaluation and analysis. Section 7 presents additional discussion about the real-world use case. Section 8 concludes the paper and provides some directions for further research.

2. Related Work

In the context of Internet of Vehicles (IoV) data transactions, trust management and privacy protection are critical components that demand special attention. To better realize trust management and privacy protection in IoV, this section analyzes the current research status from two perspectives: IoV trust management and IoV privacy protection.

2.1. Trust Management for Internet of Vehicles

IoV trust management schemes can be broadly categorized into centralized trust management and distributed trust management approaches. Centralized trust management typically relies on a centralized server or cloud platform for processing data and completing trust value calculations and storage. For instance, Li et al. [11] proposed a reputation-based announcement scheme for in-vehicle ad hoc networks. In this scheme, vehicles broadcast messages to neighboring vehicles, and recipients provide feedback to a reputation server, which aggregates and disseminates reputation scores.

However, centralized trust management systems suffer from centralization issues, lack of privacy, and inherent trust concerns. In response, researchers have turned their focus to distributed trust management research, where blockchain technology has emerged as a compelling solution. Blockchain, a decentralized and distributed digital ledger, has garnered considerable attention and has been applied to trust management in IoV. Li et al. [12] proposed a blockchain-based trust management (BBTM) model for location privacy protection, employing a trust management algorithm to regulate vehicle behaviors effectively. Zhang et al. [13] introduced a blockchain-based vehicle networking trust management

system, developing a comprehensive vehicle reputation value calculation scheme to address message credibility concerns. Malik et al. [14] presented a BBTM framework using a consortium blockchain to track interactions between supply chain members, facilitating reputation score evaluation. Kouicem et al. [15] proposed a decentralized BBTM protocol for the Internet of Things (IoT) environment, enabling IoT devices to evaluate and share trust recommendations without relying on pre-trusted entities. More recently, Chen et al. [2] proposed a blockchain-based trust management framework for vehicle networks, integrating decentralized trust evaluation into trusted execution environments to calculate the final trust value as well as an optimization-driven scalable Byzantine fault-tolerant consensus scheme as presented in [16].

In summary, distributed trust management schemes, particularly those leveraging the decentralized, transparent, and traceable characteristics of blockchain, have become the dominant trend in trust management research. Currently, there is no comprehensive solution that achieves both BBTM and privacy protection in the context of IoV data transactions.

2.2. Privacy Protection for Vehicular Trust Management

Privacy protection in IoV involves addressing data privacy and identity privacy concerns. Data privacy protection aims to prevent unauthorized acquisition of information during information exchange between parties. Message authentication is commonly used for communication messages in the IoV environment to ensure certifiability and integrity, achieving data privacy protection. For example, Nilsson et al. [17] proposed an efficient delayed data authentication method using composite message authentication codes, capable of detecting intrusion and tampering attacks in in-vehicle networks. An improved authentication scheme based on identity public key cryptosystems was introduced by Bayat et al. [18], which effectively resists impersonation attacks. Additionally, cryptographic techniques like bilinear mapping and elliptic curve cryptography have been incorporated into such schemes.

Regarding identity privacy protection methods, IoV solutions include anonymous authentication [19], pseudonym technology [20,21], and group signature [22,23]. Liu et al. [19] developed two-factor authentication schemes based on different IoV scenarios, prioritizing security and privacy protection. Song et al. [20] proposed a density-based privacy protection scheme, triggering pseudonym updates based on the density of adjacent vehicles. Ying et al. [21] introduced a pseudonym updating scheme based on candidate location lists, facilitating dynamic pseudonym changes for vehicle nodes. Shao et al. [22] presented a decentralized group model for identity authentication in VANET using a novel group signature scheme. Wu et al. [23] addressed user privacy issues in crowdsensing environments using group signature and partially blind signature technology, allowing legally authorized users to participate without disclosing their identity and data-associated privacy.

While traditional cryptographic methods have achieved certain results in protecting vehicle data and identity privacy, most of these studies focus on privacy protection in the IoV context. However, to the best of our knowledge, there is currently no solution that simultaneously achieves both BBTM and privacy protection in the context of IoV data transactions. Privacy preservation in IoV trust management demands a secure and effective privacy protection scheme integrated into a reliable trust management framework to calculate trust values effectively.

In this paper, we aim to address these challenges and develop a privacy-preserved and blockchain-based vehicular trust management scheme to ensure secure data transaction services in the IoV. We utilize the formal method of PEPA for scheme modeling and performance analysis to demonstrate its effectiveness.

2.3. Further Research on Blockchain-Based Vehicular Networks and Their Applications

Wang et al. [24] presented a solution to security challenges in vehicular networks by proposing the offloading of revocation tasks to network edges using permissioned blockchain technology. This approach aims to address latency issues in authentication

procedures, particularly for privacy-sensitive applications. The proposed method ensures tamper-proof Global Certificate Revocation List (GCRL) management with quick synchronization and the ability to detect illegal revocation behaviors, as demonstrated in a Hyperledger Fabric-based prototype compared to a Proof-of-Work scheme. The research [25] proposed COBATS, a novel consortium blockchain-based trust model for vehicular networks, addressing security and privacy concerns in data sharing among intelligent vehicles. COBATS includes a trust management model to filter malicious recommendations, ensuring high-quality data sharing, and incorporates a consensus mechanism with joint Proof-of-Stake and Practical Byzantine Fault Tolerance (PBFT) to enhance efficiency and reduce resource consumption. Simulation results demonstrate COBATS' efficacy in improving the security and quality of data sharing while effectively handling specific attacks. Moreover, Fan et al. [26] introduced a secure announcement dissemination scheme for location-based services in Vehicular Ad-hoc Networks (VANETs) using a blockchain-assisted vehicular cloud architecture. It leverages blockchain and smart contracts for automatic vehicle classification, bonus allocation, and employs threshold signature technology for generating trustworthy announcements, demonstrating robustness and efficiency in experimental results. In addition, this survey [27] examined 75 blockchain-based security schemes for vehicular networks, covering applications like transportation and data sharing, security requirements, attacks, blockchain platforms, consensus mechanisms, and simulation tools. The survey concludes by highlighting common challenges and suggesting future research directions in the field of blockchain-based vehicular networks.

3. Preliminaries

3.1. Theoretical Foundation of Cryptography

This section provides an overview of relevant cryptography concepts used in the privacy protection scheme, including Public Key Infrastructure (PKI), digital signature, homomorphic encryption, and the Paillier Cryptosystem.

Public Key Infrastructure (PKI) [28] is an infrastructure based on public key concepts and technologies that aims to implement and provide security services. It involves generating and managing keys and certificates using public key cryptosystems. PKI serves as a pervasive security infrastructure, supporting essential digital security elements such as identity authentication, integrity, confidentiality, and non-repudiation. It facilitates secure data exchange through the use of insecure channels like the Internet. PKI technology acts as a key management platform, with encryption technology forming its foundation, and certificate services as the core. PKI offers encryption and digital signature services for various network applications, along with corresponding key and certificate management systems.

Digital Signature [29] refers to an unforgeable digital string that is associated with a digital object. It is generated using PKI by the sender of the information, allowing for verification of whether the object has been altered. Digital signatures also serve to verify the identity of the sender of the object. The fundamental principle behind digital signatures lies in the use of key pairs, where the private key is used for signature creation, and the public key is used for verification. Digital signatures provide essential services such as data origin authentication, peer entity authentication, non-repudiation, and data integrity, relying on asymmetric key encryption technology and digital digest technology.

Homomorphic Encryption [30] was first proposed by Rivest et al.. Fully homomorphic encryption enables any computing functions to be performed between ciphertexts. Partial (Additive/Multiplicative) homomorphic encryption allows for encryption functions where ciphertexts obtained by adding or multiplying plaintext on the ring can be decrypted to yield the same result as the corresponding operation performed on the ciphertext after encryption. This homomorphic property enables operations on sensitive data without compromising data privacy.

Paillier Cryptosystem [31] is an additive homomorphic encryption cryptosystem based on the residual class problem of determining composite powers, first proposed by Paillier in 1999. It enables secure addition computations on encrypted data, mak-

ing it suitable for privacy-preserving computations in distributed systems. The syntax of the Paillier Cryptosystem consists of three algorithms: a key generation algorithm $Paillier.KeyGen()$, an encryption algorithm $Paillier.Enc()$, and a decryption algorithm $Paillier.Dec()$. For two encrypted messages $Paillier.Enc(m_1)$ and $Paillier.Enc(m_2)$, the equation $Paillier.Enc(m_1) \cdot Paillier.Enc(m_2) = Paillier.Enc(m_1 + m_2)$ holds due to the additive homomorphism property.

Homomorphic encryption and pseudonym technology offer practical applications across diverse real-world scenarios. Homomorphic encryption enhances privacy by enabling secure computation of encrypted data, facilitating secure data outsourcing in cloud computing and confidential analyses in domains like smart transportation and financial transactions. Pseudonym technology provides anonymous interactions through temporary identifiers, benefiting sectors such as vehicular trust evaluation [2] and secure exchange of patient information which is vital. In the context of vehicular networks and the Internet of Things, these technologies contribute to secure data processing, while in legal and government applications, pseudonym technology aids in effective monitoring without compromising individual identities. Overall, these cryptographic techniques play a pivotal role in safeguarding privacy, securing sensitive data, and enabling secure computations in various fields, promoting trust and confidentiality in the digital age.

3.2. Blockchain and Hyperledger Fabric

Blockchain, first proposed by Nakamoto [5], is a decentralized, distributed, and public digital ledger designed for recording transactions in peer-to-peer networks. Blockchain is a shared immutable ledger that facilitates transaction logging and asset tracking across business networks. It integrates peer-to-peer (P2P) networks, consensus mechanisms, cryptography, and other technologies. The blockchain comprises several layers, including the data layer, network layer, incentive layer, consensus layer, contract layer, and application layer [32]. Smart contracts can be executed on the blockchain thus making it programmable [7]. These smart contracts allow untrusted entities to conduct transactions without relying on third parties, enhancing the efficiency and security of blockchain networks.

Hyperledger Fabric [8], a prominent project within the Linux Foundation's Hyperledger consortium, stands as a robust and flexible enterprise-grade blockchain framework. Designed to facilitate the development of permissioned distributed ledger systems, Hyperledger Fabric distinguishes itself through its modular architecture and emphasis on confidentiality, scalability, and versatility. Unlike public blockchains, Hyperledger Fabric operates in a permissioned network, where participants are known and trusted, offering heightened control over access and privacy. The framework supports smart contracts, known as chaincode, enabling the execution of business logic within the network. Hyperledger Fabric's consensus model, coupled with its modular architecture, empowers organizations to tailor their blockchain solutions to specific use cases, making it a preferred choice for enterprises seeking a secure and customizable blockchain foundation.

Hyperledger Fabric, as a permissioned blockchain framework, relies on the Byzantine fault-tolerance protocol (e.g., PBFT) to achieve consensus among its network participants. Consensus mechanisms are fundamental to the reliability and security of a blockchain, ensuring that all nodes agree on the validity and order of transactions. PBFT, known for its resilience in Byzantine fault scenarios, addresses the challenges posed by malicious nodes or potential network failures. In Hyperledger Fabric, PBFT enhances the trustworthiness of the consensus process by requiring nodes to reach agreement despite potential Byzantine faults, such as nodes providing conflicting information or attempting to compromise the system. By integrating PBFT, Hyperledger Fabric strengthens its consensus layer, contributing to the overall integrity and dependability of the blockchain network in enterprise-grade applications.

3.3. PEPA

Process Algebra for Performance Evaluation (PEPA) is a formal language proposed by Jane Hillston [10] of the University of Edinburgh in her doctoral dissertation. It serves as a high-level modeling language used to represent the structure of a system. PEPA abstracts the activities performed by components into processes, incorporating time characteristics. The execution time of activities is represented as continuous random variables, preserving memorylessness (Markov property). PEPA describes the time and functional aspects of the system through state probabilities related to time. It possesses compositionality, formalization, and abstraction capabilities, making it suitable for modeling and performance evaluation of distributed systems.

4. Blockchain-Based Trust Management Framework for IoV

An effective trust management framework serves as the fundamental pillar for realizing secure data transactions and establishing a reliable trust environment for transaction management. In light of this, we propose a two-layer trust management framework built upon the consortium blockchain. Within this framework, we carefully delineate the constituent elements, define the specific functions of each layer, establish the connections between them, and provide an abstract representation of its network model. These foundational steps set the stage for the subsequent deployment of privacy protection schemes, ensuring the robustness and privacy preservation of the data transaction system within the IoV.

4.1. System Framework

Given the inherent disparities in resources and computing power between vehicle nodes and RSUs, this work employs consortium chain technology to devise a two-layer trust management framework. The framework incorporates a Trusted Execution Environment (TEE) within the RSUs to guarantee the security of the final trust value computation. Additionally, the trust management process is divided into two distinct segments: off-chain computing and on-chain storage, tailored to the capabilities of each layer of components. This strategic partitioning enhances the overall performance of the blockchain by optimizing the utilization of resources and streamlining the processing of trust-related tasks.

4.1.1. System Model

The proposed trust management framework comprises three main components: vehicle nodes, RSUs, and a consortium blockchain. Vehicle nodes serve as the foundational elements within the IoV, acting as message sources and active participants in the evaluation process. On the other hand, RSUs function as roadside units, equipped with substantial computing power and storage capacity, and they oversee the management of all vehicles operating within their communication range. Additionally, RSUs take charge of the blockchain consensus process. The consortium blockchain is collectively maintained by all RSUs, dedicated to storing the pairs of "vehicle pseudonym-vehicle trust value". This blockchain exhibits essential features such as data transparency and traceability in the consortium blockchain network. The overall framework is visually represented in Figure 1, implementing a two-layer physical architecture, comprising a vehicle layer and a consortium layer. Note that there is a Law Enforcement Agency responsible for registration and authentication, which is omitted in Figure 1 since it is independent of trust management.

The "vehicle layer" comprises numerous vehicle nodes, each equipped with on-board units (OBUs). Before entering the system, vehicle nodes are required to submit the identity information to a law enforcement authority (LEA) for registration and authentication. Within the vehicle layer, vehicles have the flexibility to function as message senders, trust evaluators, or validators, depending on their specific roles and activities within the system. This layer serves as the fundamental bedrock of the framework, and all vehicle nodes within the vehicle layer are subject to management and oversight by the consortium layer.

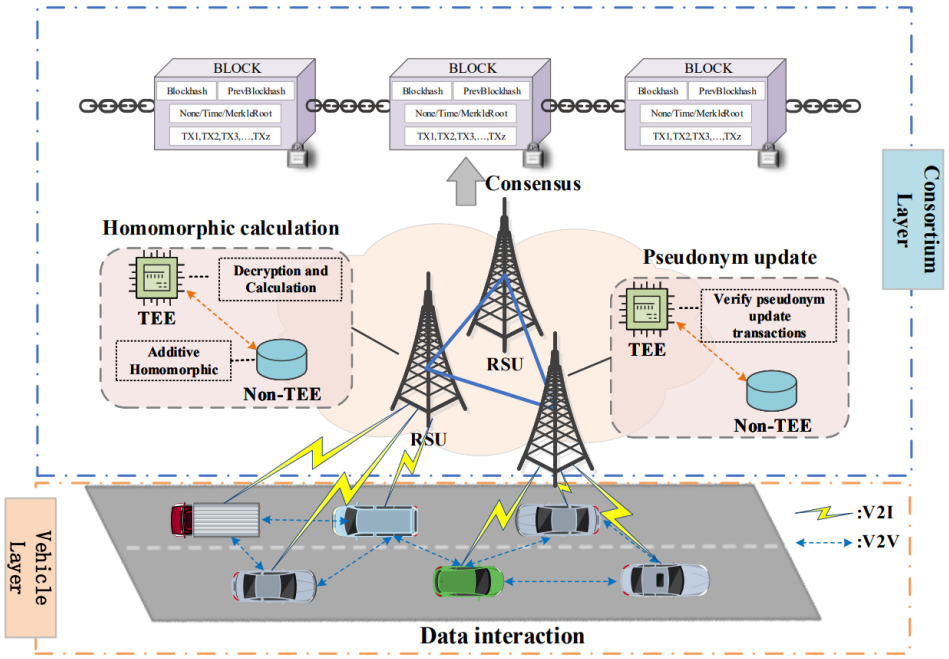


Figure 1. Blockchain-based Trust Management Framework for IoV.

It is worth mentioning that the size of an IoV system governed by a single LEA is variable, depending on factors such as geographical location, population density, and regional infrastructure. In densely populated urban areas, the IoV network may cover a smaller physical area but involve a substantial number of vehicles, while in more expansive rural regions, the coverage area may be larger with a comparatively lower vehicle count. The scale is also influenced by the integration of IoV technologies, regulatory frameworks, and the specific monitoring goals of the LEA. Notably, there is no universally defined limit for the size of an IoV system overseen by one LEA, as it is shaped by the unique characteristics and requirements of the region or jurisdiction in question.

The "consortium layer" is comprised of a set of RSUs, acting as consortium members responsible for maintaining and operating the consortium blockchain. Each RSU within the consortium layer can be divided into two parts: TEE and non-TEE sections. The non-TEE component is responsible for collecting and preprocessing messages received from vehicles. On the other hand, the TEE part handles the final trust calculation and verifies pseudonym updates. Furthermore, the consortium layer assumes responsibility for managing crucial operations, including homomorphic computation, pseudonym updates, and consensus processes, ensuring the overall integrity and functionality of the trust management framework.

The "Byzantine Fault-Tolerance (BFT) consensus protocol" is considered in our design scheme, as this protocol stands out as a well-suited solution for the Internet of Vehicles (IoV) in comparison to resource-intensive Proof-of-Work (PoW) blockchains. In the context of IoV, where real-time communication and rapid decision-making are critical, BFT protocols offer a more efficient and scalable approach. BFT consensus enables faster transaction validation through agreement among a predetermined number of nodes, ensuring the integrity of the network even in the presence of malicious actors or faults. Unlike PoW blockchains, which demand extensive computational power for consensus through competitive mining, BFT protocols are inherently more resource-efficient, making them suitable for the constrained computing environments of vehicular networks. The lightweight nature of BFT consensus allows for quicker consensus formation, reduced latency, and enhanced overall performance, making it a compelling choice for securing and managing transactions in Internet of Vehicles applications.

4.1.2. Initialization

Before joining the network, vehicle nodes must undergo authentication and registration with the LEA. In our approach, LEA acts as a trusted third party, responsible solely for the admission of new vehicle nodes and ensuring node traceability during the initialization process. Once the vehicle nodes are connected to the network, LEA does not partake in any information exchange activities. The symbol definitions used during the initialization step are summarized in Table 1.

Table 1. Notations Used in Initialization.

Symbol	Description
R_k	A roadside unit k.
V_i	The i-th vehicle node.
VID_i	The real identity of vehicle V_i.
PK_{T_k}	The public key of the TEE in R_k.
SK_{T_k}	The private key of TEE in R_k.
PK_{V_i}	Public key of vehicle V_i.
SK_{V_i}	Private key of vehicle V_i.
$P^c_{V_i}$	Initial pseudonym for vehicle V_i.
$T^c_{V_i}$	Initial trust value of vehicle V_i.

The initialization process comprises two main parts: the initialization of the vehicle node and the initialization of the RSU. Algorithm 1 presents the specific steps involved in the initialization process. In the IoV context, the vehicle node serves as the foundational element, while the RSU remains relatively stable and possesses significant computing power. Steps 4 to 10 in Algorithm 1 outline the initialization procedure for each vehicle node V_i aiming to connect to the network. Initially, V_i establishes a secure channel with the LEA to enable subsequent secure communication. Subsequently, V_i forwards an identity registration request, including its real identity information VID_i, through this channel to the LEA. Upon receiving the request, LEA compares the real identity information of vehicle node VID_i with the identity information stored in its database. In the event of false identity information being submitted, the comparison fails, leading LEA to determine the information as invalid. Consequently, LEA responds to vehicle node V_i with a result indicating "invalid real identity information". Conversely, if the comparison is successful, it confirms the authenticity and validity of the vehicle node's identity information, thus passing the verification process. Subsequently, LEA invokes the Paillier key generation function $Paillier.KeyGen()$ to generate a public-private key pair (PK_{V_i}, SK_{V_i}) specifically for vehicle node V_i. Here, $PK_{V_i} = (n, g)$ and $SK_{V_i} = (\lambda, \mu)$.

Algorithm 1 Initialization

Input: R_k, V_i, VID_i.
Output: $PK_{T_k}, SK_{T_k}, PK_{V_i}, SK_{V_i}, P^c_{V_i}, T^c_{V_i}$.
1: **for** each R_k **do**
2: $R_k \leftarrow |(PK_{T_k}, SK_{T_k}|)$;
3: **end for**
4: **for all** $|(V_i, VID_i|)$ **do** in R_k
5: **if** verify VID_i = true **then**
6: $V_i \leftarrow |(PK_{V_i}, SK_{V_i}|)$; $V_i \leftarrow |(P^c_{V_i}, T^c_{V_i}|)$;
7: **else**
8: return (invalid VID_i);
9: **end if**
10: **end for**
11: Broadcast V_i to all PK_{T_k};
12: **End**

It is essential to highlight that, for the verified vehicle node V_i, LEA securely stores the mapping relationship between its real identity and its pseudonym in its database. This secure storage ensures the highest level of confidentiality and provides a traceability channel to identify any malicious behaviors exhibited by subsequent vehicle nodes. The "pseudonym-trust value" pair of the vehicle node V_i is recorded in the consortium chain, jointly maintained by all RSUs. This consortium chain is transparent and open to the RSUs, enabling efficient management of vehicle nodes by the RSUs. It is important to note that RSUs only possess knowledge of the pseudonym of each vehicle node V_i and remain unaware of its actual identity. The real identity of V_i is exclusively known by the LEA, which is highly trusted and does not engage in any activities involving vehicle nodes after their network integration. This design ensures the complete privacy protection of vehicle node identities, effectively mitigating the risk of identity leakage.

4.2. Network Model

This solution establishes a consortium chain using Hyperledger Fabric to create a secure and reliable computing environment for IoV trust management. The network model of the consortium chain for IoV trust management is depicted in Figure 2. In this model, all RSUs form an organization, and the network includes a channel and a set of Orderer nodes. In the network model, the outermost blue rounded rectangle represents the consortium chain network dedicated to IoV. Vehicles labeled 1 to n signify the IoV clients, while the Orderer set comprises the ordering service nodes. The transaction request initiated by a vehicle node is represented as T, and the endorsement result returned by the endorsement node after verifying the request is denoted by E. The confirmation of the entire proposal is depicted as R in the result returned to the client. Within the result, the peer node refers to the endorsement node, S represents the smart contract on the chain, and B signifies the block information packaged in the consortium chain. It is important to note that L and B are distinct entities. B contains all request information Q, while L stores the verified request Q as verified by contract S.

The channel is responsible for message delivery to nodes within the same channel. Nodes sharing the same channel maintain identical ledger L and smart contract S. In this network, the PBFT consensus algorithm is employed to process vehicle node requests in four stages:

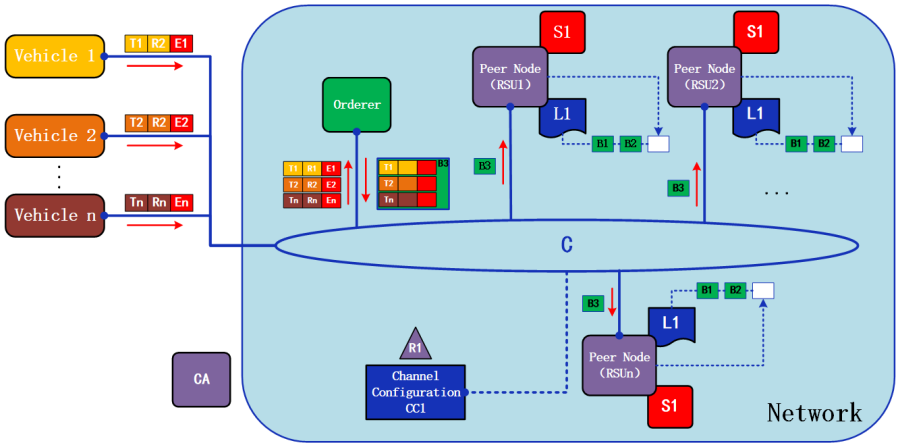


Figure 2. Network Model of IoV-based Trust Management Based on Consortium Chain.

Proposal Stage: Request transactions $T_1 \sim T_n$ generated by vehicle nodes $1 \sim n$ in the IoV are sent to RSU nodes $R_1 \sim R_n$.

Endorsement Collection Stage: RSUs verify each received transaction through the smart contract S, obtaining the corresponding endorsement result, which is then returned to the vehicle node where the request was generated.

Broadcast Sorting Stage: The vehicle node collects all endorsement results corresponding to each node, packages the requests and endorsement results into a transaction proposal and sends it to the Orderer set. The Orderer collection is responsible for ordering all transactions within the received proposal and achieving consensus, eventually forming a block B. Subsequently, the Orderer set broadcasts block B to all RSUs in the channel.

Verification and Submission Stage: Upon receiving the final block B broadcast from the Orderer collection, the RSUs validate the intra-block transactions to ensure compliance with the appropriate endorsement policy. Additionally, the RSUs ensure that the ledger state of the read-set variables has remained unchanged since the read set was generated by the transaction execution. Transactions in the block are then marked as valid or invalid based on the validation results. Once verified, the block is added to ledger L, and for each valid transaction, the write set is committed to the current state database. Furthermore, the RSUs return verification results R to the vehicle nodes, informing them that the transactions have been appended to the immutable chain and whether they were verified successfully or deemed invalid. This notification prevents the formation of strong consistency violations and chain block forks. The PBFT consensus algorithm, with its high fault-tolerance rate and efficiency, facilitates this process.

Certificate Authorities (CAs): In a blockchain system, CAs play a pivotal role in establishing and maintaining the security infrastructure. A Certificate Authority is responsible for issuing digital certificates, which serve as cryptographic credentials validating the identity of participants within the network. These certificates are crucial for facilitating secure communication and transactions. In essence, CAs act as trusted entities that verify the authenticity of participants' public keys, binding these keys to their respective identities. Through this process of certificate issuance and verification, the blockchain system ensures the integrity and authenticity of data exchanges, mitigating the risk of malicious activities such as impersonation or person-in-the-middle attacks. CAs contribute to the overall trustworthiness of the blockchain by fostering a secure environment where participants can confidently engage in transactions, thereby reinforcing the fundamental principles of transparency and immutability that define blockchain technology.

4.3. Comparative Analysis

This section presents a comparative analysis of the designed trust management scheme with existing schemes, showcasing the rationality and advantages of our proposed framework.

Firstly, compared with centralized trust management frameworks like the ART scheme proposed by Li et al. [33] and the cloud-based trust management model proposed by Chen et al. [2], our framework relies on a consortium chain, and the data is stored on the blockchain jointly maintained by RSUs, eliminating the dependency on central servers. This decentralized and fair approach ensures greater resilience and trustworthiness in the system.

Secondly, compared with traditional distributed trust management frameworks like the distributed reputation management system proposed by Huang et al. [34], our designed framework provides transparency and traceability of results. The incorporation of blockchain characteristics allows for transparent and traceable outcomes, facilitating accountability and traceability of vehicle nodes in the network, particularly when malicious behavior occurs, thereby enhancing trust management.

Furthermore, in comparison to existing trust management frameworks based on blockchain, such as the trust management system designed by Zhang et al. [13], our framework considers the security of the hardware environment. The integration of the TEE within RSUs provides hardware-based isolation technology to resist external attacks before the trust value chain, enhancing anti-attack and overall security measures.

In summary, our designed scheme outperforms centralized, traditional distributed, and existing blockchain-based trust management frameworks by providing decentralization, transparency, traceability, and enhanced security through the consortium chain and

the integration of the TEE. These features collectively contribute to a robust and reliable trust management system for Internet of Vehicles (IoV) data transactions.

5. Privacy Protection Design

In the implementation of transaction management in the IoV, frequent information exchange increases the probability of data privacy breaches and identity information disclosure, thereby posing significant security risks to the IoV. To address these privacy concerns, this section proposes two privacy protection schemes based on the two-layer trust framework presented in Section 4. The first scheme focuses on data privacy protection and employs homomorphic encryption techniques to safeguard sensitive data. The second scheme addresses identity privacy concerns and relies on pseudonym technology to protect users' identities from being revealed. By incorporating these privacy protection mechanisms, the proposed solutions aim to enhance the security and privacy of the IoV transaction environment.

5.1. Data Privacy Protection Scheme Based on Homomorphic Encryption and TEE

In order to address the data privacy problem in the trust management of the IoV, this section proposes a data privacy protection scheme based on homomorphic encryption, building upon the completed two-layer trust management framework. Our proposed scheme aims to achieve the following design objectives: prevent external attackers from forging messages, authenticate all vehicle nodes before granting access to the network, and only allow verified vehicle nodes to participate in subsequent activities within the network. Furthermore, the trust value of each vehicle node needs to be evaluated to counter the threats of internal attackers tampering with data security.

5.1.1. Detailed Protection Plan

Based on the trust management process and the structure of the proposed framework, privacy protection can be categorized into two components: trust value calculation based on homomorphic encryption within the vehicle layer chain, and trust value update using the Hyperledger Fabric-based approach within the consortium layer chain.

Homomorphic Encryption-based Trust Value Calculation. In the proposed framework, the vehicle nodes within the vehicle layer are primarily responsible for information interaction tasks, such as message sending and evaluation, to assess trust value. However, in an open IoV environment, the off-chain trust computing process may encounter the risk of privacy leakage. To safeguard the confidentiality and integrity of data during the interaction process and address the privacy concern in message transmission, the Paillier cryptosystem and digital signatures are employed.

During the trust evaluation and calculation process, we make the assumption that a vehicle node's evaluation of a message is solely related to its initial position when receiving the message. This means that if a vehicle node receives a message within the coverage of R_k and initiates the evaluation, but subsequently enters the coverage of R_{k+1} during the evaluation process, the evaluation of the message by the vehicle node remains within the range of R_k. As a result, the evaluation result needs to be submitted to R_k. At this point, the vehicle node submits the evaluation result to the current RSU, specifically R_{k+1}, which then connects with R_k and forwards the evaluation result to R_k. It is also assumed that the coverage areas of RSUs do not overlap to avoid any ambiguity.

By employing the Paillier cryptosystem and considering the non-overlapping RSU coverage areas, our proposed framework effectively ensures data privacy and integrity, enabling secure trust evaluation in an open IoV environment.

To elucidate the data privacy protection scheme, we present the trust calculation process within an RSU coverage area as an example, outlined in Algorithm 2. The symbols used in this process are defined in Table 2.

Table 2. Notations Used in Privacy Protection Design.

Notations	Description
$m_{i,j,k}$	The j-th message sent by V_i within the coverage of R_k.
$d^j_{x\to i}$	The rating value obtained by the evaluation of $m_{i,j,k}$ by the vehicle node V_x.
$[d^j_{x\to i}]_{PK_{T_k}}$	The value obtained after V_x encrypts $d^j_{x\to i}$ with PK_{T_k}.
$\mathrm{Sign}_{SK_{V_x}}(P_{V_x}, P_{V_i}, e^x_{j,i,k})$	V_x signs the evaluation result transaction with its own private key.
$\mathrm{Sum}^j_{V_i}$	The preprocessing summation result of the j messages of vehicle node V_i.
$\mathrm{Sum}^j_{V_i}$	Preprocessing summation result after TEE decryption.
$T^{dir}_{V_i}$	Direct trust value of vehicle node V_i.
$T^{his}_{V_i}$	Historical trust value of vehicle node V_i.
T_{V_i}	Final trust value of vehicle node V_i.
P_{V_i}	Current pseudonym of vehicle node V_i.
T_{V_i}	Current trust value of vehicle node V_i.
$P^{new}_{V_i}$	The new pseudonym of vehicle node V_i.
t_i	Timestamp when vehicle node V_i initiates the pseudonym request.
$\mathrm{Req}^p_{V_i}$	A pseudonym update request initiated by V_i .
$\mathrm{Rep}^p_{V_i}$	The response of R_k to the pseudonym request of $\mathrm{Rep}^p_{V_i}$.
m_k	A random number returned by R_k.
t_k	Timestamp when R_k responds $\mathrm{Req}^p_{V_i}$.

Algorithm 2 Trust Value Calculation Based on Homomorphic Encryption and TEE

Input: $V_x, m_{i,j,k}$.
Output: T_{V_i}.
1: **for** each $< V_x, m_{i,j,k} >$ **do**
2: $d^j_{x\to i} \leftarrow$ evaluate $|(m_{i,j,k}|)$;
3: $|[d^j_{x\to i}|]_{PK_{T_k}} \leftarrow$ encrypt$|(d^j_{x\to i}|)$;
4: **return** $|(e^x_{j,i,k}|)$;
5: **end for**
6: **for** each $e^x_{j,i,k}$ **do**
7: **Calculate** $\mathrm{Sum}^j_{V_i}$;
8: $\mathrm{Sum}^j_{V_i} = \prod_{x=1}^{i-1}|[d^j_{x\to i}|]_{PK_{T_k}} \times \prod_{x=i+1}^{n}|[d^j_{x\to i}|]_{PK_{T_k}}$;
9: $\mathrm{Sum}^j_{V_i} \leftarrow$ decrypt$|(\mathrm{Sum}^j_{V_i}|)$;
10: **Calculate** $T^{\mathrm{dir}}_{V_i} = \frac{\mathrm{Sum}^1_{V_i}+\mathrm{Sum}^2_{V_i}+\cdots+\mathrm{Sum}^j_{V_i}}{n-1}$;
11: **Calculate** $T_{V_i} = \alpha T^{dir}_{V_i} + \beta T^{his}_{V_i}, \alpha+\beta = 1$;
12: return $|(T_{V_i}|)$;
13: **end for**
14: **End**

During a specific time period t, a vehicle node V_i situated within the coverage of R_k acts as a message sender and transmits the j-th message $m_{i,j,k}$ to all other vehicle nodes within its range. Upon receiving the message $m_{i,j,k}$, each vehicle node $V_x(x = 0, 1, \ldots, i-1, i+1, \ldots, n)$ decides whether to evaluate this message. If the decision is affirmative, the vehicle node V_x becomes the message evaluator at that moment, and the message $m_{i,j,k}$ undergoes evaluation. To carry out the evaluation, vehicle node V_x first assesses the message $m_{i,j,k}$ to derive an evaluation rating value $d^j_{x\to i}$. Subsequently, using the public key PK_{T_k} of the TEE in R_k, vehicle node V_x encrypts the rating value $d^j_{x\to i}$ to obtain the encrypted rating value $|[d^j_{x\to i}|]_{PK_{T_k}}$. This encrypted value becomes part of the evaluation result $e^x_{j,i,k}$, represented as $e^x_{j,i,k} = \left|\langle m_{i,j,k}, |[d^j_{x\to i}|_{PK_{T_k}}\right|\rangle$.

Furthermore, vehicle node V_x evaluates the node pseudonym P_{V_x}, along with the evaluation node pseudonym P_{V_i} and the evaluation result $e^x_{j,i,k}$. These pieces of information are encapsulated in a transaction, which is then signed using the vehicle node's private key SK_{V_x}, resulting in the signed transaction $\mathrm{Sign}_{V_x}|(P_{V_x}, P_{V_i}, e^x_{j,i,k}|)$. Finally, vehicle node V_x uploads the signed transaction to its corresponding RSU, namely R_k. This process ensures that trust calculation occurs securely and privately within the RSU coverage area.

Once R_k receives evaluation transactions from all evaluation vehicle nodes within its coverage, the non-TEE part undertakes the preprocessing of these messages. Initially, the non-TEE part verifies the signature of each received evaluation transaction. Upon successful verification, the non-TEE component proceeds to classify these evaluation results based on the identification attributes of the evaluated nodes. It then consolidates all the corresponding evaluation results of the messages sent by each evaluated node. For instance, consider a vehicle node V_i during time period t, situated within the coverage area of R_k. Assuming there are a total of n vehicle nodes within R_k's coverage, when vehicle node V_i acts as a message sender, it sends j messages to other nodes. All other nodes, except V_i, perform trust evaluation on the received messages, resulting in $(n-1)$ evaluation nodes participating in the evaluation process. Thus, after preprocessing, for vehicle node V_i, there will be a total of j messages and $(n-1)$ evaluation results corresponding to each of these j messages.

Next, employing the Paillier cryptosystem, the non-TEE part conducts an additive homomorphic operation on the encrypted rating values within the evaluation results. This preprocessing operation yields the summation results $\mathrm{Sum}^j_{V_i}$ for the j messages of vehicle node V_i. The summation formula is defined as $\mathrm{Sum}^j_{V_i} = \sum_{x=0,x\neq i}^{n-1} |[e^x_{j,i,k}|]_{PK_{T_k}}$. Specifically, it can be formulated as

$$\begin{aligned}\mathrm{Sum}^j_{V_i} &= \prod_{x=1}^{i-1} |[d^j_{x\to i}|]_{PK_{T_k}} \cdot \prod_{x=i+1}^{n} |[d^j_{x\to i}|]_{PK_{T_k}} \\ &= |\left[\sum_{x=1}^{i-1} d^j_{x\to i} + \sum_{x=i+1}^{n} d^j_{x\to i}|\right]_{PK_{T_k}}.\end{aligned}$$

In this formula, $\mathrm{Sum}^j_{V_i}$ represents the aggregated evaluation results for the j messages of vehicle node V_i. The operation involves summing up the encrypted rating values $|[e^x_{j,i,k}|]_{PK_{T_k}}$ received from each evaluation node V_x, where x varies from 0 to $n-1$, with the exception of V_i. The Paillier cryptosystem ensures secure and confidential aggregation of the evaluation results, providing an effective approach for trust calculation within the RSU coverage area.

The preprocessing procedure is applied to other messages sent by the vehicle node V_i, resulting in j preprocessing summation outcomes. Subsequently, the non-TEE part aggregates these preprocessing and summation results into a transaction and transmits it to the TEE for the final trust value calculation. Upon receiving the transaction from the non-TEE, the TEE employs its private key SK_{T_k} to decrypt the preprocessing summation result and obtain the plaintext sum of the rating value Sum'_{V_i}. Consequently, the plaintext sum of these rating values is then used to calculate the direct trust value $T^{dir}_{V_i}$ of the vehicle node V_i using the following formula:

$$T^{dir}_{V_i} = \frac{\mathrm{Sum}'^1_{V_i} + \mathrm{Sum}'^2_{V_i} + \cdots + \mathrm{Sum}'^j_{V_i}}{j(n-1)}.$$

Finally, the TEE combines the historical trust value $T^{his}_{V_i}$ of the vehicle node V_i to comprehensively derive the final trust value T_{V_i}, utilizing the following formula:

$$T_{V_i} = \alpha T^{dir}_{V_i} + \beta T^{his}_{V_i}.$$

In the above equations, α and β represent the weights assigned to the direct trust value and the historical trust value of the vehicle node V_i, respectively, with the constraint that $\alpha + \beta = 1$.

Hyperledger Fabric-based Trust Value Update. Trust management in the IoV entails both trust calculation and trust storage. The blockchain technology offers a compelling solution for secure trust value storage due to its characteristics of immutability, transparency, and traceability. Once a trust value is stored on the blockchain, any tampering with a specific value within a block would affect all subsequent blocks. This tamper-resistant feature ensures data integrity, as it would require an entity to possess more than 51% of the network's computing power (a 51% attack) to make permanent changes to blockchain records. Consequently, the data stored on the blockchain is effectively safeguarded against unauthorized alterations. Furthermore, value updates based on Hyperledger Fabric technology allow for efficient supervision of information stored on the blockchain, enabling the retroactive accountability of malicious vehicle nodes.

At the consortium layer, all RSUs collaboratively maintain the blockchain. Once the TEE calculates the final trust value of a vehicle node, the RSU to which the TEE belongs acts as the initiator of the transaction proposal. This RSU initiates a trust value update transaction at the consortium layer within the established trust management framework to effectuate the trust value update.

The process unfolds as follows: RSU R_k generates a trusted update transaction proposal for the computed final trust value and broadcasts this proposal to all other RSUs in the channel. Upon receiving the transaction proposal, other RSUs function as endorsement nodes. They verify the transaction, simulate its execution based on the deployed smart contract, generate transaction results, including response values, read sets, and write sets, endorse these results, and sign them. Once endorsed, other RSUs return the endorsed transaction proposal responses to RSU R_k successively, with the return speed determined by the processing speed of each RSU. Upon collecting a sufficient number of response results in accordance with the endorsement policy, RSU R_k verifies the signature of the endorsing nodes and compares the proposal responses to ensure their consistency. If the verification is successful, RSU R_k encapsulates the trust value update transaction proposal along with the received transaction proposal responses into a transaction. This transaction is then broadcasted to the Orderer set.

Subsequently, the Orderer set receives the transaction and engages in the PBFT consensus to obtain the final transaction block that requires updating. The Orderer set then broadcasts this transaction block to all RSUs in the channel. Finally, each RSU verifies the received block and, if the verification is successful, writes the result to its local ledger. This ensures the secure and synchronized update of the trust value across all participating RSUs in the consortium.

5.1.2. Security Analysis

The designed data privacy protection scheme based on homomorphic encryption yields the following two theorems from a security perspective:

Theorem 1. *The data privacy protection scheme based on homomorphic encryption and TEE effectively safeguards the confidentiality and integrity of evaluation results, preventing potential attacks from both other evaluators and external adversaries. Additionally, any attempt to tamper with the evaluation results will be promptly detected, ensuring that attackers cannot manipulate the results without being noticed.*

Proof. Homomorphic encryption allows computations to be performed directly on encrypted data without the need for decryption, thus preserving the confidentiality of sensitive information (i.e., rating values). In the designed data privacy protection scheme, the evaluation results are computed using homomorphic encryption and the final trust value

calculation is secured with TEE, ensuring that no evaluator or external adversary can gain access to the actual data being evaluated.

Furthermore, homomorphic encryption maintains the integrity of the evaluation results by preserving arithmetic operations on encrypted data. Even if a malicious evaluator attempts to tamper with the evaluation process, the homomorphic nature of the encryption ensures that the results remain accurate and consistent. Any unauthorized modifications to the encrypted evaluation results will lead to invalid decryption during verification, which will be detected and flagged, alerting the system to potential tampering attempts.

Therefore, the utilization of homomorphic encryption and TEE guarantees the confidentiality and integrity of the evaluation results, protecting against unauthorized access and tampering. □

Theorem 2. *Our scheme provides resilience against malicious nodes attempting to alter the authenticity of events through the transmission of fake messages. Additionally, even in scenarios where certain malicious vehicles attempt to make unfair assessments, the trust calculation for each vehicle node remains accurate and reliable. Importantly, no node can modify the trust value of any vehicle node on the chain, guaranteeing the integrity and immutability of the node trust values.*

Proof. Our scheme employs a blockchain-based trust management system where all trust-related calculations and updates are recorded on an immutable ledger. The trust values of vehicle nodes are derived from verifiable and transparent evaluations made by multiple evaluators, ensuring a robust and reliable trust calculation process.

Any malicious attempts by nodes to alter the authenticity of events through fake messages will be mitigated through the trust calculation mechanism. Since trust values are derived from a consensus of evaluations from multiple nodes, any singular malicious node's influence will be minimal, and the overall trust calculation will remain accurate and resistant to manipulation.

Furthermore, the blockchain's inherent properties, such as decentralization and immutability, prevent any node, including malicious ones, from modifying trust values once recorded on the chain. This ensures the integrity and permanence of trust values for each vehicle node.

In conclusion, Theorem 2 demonstrates the scheme's resilience against malicious behaviors and its ability to maintain accurate and trustworthy trust values for vehicle nodes, while Theorem 1 confirms the security of the evaluation results through the use of homomorphic encryption and TEE, thwarting potential attacks and ensuring evaluation integrity. □

5.2. Identity Privacy Protection Scheme Based on Pseudonym Technology

In order to address the identity privacy problem within the trust management of the IoV, a pseudonym-based identity privacy protection scheme is proposed, building upon the existing two-layer trust management framework. The proposed plan aims to achieve the following design goals:

- Non-Inference of Vehicle Node Identity: The scheme ensures that an RSU cannot deduce the true identity of a vehicle node when interacting with it. The RSU is only aware of the pseudonym associated with the vehicle node, without any knowledge of its actual identity.
- Anonymous Vehicle Node Interactions: When vehicle nodes engage in communication, they are only aware that they have received a message from another legitimate vehicle node. However, they remain oblivious to the real identity of the communicating vehicle node, as the interaction occurs under the veil of pseudonyms.

By implementing the pseudonym-based identity privacy protection scheme, the trust management within the IoV system is strengthened while preserving the anonymity of individual vehicle nodes during their interactions with RSUs and other vehicles.

5.2.1. Detailed Protection Plan

The identity privacy protection scheme, based on pseudonym technology, comprises three primary components: the triggering mechanism for pseudonym update at the vehicle layer, the novel strategy for generating new pseudonyms, and the process of pseudonym update at the consortium layer.

Trigger Conditions for Pseudonym Updates. After conducting a thorough examination and analysis of the pseudonym update method, it was observed that employing a periodic or irregular pseudonym change based on the vehicle node's life cycle reduces update complexity to some extent. However, this approach also exposes a vulnerability where malicious vehicle nodes could track friendly vehicles, associating pseudonyms with sensitive information and posing security risks to these friendly nodes. Similarly, the pseudonym update strategy relying solely on traffic variables has limitations within the vehicle scenario. If there is a scarcity of vehicle interactions with information during a certain period, the threshold for triggering pseudonym updates may not be reached, consequently compromising the safety of vehicle nodes. Therefore, to address these concerns and enhance the privacy protection mechanism, this scheme proposes a novel pseudonym update trigger mechanism that combines both life cycle and traffic variables. This hybrid approach not only emphasizes the safeguarding of vehicle node location privacy but also caters to specific scenario requirements.

In the pseudonym update strategy based on traffic variables, a single pseudonym includes two key time nodes: the minimum usage time T_{min} and the mandatory update time T_{max}. Conversely, the pseudonym update strategy based on time variables sets a predefined life cycle for the node pseudonym. In our hybrid scheme, we propose a combination of both pseudonym life cycle and traffic variable thresholds. This entails introducing two pseudonym update trigger points instead of a fixed variable. Specifically, we set the mandatory update time T_{max} for the vehicle node's pseudonym update to align with the pseudonym's lifetime duration. When the current pseudonym P_{V_i} has not reached the minimum usage time T_{min}, the vehicle node continues to use this pseudonym as usual without evaluating traffic variables. However, once the pseudonym usage time exceeds the minimum usage time but falls short of the mandatory update time, the vehicle begins to monitor the designated variable (in our scheme, we assume this variable is the density of vehicle nodes). The vehicle node then determines whether the variable reaches the predefined threshold. If the threshold is met, the vehicle node initiates a pseudonym update request immediately to replace the existing pseudonym. Furthermore, if the pseudonym usage time reaches the mandatory update time but fails to reach the traffic variable threshold, the vehicle node will still proceed with an automatic pseudonym update at that moment.

Pseudonym Generation Strategy. Prior to entering the network, the vehicle node must undergo identity registration at the LEA. Only valid vehicle nodes that successfully pass the verification process will receive a public-private key pair, an initial trust value, and a pseudonym from the LEA. It is assumed that the pseudonym obtained at this stage is long-term and will be utilized for subsequent pseudonym updates. In the traditional PKI-based scheme, a considerable number of sufficient pseudonym certificates are initially allocated to registered vehicle nodes. These certificates are stored within the Tamper Proof Devices (TPD) of vehicle nodes. However, in this section, we propose a collaborative approach between the vehicle node and the RSU at the vehicle layer to generate a new pseudonym based on the initial pseudonym obtained from the LEA. This method aims to reduce the certificate load carried by the vehicle node. The specific process is detailed in Algorithm 3, and the definitions of the symbols involved can be found in Table 2.

When the vehicle node V_i meets the trigger condition for a pseudonym update, it sends a pseudonym update request to its own RSU as follows: $Req_{V_i}^{p} = |P_{V_i}, T_{V_i}, t_i|$, where t_i denotes the timestamp of the request. Upon receiving this request, RSU R_k verifies the validity of the current pseudonym P_{V_i} and the correctness of the current trust value T_{V_i}. If either of them is found to be invalid, it responds with an "invalid request" message.

However, if both the pseudonym and the trust value are valid and correct, RSU R_k sends a request-response $Rep^p_{V_i} = |R_k, m_k, t_k|$, where m_k is a random number, and t_k represents the timestamp of the response sent by R_k, which is signed using its own private key.

Algorithm 3 New Pseudonym Generation Strategy

Input: V_i, P_{V_i}, T_{V_i}.
Output: $P^{new}_{V_i}$.

for each V_i **do**
  Send a pseudonym update request $Req^p_{V_i}$;
  for each $Req^p_{V_i}$ **do**
    if Verify that P_{V_i}&T_{V_i} ==true **then**
      return $\text{Rep}^p_{V_i}$;
    else
      return (invalid);
    end if
  end for
  $P^{new}_{V_i} = H|(P_{V_i} \| m_i, t_k|)$
  return $|(P^{new}_{V_i}|)$;
end for
End

Upon receiving the reply from R_k, vehicle node V_i hashes its current pseudonym and the random number using a hash function and adds a timestamp to generate a new pseudonym $P^{new}_{V_i}$. Subsequently, the vehicle node submits a verification request for this new pseudonym to R_k. In turn, R_k verifies the existence of the pseudonym in the current network by querying the blockchain. Only if the pseudonym is valid and not already in use can V_i then utilize it for subsequent information exchange.

Hyperledger Fabric-based Pseudonym Update. In alignment with the proposed trust management framework, the "pseudonym-trust value" pairs of vehicle nodes are stored on the blockchain within the consortium layer, jointly maintained by all RSUs. This setup ensures that updating either the pseudonym or the trust value can only occur at a specific time, preventing any traceability issues. The pseudonym update process is also synchronized with the update process in Hyperledger Fabric, as depicted in Figure 3. However, it should be noted that the vehicle node initiates the pseudonym update process, and the specifics of the update process are elaborated in Figure 3.

Firstly, the vehicle node initiates a pseudonym update request along with its signature to the RSU it is associated with (denoted as R_k). Upon receiving this request, R_k verifies the validity of the signature. If the signature is valid, R_k packages the request into a proposal and broadcasts it to other RSUs in the channel. When other RSUs receive this transaction proposal, they act as endorsement nodes and verify the transaction while simulating the execution based on the deployed smart contracts. Subsequently, they generate the corresponding endorsement responses. Once the endorsement process is complete, these other RSUs sign the endorsement responses and send them back to R_k. After collecting the response results, R_k checks if they satisfy the required endorsement policy. It further verifies and compares these endorsement responses to ensure their consistency. Upon successful verification, R_k encapsulates both the pseudonym update transaction proposals and the corresponding endorsement responses into a transaction. This transaction is then broadcast to the Orderer set. The Orderer set executes the PBFT consensus algorithm on the received transaction to reach an agreement, resulting in the creation of the final transaction block. Subsequently, this transaction block is broadcast to all RSUs in the channel. Finally, each RSU verifies the integrity of the received block and proceeds to add it to the local ledger, thereby completing the pseudonym update process.

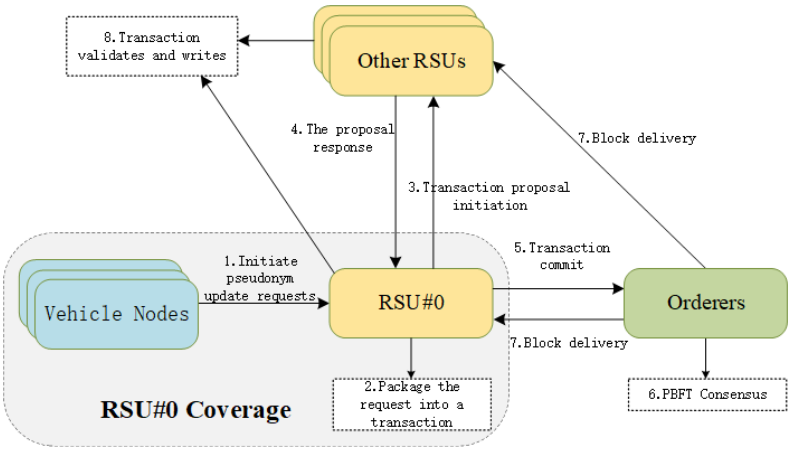


Figure 3. Hyperledger Fabric-based Pseudonym Update Process.

5.2.2. Security Analysis

Theorem 3. *A malicious node cannot generate the same pseudonym as an honest node for impersonation, effectively preventing forgery and tampering attacks.*

Proof. The proposed identity privacy protection scheme operates through a collaborative process involving the LEA, RSUs, and vehicle nodes. Each vehicle node is assigned a unique pseudonym by the LEA, which serves as the foundation for generating subsequent pseudonyms in coordination with the RSUs. The pseudonym update process employs cryptographic techniques, including private key signatures and hash functions, which render it computationally infeasible for a malicious node to replicate the precise pseudonym of an honest node. This cryptographic property ensures the uniqueness and integrity of pseudonyms, thereby making it practically impossible for a malicious node to impersonate an honest node by generating an identical pseudonym. □

Theorem 4. *A vehicle node cannot ascertain the real identity of the vehicle node it interacts with, and an RSU will remain unaware of the actual identity of the vehicle node within its jurisdiction.*

Proof. The identity privacy protection scheme utilizes pseudonyms as distinctive identifiers for vehicle nodes during their interactions. The pseudonyms are generated through a hybrid approach, incorporating initial pseudonyms obtained from the LEA and dynamically generated pseudonyms based on traffic variables. Consequently, vehicle nodes do not disclose their true identities during interactions, relying solely on their pseudonyms for identification.

Additionally, the RSUs are devoid of any knowledge regarding the real identities of the vehicle nodes within their jurisdiction. The responsibilities of RSUs include managing pseudonym update requests and ensuring the validity of pseudonyms through blockchain-based verification mechanisms. However, due to the cryptographic nature of the scheme, the actual mapping between the pseudonyms and the real identities remains concealed from the RSUs. This ensures that RSUs can efficiently oversee vehicle nodes' interactions and pseudonym updates without accessing their underlying identities, thus upholding the privacy of all involved entities.

In summary, Theorem 3 validates the resilience of our scheme against impersonation and tampering attacks, while Theorem 4 solidifies the scheme's commitment to preserving privacy by ensuring that the real identities remain undisclosed to both malicious nodes and RSUs during interactions within the system. □

5.3. Analysis of Blockchain-Related Attacks

Blockchain technology, heralded for its decentralized and transparent design, is not impervious to potential attacks that could compromise the integrity and reliability of

the system. Several key attacks have been identified, including double spending, 51% attacks, Sybil attacks, Eclipse attacks, and long-range attacks. These threats target various vulnerabilities within the blockchain ecosystem, posing risks to the validity of transactions and the overall security of the network.

To fortify blockchain systems against these attacks, BFT-based permissioned blockchains have emerged as a robust solution. BFT consensus algorithms, such as PBFT [35] and HoneyBadgerBFT [36], play a pivotal role in mitigating these security concerns. Unlike traditional proof-of-work mechanisms, BFT-based algorithms ensure consensus among nodes regarding the order and validity of transactions. This precludes the occurrence of double spending, as all nodes must collectively agree before incorporating transactions into the ledger.

One of the prominent vulnerabilities in proof-of-work blockchains, the 51% attack, is effectively mitigated by BFT-based approaches. By employing consensus algorithms resistant to Byzantine faults, BFT-based blockchains thwart the ability of a single entity to manipulate transactions, even if it controls a majority of the network's computational power. Additionally, permissioned blockchains restrict participation to a predetermined set of trusted nodes, thereby countering Sybil attacks where malicious entities attempt to create multiple false identities to influence the network.

The Eclipse attack, which involves isolating a specific node to control the information it receives, is addressed through the collaborative nature of BFT-based consensus mechanisms. Even if a node is temporarily isolated, it can rejoin the network and achieve consensus, preventing the manipulation of information. Furthermore, BFT algorithms often incorporate cryptographic signatures and real-time voting mechanisms, rendering long-range attacks, wherein adversaries attempt to recreate the blockchain's historical data, exceedingly challenging. In summary, BFT-based permissioned blockchains demonstrate a resilient defense against a spectrum of attacks, enhancing the security and trustworthiness of blockchain networks by leveraging consensus algorithms designed to withstand Byzantine faults and by restricting participation to trusted entities.

6. Modeling and Performance Analysis

One notable aspect of PEPA is its versatility, as it not only serves the purpose of semantic verification but also offers the capability of performance analysis. This makes it particularly suitable for modeling and evaluating the performance of concurrent systems [10].

The syntax of PEPA can be summarized as follows:

$$P ::= (a, \lambda).P \mid P + Q \mid P \underset{L}{\bowtie} Q \mid P \mid Q \mid A,$$

where:

- $(a, \lambda).P$ represents an action a with a time rate λ followed by the continuation process P.
- $P + Q$ denotes the choice between two processes P and Q.
- $P \underset{L}{\bowtie} Q$ indicates a synchronization between processes P and Q over a label L.
- $P \mid Q$ stands for the parallel composition of processes P and Q.
- A represents atomic processes or the base case of the syntax.

This concise syntax allows for the representation and manipulation of systems in a structured manner, facilitating the analysis of their performance and behavior. PEPA's formal nature and powerful expressiveness make it an essential tool in various domains, particularly for analyzing concurrent systems.

6.1. Homomorphic Encryption-Based Data Privacy Preserving

6.1.1. Modeling of Trust Value Calculation Based on Homomorphic Encryption and TEE

This process primarily involves a set consisting of the RSU and all vehicle nodes within its coverage. The vehicle nodes can be further categorized into message senders and evaluators based on their respective roles. Similarly, the RSU can be divided into two parts: the TEE and the non-TEE parts, depending on the internal and external environment.

The detailed PEPA model for the evaluator is provided below:

$$
\begin{aligned}
&Eva_0 \overset{def}{=} (broad\_mess, r_{broad\_mess}).Eva_1;\\
&Eva_1 \overset{def}{=} (not\_eval, r_{not\_eval}).Eva_0\\
&\quad + (eval\_mess, r_{eval\_mess}).Eva_2;\\
&Eva_2 \overset{def}{=} (encry\_rating\_value, r_{encry\_rating\_value}).Eva_3;\\
&Eva_3 \overset{def}{=} (gene\_eval\_tran, r_{gene\_eval\_tran}).Eva_4;\\
&Eva_4 \overset{def}{=} (send\_eval\_tran, r_{send\_eval\_tran}).Eva_0;
\end{aligned}
$$

The detailed PEPA model of TEE is shown as follows:

$$
\begin{aligned}
&TEE_0 \overset{def}{=} (pass\_SumCiph, r_{pass\_SumCiph}).TEE_1;\\
&TEE_1 \overset{def}{=} (decry\_SumCiph, r_{decry\_SumCiph}).TEE_2;\\
&TEE_2 \overset{def}{=} (calc\_trust\_value, r_{calc\_trust\_value}).TEE_3;\\
&TEE_3 \overset{def}{=} (gene\_TrustUp\_tran, r_{gene\_TrustUp\_tran}).TEE_4;
\end{aligned}
$$

6.1.2. Hyperledger Fabric-Based Trust Value Update Modeling

The process comprises three essential components: RSUs responsible for initiating update transactions, a group of RSUs serving as endorsement nodes, and a set of Orderers acting as consensus nodes. The RSU that initiates the update transaction, along with the endorsement node RSU set, accomplishes the endorsement and bookkeeping process, while the Orderer set executes the PBFT consensus process.

The detailed PEPA model for the TEE is presented as follows:

$$
\begin{aligned}
&Tee_0 \overset{def}{=} (broad\_tran\_prop, r_{broad\_tran\_prop}).Tee_1;\\
&Tee_1 \overset{def}{=} (retu\_prop\_resp, r_{retu\_prop\_resp}).Tee_2;\\
&Tee_2 \overset{def}{=} (coll\_resp, r_{coll\_resp}).Tee_3;\\
&Tee_3 \overset{def}{=} (retu\_coll\_resu, r_{retu\_coll\_resu}).Tee_4;\\
&Tee_4 \overset{def}{=} (Tnot\_enough, r_{Tnot\_enough}).Tee_1\\
&\quad + (veri\_resp, r_{veri\_resp}).Tee_5;\\
&Tee_5 \overset{def}{=} (gene\_tran, r_{gene\_tran}).Tee_6;\\
&Tee_6 \overset{def}{=} (broad\_tran, r_{broad\_tran}).Tee_7;\\
&Tee_7 \overset{def}{=} (broad\_tran\_block, r_{broad\_tran\_block}).Tee_8;\\
&Tee_8 \overset{def}{=} (Tveri\_tran, r_{Tveri\_tran}).Tee_9;\\
&Tee_9 \overset{def}{=} (Tupdate\_ledg, r_{Tupdate\_ledg}).Tee_0;
\end{aligned}
$$

The detailed PEPA model of the RSU of the endorsement node is as follows:

$$
\begin{aligned}
&RSUn_0 \overset{def}{=} (broad\_tran\_prop, r_{broad\_tran\_prop}).RSUn_1;\\
&RSUn_1 \overset{def}{=} (veri\_prop, r_{veri\_prop}).RSUn_2;\\
&RSUn_2 \overset{def}{=} (gene\_prop\_resp, r_{gene\_prop\_resp}).RSUn_3;\\
&RSUn_3 \overset{def}{=} (retu\_prop\_resp, r_{retu\_prop\_resp}).RSUn_4;
\end{aligned}
$$

$$RSUn_4 \overset{def}{=} (retu\_coll, r_{retu\_coll}).RSUn_5$$
$$RSUn_5 \overset{def}{=} (Rnot\_enough, r_{Rnot\_enough}).RSUn_3 + (broad\_tran\_block, r_{broad\_tran\_block}).RSUn_6;$$
$$RSUn_6 \overset{def}{=} (Rveri\_tran, r_{Rveri\_tran}).RSUn_7;$$
$$RSUn_7 \overset{def}{=} (Rupdate\_ledg, r_{Rupdate\_ledg}).RSUn_0;$$

6.1.3. Performance Evaluation and Analysis

To evaluate the efficiency of the proposed data privacy protection scheme, an analysis of response time and throughput is conducted. The assessment starts with an examination of the IoV scale, analyzing the trust calculation for different role types and varying numbers and scales. Additionally, the impact of the proposed data privacy scheme on the original trust calculation is verified.

In this scheme, the utilization of homomorphic encryption during the trust value calculation process ensures data privacy. The combination of the TEE and homomorphic encryption further enhances the protection of sensitive information during trust value calculations. Assuming a transaction size of 4 KB and a block size of 1 MB, with each block accommodating 256 transactions, the evaluation process proceeds.

Firstly, the number of participating vehicle nodes is fixed, and the response time for trust calculation is tested with varying numbers of sender nodes sending messages. For sender numbers set at 100, 150, and 200, cumulative distribution function (CDF) plots are compared. As depicted in Figure 4a, as the number of senders increases, the probability decreases, indicating that the response time increases. The higher response time is attributed to the growing number of messages published by the senders, leading to the increased processing time for each evaluation node and, consequently, elevated trust calculation time.

Next, the response time for trust computation is compared for different numbers of evaluation nodes, with a fixed number of sender nodes sending messages. With evaluator node numbers set at 10, 30, and 50, CDF graphs are compared (Figure 4b). As the number of evaluation nodes rises, the response time for trust value calculation increases. This is due to the increased participation of evaluators, leading to more message evaluation results. Consequently, the time required for non-TEE classification evaluation result transactions also rises, contributing to the overall increase in response time for trust value calculation. However, the figure shows that the response time increase is not significant, and greater participation of evaluation nodes results in more accurate trust value calculations.

Subsequently, the number of sender vehicle nodes, evaluator vehicle nodes, and RSUs remains fixed, and the response time for trust value calculation is compared with and without adopting the homomorphic encryption method. As demonstrated in Figure 4c, trust value calculation based on homomorphic encryption and TEEs incurs a slightly longer time compared to direct trust value calculation. Nevertheless, the increase is not substantial, indicating that although the introduction of homomorphic encryption results in some system performance loss, it is not significant.

Finally, system throughput for trust value calculation is compared with and without homomorphic encryption for different numbers of evaluation nodes. As shown in Figure 4d, the system throughput decreases as the number of evaluator nodes increases. This decrease is attributed to the growing number of evaluators participating in message evaluation, leading to a proportional increase in evaluation results. Consequently, RSUs need to wait for all evaluation results within their coverage areas to be submitted before calculating the trust value of the sender vehicle node. This waiting time contributes to the decrease in throughput. Moreover, the increased evaluation results also elevate RSU's trust value computation overhead, further impacting throughput and resulting in a downward trend.

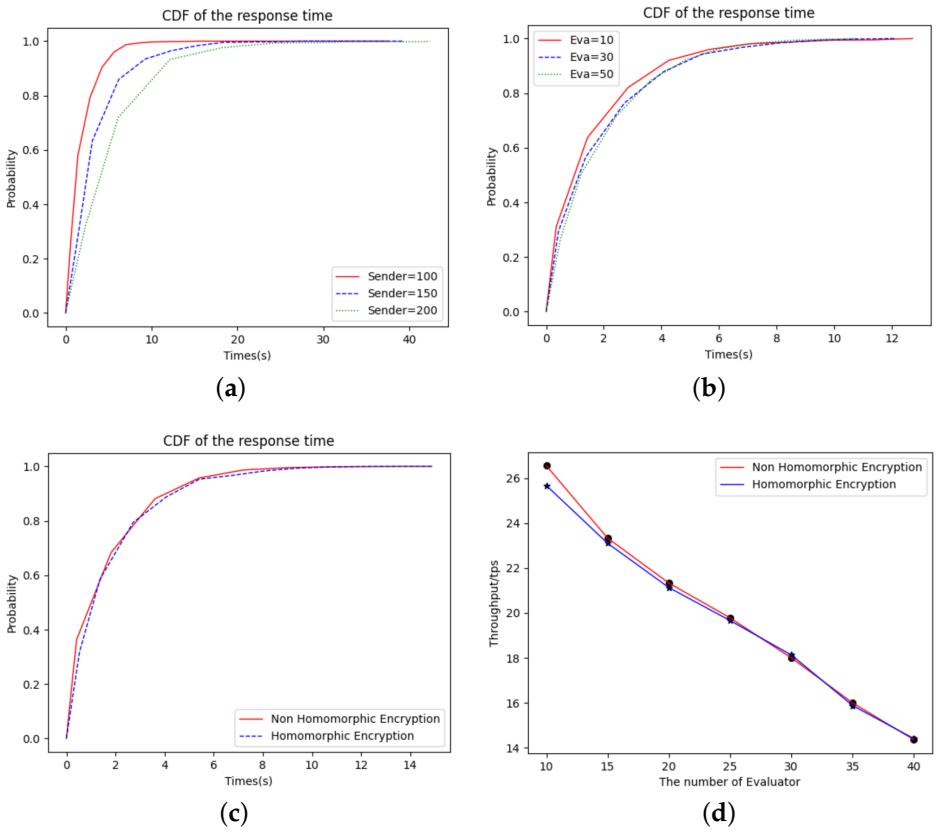


Figure 4. (**a**) CDF of response time for different numbers of senders; (**b**) CDF of response time for different numbers of raters; (**c**) Whether to add the response time CDF of homomorphic encryption; (**d**) Throughput with and without homomorphic encryption with different numbers of evaluator nodes.

6.2. Identity Privacy Protection Based on Pseudonym Technology

6.2.1. New Pseudonym Generation Process Modeling

The modeling of the new pseudonym generation process involves two key components: the modeling of vehicle nodes and the modeling of RSUs. The generation of new pseudonyms requires several verification interactions between these two entities to be determined.

RSUs play a crucial role in the new pseudonym generation process and achieve this through two interactions with vehicle nodes. In this process, RSUs primarily take responsibility for verifying the trust value and pseudonym of the pseudonym initiator, providing the request result and verifying the validity of the new pseudonym.

The detailed PEPA model of RSU is presented below:

$$RSU_0 \overset{def}{=} (NewPseu\_gene\_requ, r_{NewPseu\_gene\_requ}).RSU_1;$$

$$RSU_1 \overset{def}{=} (veri\_CurrPseu, r_{veri\_CurrPseu}).RSU_2;$$

$$RSU_2 \overset{def}{=} (veri\_TrValu, r_{veri\_TrValu}).RSU_3;$$

$$RSU_3 \overset{def}{=} (retu\_GenResp, r_{retu\_GenResp}).RSU_4$$

$$RSU_4 \overset{def}{=} (RGenResp\_invalid, r_{RGenResp\_invalid}).RSU_0 + (NewPseu\_veri\_requ, r_{NewPseu\_veri\_requ}).RSU_5;$$

$$RSU_5 \overset{def}{=} (veri\_NewPseu, r_{veri\_NewPseu}).RSU_6$$

$$RSU_6 \overset{def}{=} (retu\_VerResp, r_{retu\_VerResp}).RSU_7$$

$$RSU_7 \stackrel{def}{=} (RVerResp\_invalid, r_{RVerResp\_invalid}).RSU_0 + (gene\_PseuUp\_tran, r_{gene\_PseuUp\_tran}).RSU_0;$$

The detailed PEPA model of vehicle node is shown as follows:

$$V_0 \stackrel{def}{=} (NewPseu\_gene\_requ, r_{NewPseu\_gene\_requ}).V_1;$$
$$V_1 \stackrel{def}{=} (retu\_GenResp, r_{retu\_GenResp}).V_2;$$
$$V_2 \stackrel{def}{=} (VGenResp\_Invalid, r_{VGenResp\_Invalid}).V_0 + (gene\_NewPseu, r_{gene\_NewPseu}).V_3;$$
$$V_3 \stackrel{def}{=} (NewPseu\_veri\_requ, r_{NewPseu\_veri\_requ}).V_4;$$
$$V_4 \stackrel{def}{=} (retu\_VerResp, r_{retu\_VerResp}).V_5;$$
$$V_5 \stackrel{def}{=} (VVerResp\_invalid, r_{VVerResp\_invalid}).V_0 + (end, r_{end}).V_0;$$

6.2.2. New Pseudonym Generation to Update Complete Process Modeling

The complete process of new pseudonym generation and update comprises two key stages: new pseudonym generation and Hyperledger Fabric-based pseudonym update. This section focuses on modeling the different components involved in the process, which include vehicle nodes, the TEE, the RSU set serving as the backing node, and the Orderer set acting as the consensus node.

The TEE plays a pivotal role throughout the entire process, engaging in interactions with the vehicle nodes during new pseudonym generation, collaborating with other RSUs during the endorsement process, and communicating with the Orderer during pseudonym updates.

The following presents a detailed PEPA model of the TEE:

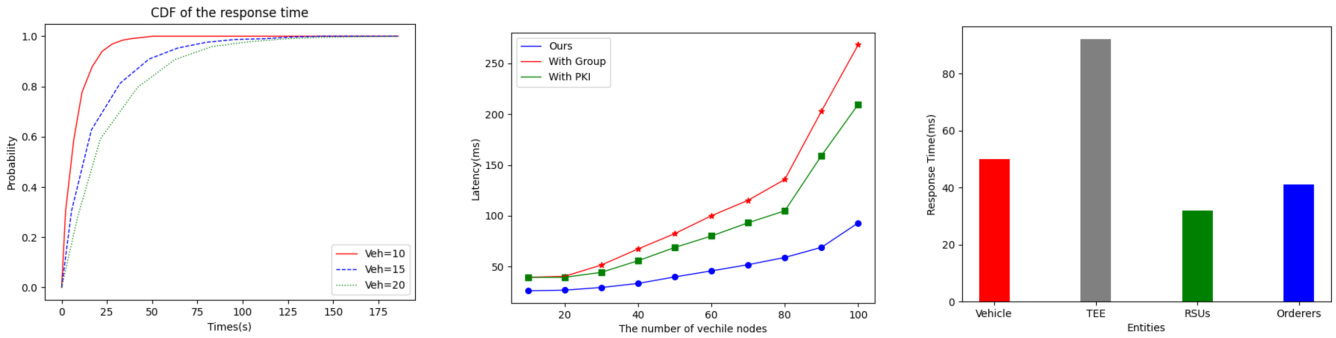
$$Tee_0 \stackrel{def}{=} (NewPseu\_gene\_requ, r_{NewPseu\_gene\_requ}).Tee_1;$$
$$Tee_1 \stackrel{def}{=} (veri\_CurrPseu, r_{veri\_CurrPseu}).Tee_2;$$
$$Tee_2 \stackrel{def}{=} (veri\_TrValu, r_{veri\_TrValu}).Tee_3;$$
$$Tee_3 \stackrel{def}{=} (retu\_resp, r_{retu\_resp}).Tee_4;$$
$$Tee_4 \stackrel{def}{=} (resp\_invalid, r_{resp\_invalid}).Tee_0 + (NewPseu\_veri\_requ, r_{NewPseu\_veri\_requ}).Tee_5;$$
$$Tee_5 \stackrel{def}{=} (veri\_NewPseu, r_{veri\_NewPseu}).Tee_6;$$
$$Tee_6 \stackrel{def}{=} (retu\_resp, r_{retu\_resp}).Tee_7;$$
$$Tee_7 \stackrel{def}{=} (resp\_invalid, r_{resp\_invalid}).Tee_0 + (gene\_PseuUp\_tran, r_{broad\_tran\_prop}).Tee_8;$$
$$Tee_8 \stackrel{def}{=} (broad\_tran\_prop, r_{broad\_tran\_prop}).Tee_9;$$
$$Tee_9 \stackrel{def}{=} (retu\_prop\_resp, r_{retu\_prop\_resp}).Tee_{10};$$
$$Tee_{10} \stackrel{def}{=} (coll\_resp, r_{coll\_resp}).Tee_{11};$$
$$Tee_{11} \stackrel{def}{=} (retu\_coll\_resu, r_{retu\_coll\_resu}).Tee_{12};$$
$$Tee_{12} \stackrel{def}{=} (not\_enough, r_{not\_enough}).Tee_9 + (veri\_resp, r_{veri\_resp}).Tee_{13};$$
$$Tee_{13} \stackrel{def}{=} (gene\_tran, r_{gene\_tran}).Tee_{14};$$

$$Tee_{14} \stackrel{def}{=} (broad\_tran, r_{broad\_tran}).Tee_{15};$$
$$Tee_{15} \stackrel{def}{=} (broad\_tran\_block, r_{broad\_tran\_block}).Tee_{16};$$
$$Tee_{16} \stackrel{def}{=} (veri\_tran, r_{veri\_tran}).Tee_{17};$$
$$Tee_{17} \stackrel{def}{=} (update\_ledg, r_{update\_ledg}).Tee_{0};$$

6.2.3. Performance Evaluation and Analysis

To verify the effectiveness of the proposed scheme, the constructed PEPA model is simulated and implemented in this section using Python for the process. Regarding performance metrics, we test the latency of new pseudonym generation under different parameters, obtain the cumulative distribution function graph, and compare the throughput of the system with varying numbers of vehicle nodes. Additionally, we simulated the entire pseudonym update process and tested the response time of different components involved in the pseudonym update process.

As depicted in Figure 5a, we compare the time required to generate new pseudonyms within an RSU coverage when the number of vehicle nodes updating their pseudonyms is 10, 15, and 20, respectively. The experimental results reveal that the response time for new pseudonym generation increases with the number of vehicle nodes. This can be attributed to the process wherein a vehicle node, requiring pseudonym updates, must submit a request to the respective RSU. Upon receiving and verifying the update request, the RSU returns a random number, based on which the vehicle node generates a new pseudonym. However, only one RSU handles these operations within its coverage. As the number of vehicle nodes and pseudonym update requests increases, the generation time for new pseudonyms also rises.



(**a**) (**b**) (**c**)

Figure 5. (**a**) CDF of response time for different numbers of vehicle nodes; (**b**) Comparison of system delays under different schemes and different vehicle nodes; (**c**) Response time of components during pseudonym update.

In Figure 5b, we observe that the system latency increases with the number of vehicle nodes. The blue circular line represents the scheme proposed in this thesis, the green square line denotes the traditional PKI-based privacy protection scheme, and the black asterisk line signifies the group signature-based privacy protection scheme. The curves demonstrate that our proposed scheme exhibits lower latency compared to the other two. The PKI-based privacy protection scheme typically involves storing numerous certificates at the vehicle nodes, leading to increased node communication load. Conversely, the group-based privacy protection scheme conceals node identities by forming groups with multiple participants, resulting in heightened communication overhead.

Figure 5c illustrates the response time generated by different components involved in the pseudonym update process. The figure reveals that a significant portion of computational overhead is concentrated in the Trusted Execution Environment (TEE). This

is due to the TEE's multifaceted tasks, including validating received pseudonym update requests during the new pseudonym generation phase, generating random numbers for transmission to vehicle nodes, creating pseudonym update transactions in the Hyperledger Fabric-based pseudonym update, participating in the validation of transaction responses, and finally, engaging in blockchain bookkeeping.

6.3. Practical Experiments and Performance Analysis

This section presents a performance comparison between PBFT and Zyzzyva on the proposed system, aiming to assess their suitability for mobile network environments. The experiments were conducted using mobile device emulators on a 2.8 GHz Core-i7 personal computer. These emulators were integrated within the Android Studio IDE, equipped with 1536 MB RAM and 6 GB internal storage, accurately simulating the hardware performance of Google Pixel-2 smartphones. To construct a virtual local area network, each emulator was connected to a virtual router via port redirection.

Given the limitations of the PC hardware, the experiment involved a system comprised of four Android devices. The client and replica software were seamlessly integrated into the mobile test environment. To ensure reliable execution, it was assumed that received requests would not be lost, thereby guaranteeing the processing of all requests in the task queue. In order to emulate real-world conditions, the experiment introduced a network delay with varying lengths ranging from 50 ms to 100 ms, simulating an ordinary 4G mobile network. Initially, the experiment evaluated the system's performance under normal network conditions with no failures. Two key variables were considered in the test: the time interval for sending requests and the message size. The test collected logs for 1000 transactions, during which the client dispatched 1000 fixed-size requests with specified time intervals, and the operation results were recorded. Subsequently, the process was repeated with the client sending 1000 fixed-interval requests, but with different message sizes. Through analysis of the logs on the devices, crucial performance metrics such as throughput and latency were calculated. To assess the system's resilience to failures, the aforementioned steps were replicated in scenarios involving f replicas failure and primary sleeping. This allowed for a comprehensive performance observation of PBFT and Zyzzyva in challenging conditions.

Figures 6a,c display the throughput under different request time intervals and message sizes in the normal case. Generally, as the request time interval increases, both mechanisms experience a decline in throughput and eventually approach similar values when the request interval exceeds 2.5 s. When requests are sent more frequently, both algorithms become saturated, with their request speed surpassing the processing speed. Notably, when the request interval is less than 2.5 s, the PBFT system reaches saturation with a throughput of 0.41 TPS, while Zyzzyva's throughput remains unsaturated until the request interval is reduced to 1.0 s, reaching a maximum throughput of 0.78 TPS, which is 90% higher than PBFT. Remarkably, irrespective of the algorithm, an increase in message size up to 100 KB has little effect on the throughput rate of DFIT, as the time interval (4.0 s) is greater than the execution time of a single request.

Figures 6b,d demonstrate that the latency of PBFT consistently surpasses that of Zyzzyva across various request intervals and message sizes. Zyzzyva achieves a latency of 1.25 s, which is 50% lower than PBFT. Consequently, Zyzzyva outperforms PBFT in terms of both higher throughput and lower latency in a normal mobile system.

These findings shed light on the performance characteristics of DFIT with PBFT and Zyzzyva in different scenarios. The results indicate that Zyzzyva exhibits superior efficiency and responsiveness in typical mobile network conditions, making it a promising option for applications demanding high throughput and low latency.

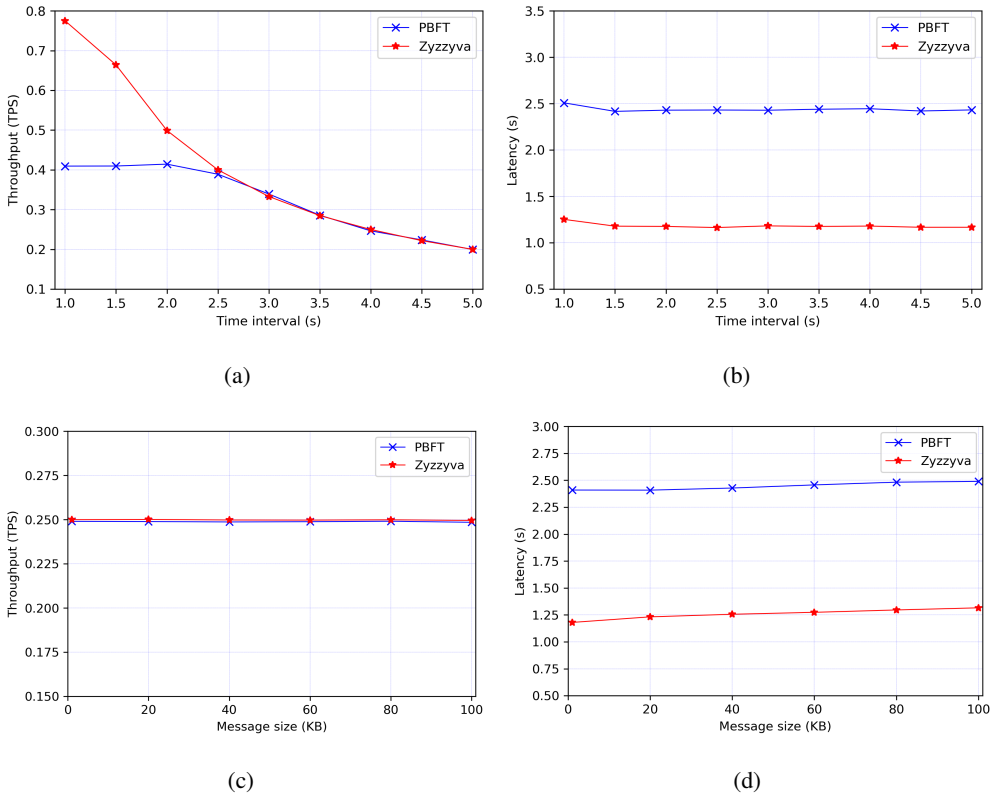


Figure 6. Throughput and latency for 1000 transactions in the normal case. (**a**) Throughput and (**b**) latency when the request time interval varies from 1.5 to 5.0 s. Message size = 1 KB. (**c**) Throughput and (**d**) average latency when the message size varies from 1 KB to 100 KB. Request interval = 4.0 s.

In summary, the experiments presented in this section provide valuable insights into the performance characteristics of PBFT and Zyzzyva within a mobile network context. The outcomes contribute to a deeper understanding of the applicability of these consensus protocols for ensuring secure and efficient operations in vehicular networking environments.

We further conducted experiments on five Azure cloud VMs, each VM equipped with 8 vCPUs (2.45GHz) and 32 GB of RAM [16,37]. Figure 7 illustrates the throughput variations of different state-of-the-art consensus protocols, such as SBFT [38], HotStuff [39], and SharBFT [16]. The PBFT (i.e., BFT-SMaRt in the figure) protocol relies on mutual voting among vehicle nodes, resulting in a message complexity of $O(n^2)$ and substantial communication overhead. Consequently, as the number of vehicle nodes increases, system throughput experiences a sharp decline. In contrast, SBFT and HotStuff employ a linear consensus scheme, surpassing PBFT in terms of system throughput. Meanwhile, the SharBFT [16] protocol utilises a scalable and linear consensus operation design, demonstrating a consistently high throughput superior to other methods. Notably, SharBFT achieves parallel consensus on blocks, while other approaches can only achieve consensus on one block at a time. Figure 8 details the end-to-end latency, covering the duration from client initiation to receiving server responses. According to our previous experiments [37], the obtained Figures 7 and 8 figures highlight that, compared to SBFT, HotStuff, and PBFT, the SharBFT algorithm reduces latency by 600%, 490%, and 2900%, respectively.

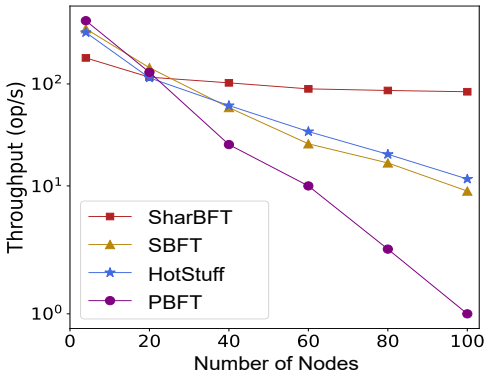


Figure 7. Throughput Comparison [37].

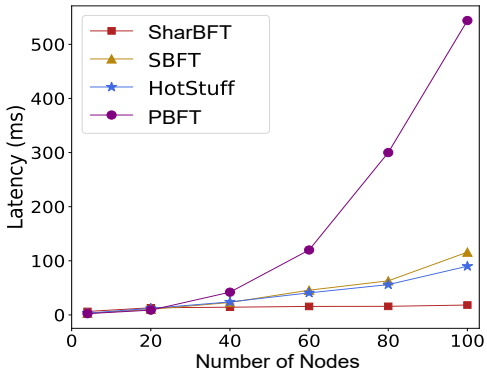


Figure 8. Latency Comparison [37].

7. Discussion

In a real-world traffic scenario, scaling issues can significantly impact the effectiveness of our proposed blockchain-integrated IoV framework. For this reason, future research should delve deeper into assessing scalability aspects, particularly in urban environments where traffic density is high, to ensure our solution remains robust and efficient under varying conditions. Moreover, a more thorough comparative analysis is required by considering various existing models, protocols, and technologies in the IoV domain to establish a comprehensive evaluation of our proposed trust management framework and privacy protection scheme. In addition, the deployment of our proposed blockchain-integrated IoV framework presents several challenges in terms of user experience and potential regulatory considerations. User experience is a pivotal factor influencing the acceptance and effectiveness of technological solutions, especially in dynamic environments like the IoV. Ensuring an intuitive interface, seamless interactions, and user-friendly features will be crucial for fostering user acceptance and satisfaction. Additionally, navigating potential regulatory challenges is imperative for the successful implementation of our framework. Compliance with data privacy regulations, adherence to legal frameworks, and alignment with industry standards will be essential to mitigate regulatory risks and ensure the ethical and lawful deployment of the IoV system. Balancing these aspects in the design and implementation phases is vital for the framework's overall success, warranting a meticulous examination of user experience and regulatory landscapes to address these challenges comprehensively.

8. Conclusions

This paper has tackled the crucial issues of distrust and privacy leakage arising from data transactions between nodes in vehicular networking. We have successfully devised a robust framework for managing vehicular networking transactions and have implemented a privacy protection scheme within this framework. Our approach involves the design of a

two-tier federated blockchain-based in-vehicle network architecture, wherein we leverage homomorphic encryption and pseudonym technology to ensure both data security and identity privacy. By incorporating a novel compositional approach, PEPA, we were able to effectively model and implement the performance analysis of our scheme.

Looking ahead, our future work will focus on enhancing data and identity protection in the face of threats to the RSUs. Furthermore, we recognize the importance of minimizing overhead while upholding security, which will be a significant consideration in our ongoing research. By addressing these challenges and pursuing further advancements, we aim to contribute significantly to the advancement of secure and private vehicular networking systems. Our research stands as a stepping stone towards building a safer and more trustworthy environment for vehicular data transactions and communications.

Author Contributions: Conceptualization, J.D., N.J. and X.C.; writing—original draft preparation, N.J.; supervision, J.D.; formal analysis, H.W.; writing—review and editing, N.J. and H.W.; software and validation, K.M. and L.S.; funding acquisition, H.W.; project administration, X.C. All authors have read and agreed to the published version of the manuscript.

Funding: The work of Haiqin Wu was supported by the National Natural Science Foundation of China with grant no. 62202167.

Data Availability Statement: The data and source codes are available upon request to the corresponding authors.

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

References

1. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2017**, *5*, 3701–3709. [CrossRef]
2. Chen, X.; Xue, G.; Yu, R.; Wu, H.; Wang, D. A Vehicular Trust Blockchain Framework with Scalable Byzantine Consensus. *IEEE Trans. Mob. Comput.* **2023**, 1–13. [CrossRef]
3. Zhu, H.; Wang, Z.; Yang, F.; Zhou, Y.; Luo, X. Intelligent Traffic Network Control in the Era of Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9787–9802. [CrossRef]
4. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the Internet of Vehicles: Network Architectures and Applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [CrossRef]
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN* **2019**, 1–9. [CrossRef]
6. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in Distributed Blockchain: Analysis, Requirements and Open Issues. *Future Gener. Comput. Syst.* **2019**, *100*, 325–343. [CrossRef]
7. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
8. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
9. Chen, C.; Wu, J.; Lin, H.; Chen, W.; Zheng, Z. A Secure and Efficient Blockchain-based Aata Trading Approach for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9110–9121. [CrossRef]
10. Hillston, J. A Compositional Approach to Performance Modelling. Ph.D. Thesis, University of Edinburgh, Edinburgh, UK, 1994.
11. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.L.; Zhang, J. A Reputation-based Announcement Scheme for VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 4095–4108.
12. 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]
13. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N. Blockchain-based Trust Management for Internet of Vehicles. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1397–1409. [CrossRef]
14. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust Management in Blockchain and IOT Supported Supply Chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Seoul, Republic of Korea, 14–17 May 2019; pp. 184–193.
15. Kouicem, D.E.; Imine, Y.; Bouabdallah, A.; Lakhlef, H. A Decentralized Blockchain-based Trust Management Protocol for the Internet of Things. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1292–1306. [CrossRef]
16. Chen, X. Scaling Byzantine Fault-Tolerant Consensus with Optimized Shading Scheme. *IEEE Trans. Ind. Inform.* **2023**, 1–14. [CrossRef]

17. Nilsson, D.K.; Larson, U.E.; Jonsson, E. Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes. In Proceedings of the 2008 IEEE 68th Vehicular Technology Conference, Calgary, AL, Canada, 21–24 September 2008; pp. 1–5. [CrossRef]
18. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A Secure Authentication Scheme for VANETs with Batch Verification. *Wirel. Netw.* **2015**, *21*, 1733–1743. [CrossRef]
19. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
20. Song, J.H.; Wong, V.W.; Leung, V. Wireless Location Privacy Protection in Vehicular Ad-hoc Networks. *Mob. Netw. Appl.* **2010**, *15*, 160–171. [CrossRef]
21. Ying, B.; Makrakis, D. Pseudonym Changes Scheme Based on Candidate-location-list in Vehicular Networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7292–7297. [CrossRef]
22. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1711–1720. [CrossRef]
23. Wu, H.; Wang, L.; Xue, G.; Tang, J.; Yang, D. Enabling Data Trustworthiness and User Privacy in Mobile Crowdsensing. *IEEE/ACM Trans. Netw.* **2019**, *27*, 2294–2307. [CrossRef]
24. Wang, Q.; Gao, D.; Foh, C.H.; Zhang, H.; Leung, V.C.M. Decentralized CRL Management for Vehicular Networks with Permissioned Blockchain. *IEEE Trans. Veh. Technol.* **2022**, *71*, 11408–11420. [CrossRef]
25. Fan, Q.; Xin, Y.; Jia, B.; Zhang, Y.; Wang, P. COBATS: A Novel Consortium Blockchain-Based Trust Model for Data Sharing in Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 12255–12271. [CrossRef]
26. Li, X.; Yin, X.; Ning, J. Trustworthy Announcement Dissemination Scheme With Blockchain-Assisted Vehicular Cloud. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 1786–1800. [CrossRef]
27. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1212–1239. [CrossRef]
28. Adams, C.; Lloyd, S. *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*; Sams Publishing: Indianapolis, IN, USA, 1999.
29. Merkle, R.C. A Digital Signature Based on a Conventional Encryption Function. In *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1987; pp. 369–378.
30. Rivest, R.L.; Adleman, L.; Dertouzos, M.L. On Data Banks and Privacy Homomorphisms. *Found. Secur. Comput.* **1978**, *4*, 169–180.
31. Paillier, P. Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.
32. Yuan, Y.; Wang, F.Y. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1421–1428. [CrossRef]
33. Li, W.; Song, H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 960–969. [CrossRef]
34. 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]
35. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI'99, New Orleans, LO, USA, 22 March 1999; pp. 173–186.
36. Miller, A.; Xia, Y.; Croman, K.; Shi, E.; Song, D. The Honey Badger of BFT Protocols. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS'16, Vienna, Austria, 24–28 October 2016; pp. 31–42. [CrossRef]
37. Meng, K.; Sun, L. A Decentralized Vehicle-to-Vehicle Energy Trading System Based on Efficient Sharding Services. In Proceedings of the 21st IEEE International Symposium on Parallel and Distributed Processing with Applications, Wuhan, China, 21–24 December 2023.
38. Gueta, G.G.; Abraham, I.; Grossman, S.; Malkhi, D.; Pinkas, B.; Reiter, M.; Seredinschi, D.; Tamir, O.; Tomescu, A. SBFT: A Scalable and Decentralized Trust Infrastructure. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Los Alamitos, CA, USA, 24–27 June 2019; pp. 568–580. [CrossRef]
39. Yin, M.; Malkhi, D.; Reiter, M.K.; Gueta, G.G.; Abraham, I. HotStuff: BFT Consensus with Linearity and Responsiveness. In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC'19, New York, NY, USA, 29 July–2 August 2019; pp. 347–356. [CrossRef]