



A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the Internet of Vehicles

Kashif Naseer Qureshi, Luqman Shahzad, Abdelzahir Abdelmaboud, Taiseer Abdalla Elfadil Eisa, Bandar Alamri, Ibrahim Tariq Javed, Arafat Al-Dhaqm, Noel Crespi

Publication date

01-01-2022

Published in

Applied Sciences;12, 476

Licence

This work is made available under the [CC BY-NC-SA 1.0](#) licence and should only be used in accordance with that licence. For more information on the specific terms, consult the repository record for this item.

Document Version

1

Citation for this work (HarvardUL)



Naseer Qureshi, K., Shahzad, L., Abdelmaboud, A., Abdalla Elfadil Eisa, T., Alamri, B., Javed, I.T., Al-Dhaqm, A. and Crespi, N. (2022) 'A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the Internet of Vehicles', available: <https://hdl.handle.net/10344/10959> [accessed 25 Jul 2022].

This work was downloaded from the University of Limerick research repository.

For more information on this work, the University of Limerick research repository or to report an issue, you can contact the repository administrators at ir@ul.ie. If you feel that this work breaches copyright, please provide details and we will remove access to the work immediately while we investigate your claim.

Article

A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles

Kashif Naseer Qureshi ¹, Luqman Shahzad ¹, Abdelzahir Abdelmaboud ², Taiseer Abdalla Elfadil Eisa ², Bandar Alamri ³, Ibrahim Tariq Javed ^{1,*}, Arafat Al-Dhaqm ^{4,5} and Noel Crespi ⁶

¹ Department of Computer Science, Bahria University, Islamabad 44000, Pakistan; knaseer.buic@bahria.edu.pk (K.N.Q.); luqmanshahzad93@gmail.com (L.S.)

² Department of Information Systems, College of Science and Arts, King Khalid University, Muhayil Asir 61913, Saudi Arabia; aelnour@kku.edu.sa (A.A.); Teisa@kku.edu.sa (T.A.E.E.)

³ Lero-The Irish Software Research Centre, University of Limerick, V94 T9PX Limerick, Ireland; Bandar.Alhamri@ul.ie

⁴ School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Skudai 81300, Malaysia; mrrarafat1@utm.my

⁵ Department of Computer Science, Aden Community College, Aden 8916862, Yemen

⁶ Institut Polytechnique de Paris Telecom SudParis Evry, Courcouronnes FR, 9 Rue Charles Fourier, 91000 Evry, France; noel.crespi@mines-telecom.fr

* Correspondence: itariq.buic@bahria.edu.pk



Citation: Qureshi, K.N.; Shahzad, L.; Abdelmaboud, A.; Elfadil Eisa, T.A.; Alamri, B.; Javed, I.T.; Al-Dhaqm, A.; Crespi, N. A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles. *Appl. Sci.* **2022**, *12*, 476. <https://doi.org/10.3390/app12010476>

Academic Editors: Paula Fraga-Lamas and Gianluca Lax

Received: 3 October 2021

Accepted: 16 December 2021

Published: 4 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: The rapid advancement in the area of the Internet of Vehicles (IoV) has provided numerous comforts to users due to its capability to support vehicles with wireless data communication. The exchange of information among vehicle nodes is critical due to the rapid and changing topologies, high mobility of nodes, and unpredictable network conditions. Finding a single trusted entity to store and distribute messages among vehicle nodes is also a challenging task. IoV is exposed to various security and privacy threats such as hijacking and unauthorized location tracking of smart vehicles. Traceability is an increasingly important aspect of vehicular communication to detect and penalize malicious nodes. Moreover, achieving both privacy and traceability can also be a challenging task. To address these challenges, this paper presents a blockchain-based efficient, secure, and anonymous conditional privacy-preserving and authentication mechanism for IoV networks. This solution is based on blockchain to allow vehicle nodes with mechanisms to become anonymous and take control of their data during the data communication and voting process. The proposed secure scheme provides conditional privacy to the users and the vehicles. To ensure anonymity, traceability, and unlinkability of data sharing among vehicles, we utilize Hyperledger Fabric to establish the blockchain. The proposed scheme fulfills the requirement to analyze different algorithms and schemes which are adopted for blockchain technology for a decentralized, secure, efficient, private, and traceable system. The proposed scheme examines and evaluates different consensus algorithms used in the blockchain and anonymization techniques to preserve privacy. This study also proposes a reputation-based voting system for Hyperledger Fabric to ensure a secure and reliable leader selection process in its consensus algorithm. The proposed scheme is evaluated with the existing state-of-the-art schemes and achieves better results.

Keywords: IoV; authentication; security; blockchain; privacy; network; latency; scalability

1. Introduction

Internet of Vehicles (IoV) networks are able to improve driving safety, efficiency, and traffic management using On-Board Units (OBUs) for data communication, with or without prior infrastructure. As a result of the increase in the number of users and the open nature of these networks, security threats are a challenge. Security requirements such as

authentication, the privacy of vehicle nodes, and audibility are necessary to avoid these networks from different types of attacks, such as impersonation attacks, and spreading of false information. Authentication of nodes in a network is the first line of defense to block any unwanted activity in a network [1,2]. If the network allows unauthenticated vehicle nodes, then malicious vehicle nodes can also join the network and undertake different types of activities, e.g., impersonate an ambulance to exceed the given speed limits. If integrity is not provided during message transmission, then vehicle nodes can misbehave and alter the content of a message. In such a case, the receiver only knows that the message was sent by a legitimate vehicle, and they would be responsible for any damage. Privacy is a core feature of IoV, but traceability is also necessary in the case of any unwanted activity in a network. In this case, the privacy of the vehicle should be revoked and punished.

Existing solutions of IoV are vulnerable to and suffer from various privacy threats. Due to this loophole, many fake messages may be delivered, resulting in numerous victims. The conventional security solutions are based on a centralized approach, which necessitates a trusted central authority and faces a single point of failure. This potential also exposes different security and privacy attacks such as hijacking and unauthorized tracking of vehicle nodes' locations. These solutions do not guarantee timely notification [3]. Another example is the broadcasting of fake information by an intruder to mislead or confuse other vehicle nodes in the network. Hence, ensuring the authentication, non-repudiation, authenticity, and traceability of messages in IoV is crucial. Vehicle privacy is also another critical challenge because a vehicle's sensitive information, such as its location and identity, should not be revealed to other nodes in the network. Conditional privacy can prevent vehicles misbehaving, via tracing and penalizing by one or many entities. Although users normally trust a third party to check the legitimacy of their transactions before bringing them into effect, a middle party may be suspected of cheating its customers. Currently, conventional security and trust methods used in smart vehicles are ineffective due to many challenges, such as inefficient communication among the vehicles, centralization, insecure communication, and untraceability of malicious nodes.

To address these issues, blockchain is one of the most promising technologies, in which an agreement called a "consensus algorithm" is shared among all entities that want to add their proposed blocks. In a blockchain, algorithms enable the different users to agree on the current state, even if they do not trust each other or there is no central authority between them. To address vehicle data-sharing issues, blockchain creates a safe, trustworthy, and decentralized intelligent transportation ecosystem [4]. Blockchain is a form of decentralization in which transactions are registered through a peer-to-peer network rather than relying on a centralized authority and centralized server. Therefore, the system is able to run without interruption in the case of any single point failure. Every entity in a network maintains the same copy of the digital ledger. If the ledger is public, it provides all the information in the ledger to all the members of the network [5]. Another exciting feature of blockchain is immutability, which ensures that anything committed on the ledger cannot be altered or changed. This is in contrast to the conventional system. Each entity in a network has a copy of the ledger. Before any information is committed to the ledger, it is first validated by the nodes. If the transactions pass the validation process undertaken by the majority of the nodes, then the transactions will be added to the ledger [6,7]. This core feature of blockchain ensures transparency. It is impossible to reverse or change the hash. If a single change is made to the input, then the hash is generated completely differently. In order for a malicious node to corrupt the data in the network it must change the data stored in the ledger on every node. This is highly complex if the network consists of millions of nodes and each node has the same digital copy of the ledger. Each transaction in a blockchain network is stored and a hash of the block is recorded in the next block to trace the transaction and ensure transparency.

The main existing privacy-preserving strategies and solutions for blockchain are identified in this paper, to provide insight into the different cryptographic primitives and privacy-preserving approaches, methods, and techniques used in blockchain. This paper

proposes an efficient, secure, decentralized Conditional Privacy-Preserving and Authentication (CPPA) scheme for IoV networks. The proposed scheme is based on Hyperledger Fabric for the selection of leaders in the consensus algorithm. It also provides traceability and anonymity ensure that authorities can trace the vehicle nodes in case of disputes. Hyperledger Fabric is an open source blockchain developed by Linux foundation. Hyperledger is a permissioned blockchain technology in which all participants are identified and authenticated. Hyperledger allows the execution of smart contracts which are called chaincodes. Most importantly, it ensures privacy by facilitating confidential transactions.

The main contributions of this paper are as follows:

- The proposed scheme handles multiple transactions at once and provides scalability by using blockchain technology.
- The scheme provides multiple decentralized trusted authorities and avoids the issue of a single point of failure in traditional networks.
- The scheme provides feature traceability for malicious node detection

The remainder of this paper is organized as follows: Section 2 presents a review of the relevant literature. Section 3 presents an efficient, secure, decentralized, and conditional privacy and authentication scheme for IoV. Section 4 illustrates the results and provides a discussion. The last section concludes the paper with possible future directions.

2. Related Work

The authors in [8] proposed a Conditional Privacy-Preserving Authentication (CPPA) scheme for vehicular ad hoc networks that uses Schnorr's signature. The secret key is pre-loaded on the vehicle but a long-term secret key can be accessed by an adversary when it has physical access. In another study [9], the authors presented an Efficient, Anonymous Authentication with Conditional Privacy (EAAP) scheme based on a bilinear pairing technique, using anonymous certificates that are valid for short-term and public keys for IoV. In [10], the authors presented secure authentication solution for authentication, integrity, and confidentiality. Traceability depends on a Trusted Authority (TA). If the TA is compromised, then the entire network is disrupted. The authors in [11] presented a scheme based on blockchain to protect the security and privacy of vehicle nodes. The authors proposed a Lightweight Scalable Blockchain (LSB), without traceability of the malicious vehicle nodes. The approach uses an Overlay Block Manager (OBM), which acts as a cluster head. It also did not provide batch verification or batch authentication. The proposed model is also affected by the issues of key management, caching data, and mobility. In [12], the authors briefly described a model which has three layers: perception, service, and edge computing. It ensures the security of vehicle nodes through blockchain technology. It also offers computing capabilities and cloud services. The authors in [13] proposed blockchain-based IoV and proposes an authentication and secure data transfer algorithm. However, it does not provide traceability, batch verification, or authentication. In [14], the authors proposed a secure information sharing scheme for IoV based on blockchain. The authors achieved conditional privacy using threshold secret sharing and fair-blind signatures.

The authors in [15] presented a seven-layer architecture for transportation systems. This paper also presented delegated proof-of-stake (DPOS), which is appropriate for vehicular communication because it establishes blockchain-based vehicular networks. The authors in [16] presented a distributed trust management scheme for a clustering mechanism for IoV based on blockchain technology. In this paper, block validation is performed by proof of work and roadside units function as miners performing POW for the consensus mechanism. In [17], the authors proposed a Byzantine fault tolerance consensus algorithm for IoV. This algorithm provides a privacy-preserving incentive announcement network. By using reputation points, this announcement mechanism allows vehicle nodes to forward and collect accurate information. However, this consensus scheme faces limited scalability. The authors in [18] proposed a reputation-based data sharing scheme using a subjective logic model to improve data integrity and provide a secure data exchanging system in vehicular communication. In this paper, proof of work is utilized for exchanging infor-

mation, auditing, and verification of the record. To encourage vehicle nodes, a scheme named proof-of-storage is also presented to allow and incentivize vehicles to share storage resources. An updated DPOS consensus algorithm for reliable reputation management is proposed in [19]. The authors used a multi-weight subjective logic model and contract theory to prevent internal collision among miners. The authors in [20] recognize the difference between correct and fake transactions. In addition to increasing accuracy, this recognition prevents double-spending problems in which someone may be able to create multiple correct transactions and thus combine them to create a fraudulent transaction. The third phase is the latency of the system and computing power, which is needed to enable the correctness and agreement processes.

The authors in [21] adopted the properties of the POS algorithm and included additional security measures. The algorithm focuses on two properties, namely, persistence and liveness. Persistence indicates that, if a node in a network declares a specific transaction as being stable, then all the remaining nodes will report it as stable, but only if they are responding honestly. Liveness states that the transaction will be stable when an honestly generated transaction is available to the nodes in a network for a significant amount of time. To ensure the randomness of a leader in an election process, the algorithm employs the coin-flipping protocol. In [22], the authors proposed an Efficient Threshold Anonymous Authentication (ETAA) protocol for VANETs. This protocol uses a group signature and a decentralized group model, and the threshold authentication method, to obtain threshold authentication, efficient revocation, unforgeability, anonymity, and traceability for VANETs. The group signature strategy uses independent interest to provide traceability and linkability.

The authors in [23] proposed a metaheuristic algorithm for anomaly detection in IoT networks using an activity footprint-based method. This algorithm captures the semantic context and high dimensional vectors, which are assigned to the mobile agents. The isolated agents are monitored for abnormal activities and can be associated with potential intruders. The proposed algorithm was tested in a simulation environment to confirm and validate the metaheuristic algorithm. However, this algorithm was designed for IoT networks where the movement of the devices is not as fast as those in IoV networks. These types of solutions are not feasible for IoV networks. The authors in [24] presented a hybrid method for anomaly detection using metaheuristic methods for high speed networks. The hybrid method uses large scale datasets and detector generation based on multi-start metaheuristic and genetic methods. The proposed method achieved accuracy of 96.1% with machine learning algorithms. However, this method was designed for fixed networks and is not feasible for ad hoc networks such as IoV.

3. Design and Development of Blockchain-Based IoV

In this section, we present an efficient, secure, decentralized, and anonymous network model for IoV to overcome the above limitations. The proposed scheme provides traceability to identify malicious vehicle nodes. The proposed reputation scheme is based on the Hyperledger Fabric leader selection process. The scheme also satisfies the security and authentication requirements.

3.1. Network Model

The proposed scheme uses the Fabric Certificate Authority (CA) for the registration of identities. It has sufficient capabilities, such as high computation, fast communication, and enough storage. CA is also responsible for the generation of certificates for vehicles and roadside units. Additionally, once their registration is complete, the TA produces the initial security parameters for all vehicles and roadside units (RSUs), and sends them to the vehicles via TLS. Issuance of Enrollment Certificates (ECerts) is an enrollment process whereby the Fabric CA issues a certificate key-pair, comprised of a signing certificate and a private key that forms the identity [25]. The private and public keys are first generated locally by the Fabric CA client, and then the public key is sent to the CA,

which returns an encoded certificate, the signing certificate for certificate renewal, and revocation. Orderers are stationary nodes deployed on the roadside. These orderers act as the RSUs. The orderer maintains the list of the organizations that can create and configure the channel, and are responsible for ordering and packaging the transactions. The orderer also obtains the certificates that represent identities, and the Membership Service Provider (MSP) contains the permission identities. The orderer utilizes a dedicated short-range communication protocol for V2V and V2R wireless communications. The MSP authenticates traffic messages from vehicles and processes them locally or forwards them to the TA. The law enforcement department may request the CA to revoke the real identity of the message sender if malicious activity is detected. Vehicle nodes are embedded with high processing, storage, and wireless communication modules. The vehicle-to-vehicle and vehicle-to-RSU communications are conducted through wireless networks. Figure 1 shows the layers of the proposed solution.

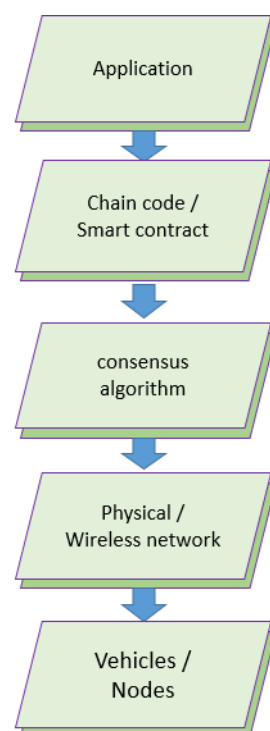


Figure 1. Layers of the proposed network.

Figure 1 shows the different layers of the proposed network, comprising the application layer, chain code/smart contract layer, consensus layer, physical/wireless network, and the ground vehicular nodes. Smart contracts are blockchain based programs that execute when certain criteria are met. The contracts are decentralized applications that respond to events by executing business logic. These are often used to automate contract execution so that all parties immediately know the outcome without the need for any intermediaries.

3.2. Enhanced Hyperledger Fabric

Vehicles with OBU and digital networking equipment are blockchain-based IoV to communicate with neighboring RSUs, to thus access vehicular networks. The OBU performs basic functions, collects local data, and sends it to the orderer via a communication channel. Vehicle nodes work as information providers and provide their information to data requesters. Vehicle nodes send their messages to the neighboring orderer. Orderers are stationed along roads to ensure that cars can connect with orderers. Orderers are roadside nodes that are stationary. According to their locations, the entire network is split into several regions. Without the help of a trustworthy third party, a group of auditors has the

secret tracing key. If malicious conduct is discovered, the law enforcement department can request that group auditors revoke the true identity of the message. To retrieve the real identity of the sender, at least 't' tracers must work together. This is used to prevent misuse of power. We should mention that the CA and vehicle nodes in the scheme elect the issuers and auditors. The steps of the proposed scheme are system configuration, registration enrollment process, transaction handling, consensus process, ledger update, and traceability.

3.2.1. System Configuration

Because the certificates associated with a node must be generated before the node itself can be implemented, the first part that must be installed in the network to configure the device is a CA. After passing identity verification by the CA, any entity appears to be valid. It is not mandatory to use the Fabric CA for certificate generation. However, it is used in the current proposal because it produces MSP directories, which are required for organizations and entities to be properly defined; otherwise, we must create the MSP directories ourselves. We check that CAs are deployed in our network. All the intermediate CA's will be created by a single root CA. Intermediate CAs are an effective means of preventing the root CA from being overworked. We use a dual-headed CA consisting of a TLS CA, which necessitates setting up (1) a TLS CA and using it to create TLS certificates; and (2) an organizational CA, which is used to generate admin certificates for an entity, the MSP, and the nodes owned by that organization. For the state database, we use the Level DB because we prioritize speed. All the peer nodes on the channels are required to utilize the same state database (CouchDB or Level DB). To maintain anonymity and isolation for such transactions, channels are deployed depending on the geographical area. After the CA has been configured, it can be utilized to register and enroll vehicles. The administrator of the CA assigns a username and password for the vehicle in the first stage. The vehicles are also granted roles and associations. It now builds a directory known as an MSP, which includes the public certificate of the CA granting the certificate in addition to the CA's root of trust. The vehicle is registered and enrolled in both an 'Enrollment CA' and a 'TLS CA', much like an admin identity. The CA assigns the function of orderer or peer, rather than admin, when registering the vehicle. Peers and orderers who are owned by different organizations are now deployed; thus, these organizations are called peer organizations and orderer organizations. These organizations are connected, and smart contracts, where ledgers are stored, are installed on both peers and orderers.

3.2.2. Registration and Enrollment

In the registration and enrollment phase, when any vehicle wants to connect to the network for the first time, it requires registration from the CA. The CA generates a public/secret key-pair and sends credentials to the vehicle through TLS after verifying the information's identity. The CA stores public keys on its database. This database can be checked to determine if a car is registered in the network by looking up the public key of the vehicle in the database. The association between the public key (pk) and the vehicle's identification details is known only to the CA. Any vehicle in each area can register in the same regions in the intermediate CA. The Fabric CA automatically functions as an Idemix issuer. When the CA is started with the "init" command, two files are generated in the CA's home directory: "IssuerPublicKey" and "IssuerRevocationPublicKey". The Idemix MSP is created using these keys. When an Idemix credential is being used, the Client-Identity library is used to help the GetAttribute-Value feature. The peers only use Idemix MSP for signature authentication. Only the Client SDK is used to sign with the Idemix MSP.

3.2.3. Transaction Handling

After setting up and executing the channel, the system ensures that vehicles undergo the registration and enrollment phase with the CA and have cryptographic identities that are known for their authentication. The system also checks that the chain code is already

written on all the vehicles and activated on the channel. The chain code is also given an endorsement scheme which requires that all the vehicles must endorse the message transaction. Let us suppose that vehicle (VA) wants to share the message to all the vehicles in that channel. In the first phase, VA initiates a transaction message (for example: about the road condition). A request is submitted in the channel by targeting all vehicles. Then, a transaction proposal is created. To create a transaction proposal, the vehicle uses a supported SDK. The proposal enables a chain code to be invoked with certain input parameters to read or update the ledger. The SDK envelopes the proposal of the message into a particular format and uses the user's account details to create a unique signature for it. The endorsement policy defines that all vehicles must endorse the transaction; hence, the request goes to all vehicles. Then, the endorsing vehicles verify that the transaction proposal has not been previously sent, to prevent a replay attack, and also check whether the signature is valid by using the MSP. Additionally, they confirm that the sender can execute this process on the channel. The transaction proposal inputs are transferred to the invoked chain codes by the endorsing vehicles. The chain code is run with Level DB to generate output that includes the answer-value, read-set, and write-set. At this point, ledgers are not updated. All of these values, in addition to the signatures of the endorsing vehicles, are returned as a proposal reply to VA.

In the next phase, the sender verifies the signatures of all endorsing vehicles and ensures that the proposal responses from all the vehicles are the same. It verifies that the specified endorsement rules are achieved before submission. If the sender does not inspect responses and forwards messages without endorsement, then the endorsement rules are still imposed by other vehicles in the channel and upheld at the "commit validation phase". After verifying the responses and updating the ledger, it sends a message to the RSU (ordering service). The message proposal and endorsing reply are then bundled into a message and sent to the RSU by VA. The OS does not need to search the whole content of the message; however, it simply orders all of the transactions received from the channels, and generates blocks of transactions for each channel. In the next phase, the transaction blocks are delivered by OS to all vehicles on that channel. The endorsement rules are verified by validating the message within the block. The block's transactions are classified as "valid" or "invalid". Each vehicle adds the block to the channel's chain and, if the transactions are valid, then write sets are committed to Level DB. Each vehicle notifies VA that the message has been added to the chain, and whether the message was validated. Figure 2 shows the flow diagram of the enhanced Fabric.

3.2.4. Consensus Process

The Raft consensus protocol in Hyperledger Fabric utilizes the "leader and follower" model in which a channel's ordering nodes dynamically elect a leader, and that leader forwards data to all of its followers. Because the network can tolerate the failure of nodes, including leader nodes, because several ordering nodes exist, Raft is called "Crash Fault Tolerance". For instance, if a channel has five vehicles, it can afford the loss of two vehicles. This feature of Raft provides a high-availability strategy for the ordering service. RSUs are in different locations and, if any RSU or the entire location becomes unavailable, then RSUs in other locations will continue to operate. The ordering nodes that are actively involved in the consensus process for a given channel are referred to as the "consenter set". The quorum is the minimum number of consenter who agree to a proposal to serialize the transactions.

Leader, follower, and candidate are the three possible states for the RSU. The RSU is initiated as a follower. It may approve logs from the leader or vote for the leader selection at this time. If there are no logs or heartbeats obtained for a specific amount of time, then it will be self-promoted to the candidate state. In this stage, it will request votes from other RSUs. It will be appointed a leader if it earns a quorum of votes. The leader RSU oversees generating new logs, sending these logs to follower RSUs, and determining whether logs are committed.

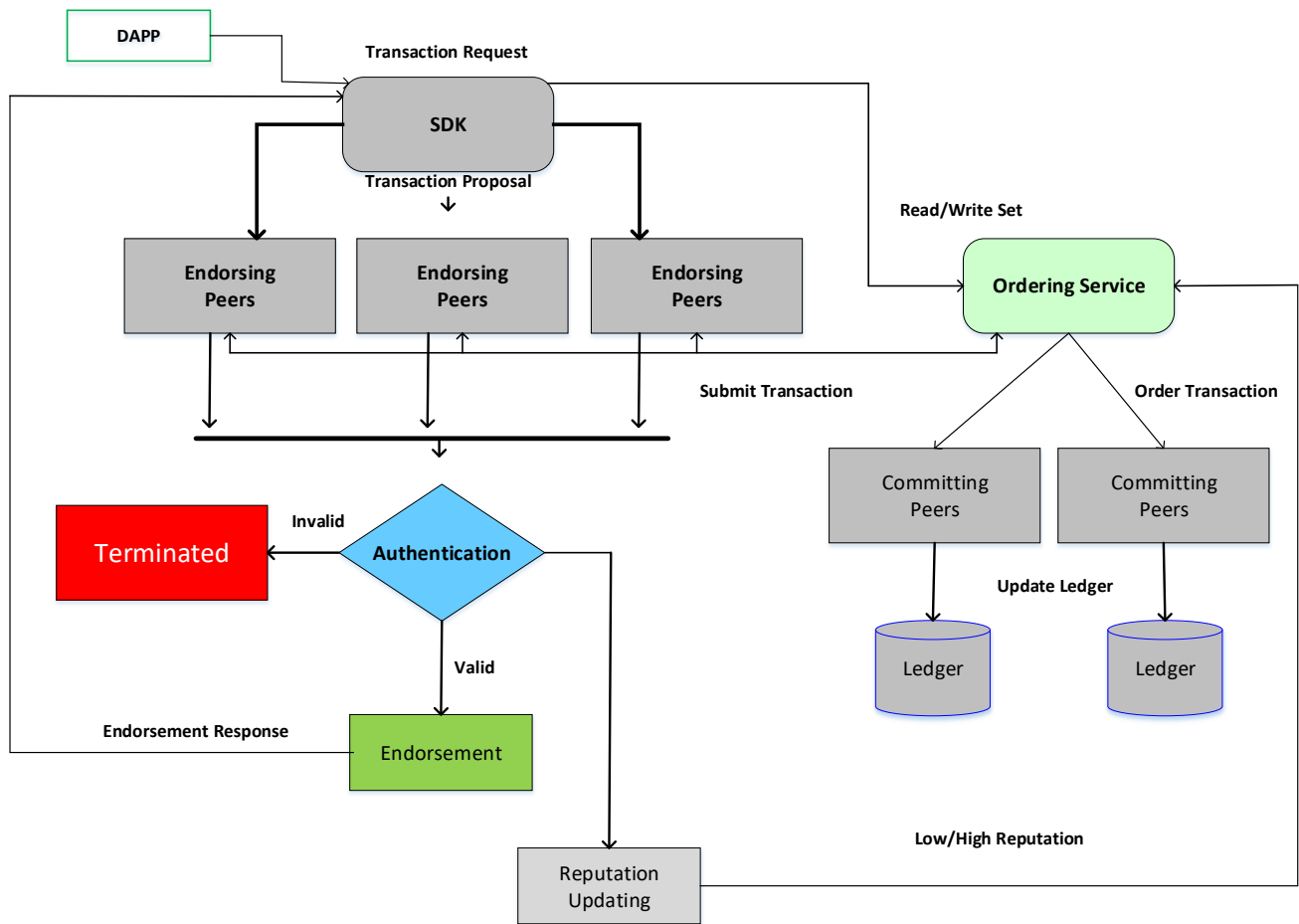


Figure 2. Flow diagram of enhanced Fabric.

3.2.5. Calculating and Updating Reputation

RSUs can calculate the reputation of all members in the ordering service. This is focused on previous experiences, in addition to new recommendations from the vehicles. To form the local opinion on each RSU, the model considers three weights based on previous experiences. The vehicular blockchain contains the most recent recommended opinions. To receive a final reputation on each RSU, each vehicle computes its local and recommended opinions. Vehicles update and review a current data block for that round of the consensus mechanism. If the information is accurate, vehicles upgrade their reputation opinions for the RSU and send their opinions to OS. The RSUs work together to apply legitimate reputation values to the vehicular blockchain through a consensus mechanism. The following security study should be used to solve the concerns of the vulnerable leader in the proposed scheme: reputation is utilized to select the RSU to indicate the trustworthiness of nodes by considering their past behaviors. A high-reputation RSU is chosen as the leader. Hence, the leader is trustable, and there is a very small chance that it will damage the system. This leader is selected for a time slot because, if a leader is compromised and tries to harm the system, then it can only harm the system in its time slot. The endorsing vehicles can also check for mistakes in the block data on the vehicular blockchain during the validation and commit phase. Then, the leader is accused and blacklisted. Figure 3 shows the blockchain-based IoV.

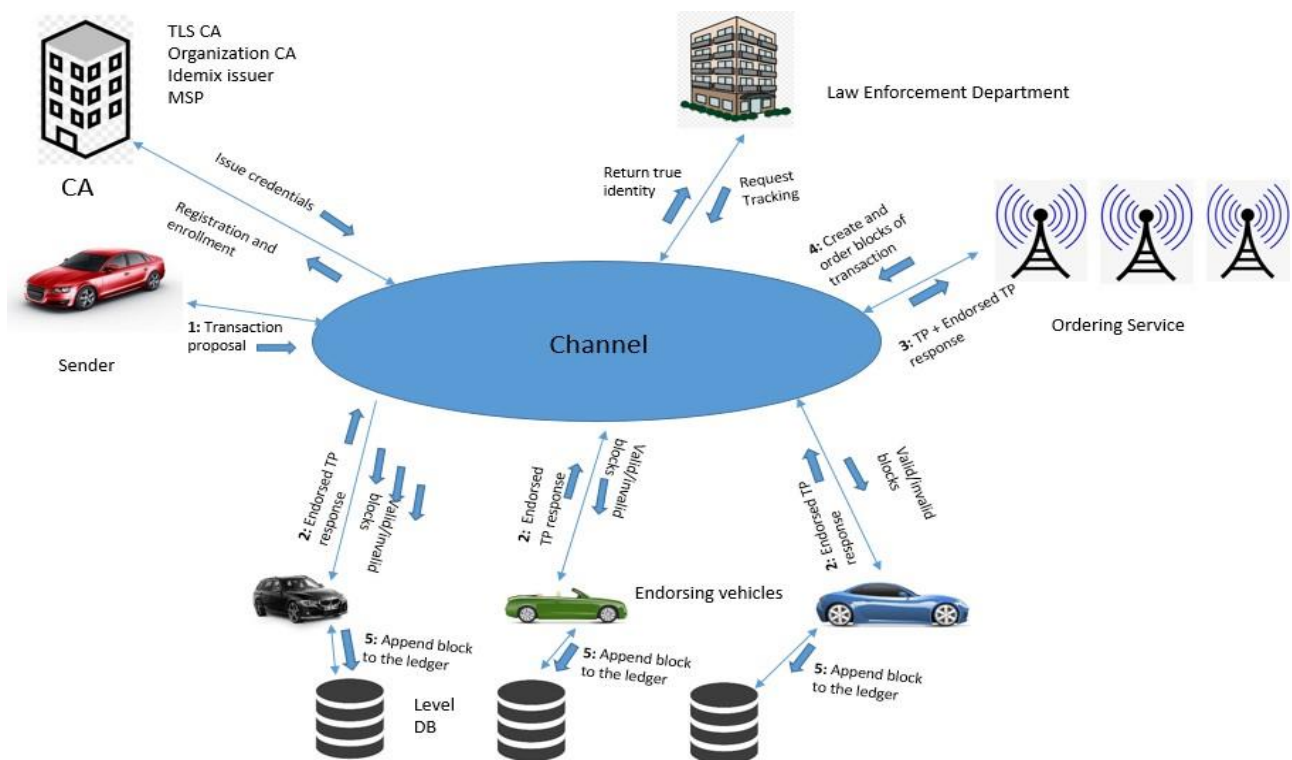


Figure 3. Blockchain-based IoV.

3.2.6. Local Opinions for Ordering Services

Suppose a peer (V_i) and an ordering service (RU_j) interact with each other. The vector defined for the local opinion of V_i to RU_j is $\omega_{i \rightarrow j} := b_{i \rightarrow j}, d_{i \rightarrow j}, u_{i \rightarrow j}, k_{i \rightarrow j}$ where $b_{i \rightarrow j}$ represents trust, $d_{i \rightarrow j}$ represents mistrust, $u_{i \rightarrow j}$ represents uncertainty, and $k_{i \rightarrow j}$ is a constant which shows a willingness to trust ordering services and is less than 1 (0.5). The values of $b_{i \rightarrow j}, d_{i \rightarrow j}, u_{i \rightarrow j}$, in addition to the relationships between them, are particularly important. Hence, $b_{i \rightarrow j}, d_{i \rightarrow j}, u_{i \rightarrow j} \in \{0,1\}, b_{i \rightarrow j} + d_{i \rightarrow j} + q_{i \rightarrow j} = 1$.

$$\begin{cases} u_{i \rightarrow j} = 1 - q_{i \rightarrow j} \\ b_{i \rightarrow j} = (1 - u_{i \rightarrow j}) \frac{\alpha_i}{\alpha_i + \beta_i} \\ d_{i \rightarrow j} = (1 - u_{i \rightarrow j}) \frac{\beta_i}{\alpha_i + \beta_i} \end{cases}$$

α_i and β_i are the number of good and bad experiences, respectively. $q_{i \rightarrow j}$ is the communication quality of a link between vehicle i and RSU_j . The reputation according to $\omega_{i \rightarrow j}, x_{i \rightarrow j}$ denotes the expected trust of vehicle V_i that RSU is trustworthy and behaves appropriately throughout a consensus period, represented as $x_{i \rightarrow j} = b_{i \rightarrow j} + k_{i \rightarrow j} u_{i \rightarrow j}$.

3.3. Multi-Weight Local Opinions for Subjective Logic

Different dynamics affect local opinions by utilizing the subjective logic model [26]. Both reputation logics are handled similarly in standard subject logic. However, different reputation logics originating from different sources must be weighted correctly to be aggregated with greater precision. If the vehicle has existing experience of, and maintains more recent ratings for, the RSU , the accuracy of the reputation will be significantly improved. Regarding weighting operations, this model progresses into “multi-weight subjective logic”. We use the following weights.

3.3.1. Rate of Experiences

The rate of experiences shows how much the vehicle knows about RSU . If the rate of experience is large, it indicates that the vehicle (VA) knows a significant amount about

RSU_j. The ratio of the number of times that vehicle (VA) communicates with RSU (RSU_j) to the total amount of times that the vehicle communicates with other RSUs during some time 'T' is the rate of experiences between them.

$$f_{i \rightarrow j}^i = \frac{M_{i \rightarrow j}}{\overline{M}_i} \tag{1}$$

where $M_{i \rightarrow j} = (\alpha_i + \beta_i)$, and $\overline{M}_i = \frac{1}{|Q|} \sum_{q \in Q} M_{i \rightarrow q}$. Q is the ordering service (group of RSUs) interacting with vehicle V_i during the time window. A high rate of experience indicates a high reputation value.

3.3.2. Recent Experiences

In IoV, the more recent experiences are given a higher weight to the RSU, which may not always be trustworthy and secure because widely spread RSUs can be vulnerable to a breach due to insufficient protection. Both the trustworthiness and reputation of V_i to Ru_j are continually changing. For local opinions, recent and past experiences have different weights. The parameters γ and δ indicate the weights of recent and past experiences, respectively. $\gamma + \delta = 1$, whereas $\gamma > \delta$.

3.3.3. Experience Effects

If the RSU has good experiences, this will increase the RSUs' reputation, and if it has/had bad experiences, it will decrease the RSU's reputation. As a result, bad experiences had a greater effect on local vehicle opinions than good experiences. Good experiences have a weight of μ , and the weight of negative interactions is ν , where $\mu + \nu = 1$, $\mu < \nu$. The weights of recent experiences and experience effects are coupled to create a new experience frequency:

$$\alpha_i = \gamma\mu\alpha_1^i + \delta\mu\alpha_2^i, \beta_i = \gamma\nu\beta_1^i + \delta\nu\beta_2^i \tag{2}$$

α_1^i and β_1^i are good and bad recent experiences with time t , which satisfies $t \leq t_r$. If $t > t_r$, α_2^i and β_2^i are good and bad past experiences, respectively. Hence the updated rate of experience from V_i to RU_j is:

$$f_{i \rightarrow j}^i = \frac{M_{i \rightarrow j}}{\overline{M}_i} = \frac{\mu(\gamma\alpha_1^i + \delta\alpha_2^i) + \nu(\gamma\beta_1^i + \delta\beta_2^i)}{\frac{1}{|q|} \sum_{q \in Q} M_{i \rightarrow q}} \tag{3}$$

As a result, for local opinions, the total weight of reputation is $\sigma_{i \rightarrow j} = \tau_i * f_{i \rightarrow j}^i$, whereas the parameter of the pre-defined weight is $0 \leq \tau_i \leq 1$.

3.4. Recommended Opinions for Ordering Services

Recommended opinions and common opinions are combined as:

$$\omega_{y \in j}^r := b_{y \in j}^r, d_{y \in j}^r, u_{y \in j}^r \tag{4}$$

$$\begin{cases} b_{x \rightarrow j}^r = \frac{1}{\sum_{y \in Y} \sigma_{x \rightarrow j}} \sum_{y \in Y} \sigma_{y \rightarrow j} b_{y \rightarrow j} \\ d_{x \rightarrow j}^r = \frac{1}{\sum_{y \in Y} \sigma_{x \rightarrow j}} \sum_{y \in Y} \sigma_{y \rightarrow j} d_{y \rightarrow j} \\ u_{x \rightarrow j}^r = \frac{1}{\sum_{y \in Y} \sigma_{x \rightarrow j}} \sum_{y \in Y} \sigma_{y \rightarrow j} u_{y \rightarrow j} \end{cases} \tag{5}$$

Here, $y \in Y$ is another group of vehicles which have had experience with RU_j . Taking opinions from different vehicles and combining them is known as a recommended opinion.

3.5. Combination of Local Opinions and Recommended Opinions

When vehicles obtain the recommended opinion from other vehicles of RSU_j based on their experience with them, the vehicle will use its local opinion to create the final reputation opinion, $\omega_{i \rightarrow j}^f := b_{i \rightarrow j}^f, d_{i \rightarrow j}^f, u_{i \rightarrow j}^f$ where

$$\begin{cases} b_{i \rightarrow j}^f = \frac{b_{i \rightarrow j}^r u_{y \rightarrow j}^r + b_{y \rightarrow j}^r u_{i \rightarrow j}^r}{u_{i \rightarrow j}^r + u_{y \rightarrow j}^r - u_{y \rightarrow j}^r u_{i \rightarrow j}^r} \\ d_{i \rightarrow j}^f = \frac{d_{i \rightarrow j}^r u_{y \rightarrow j}^r + d_{y \rightarrow j}^r u_{i \rightarrow j}^r}{u_{i \rightarrow j}^r + u_{y \rightarrow j}^r - u_{y \rightarrow j}^r u_{i \rightarrow j}^r} \\ u_{i \rightarrow j}^f = \frac{u_{i \rightarrow j}^r u_{y \rightarrow j}^r + u_{y \rightarrow j}^r u_{i \rightarrow j}^r}{u_{i \rightarrow j}^r + u_{y \rightarrow j}^r - u_{y \rightarrow j}^r u_{i \rightarrow j}^r} \end{cases} \quad (6)$$

Therefore, the final reputation opinion of VA to RSU_j is $T_{i \rightarrow j}^f = b_{i \rightarrow j}^f + \gamma \mu_{i \rightarrow j}^f$. These reputations are utilized for leader selection in the ordering service. The RSU with the highest reputation is selected as a leader in Hyperledger Fabric.

4. Experiment Setup and Results

Hyperledger Fabric was selected for the implementation of blockchain-based IoV. The designed network consists of three categories including peer nodes, ordering services, and law enforcement departments. First, we selected the database for Fabric, and selected the Level database (DB) for the state database. After selecting the database and organizations, the dual-headed certificate was adopted as the authority that involves two CAs. One TLS CA is responsible for secure communications and generating TLS certificates. The other CA is an organizational CA, which is responsible for generating the admin certificates of an organization. After deployment of CAs, the channels are deployed and configured for the privacy of transactions, so that members on the other channels cannot access the transactions. The use of firewalls is also necessary for the deployment of IoV because nodes that belong to an organization can require access to other organizations; thus, there is a need for the configuration of advanced networking. The docker is deployed for peer nodes and other entities on the laptop. Then, the volumes are mounted for external entities where the entities are placed. Due to limited space, we used one channel. Nonetheless, the resources must be monitored to ensure that there is sufficient space for the blockchain and the database. In Hyperledger Fabric, CA is the first entity that must be deployed because the certificates of the nodes must be created before creation of the nodes themselves to identify who is the admin of this node.

The dual-headed CA is used based on different geographical locations. One CA is used for the MSP of the organization for enrollment of any node that is owned by that organization. This is also called the enrollment CA because it is responsible for enrolling nodes in the network. The other CA generates Transport Layer Security (TLS) certificates to secure communications. This CA is also known as a "TLS-CA". These certificates avoid attacks such as man in the middle attacks. Certificates of "intermediate" CAs are issued by a "root CA" or another intermediate CA that responds to a root CA. Intermediate CAs are useful because if the root CA is compromised then the entire network, including admins and peers, can be damaged. Then, Lightweight Directory Access Protocol (LDAP) is configured to manage identities. For three organizations, it is recommended to use at least three dual-headed CAs. One CA is responsible for ordering services, one CA is responsible for peers, and one CA is responsible for auditing departments.

After creating the CAs, we can create certificates for the identities using these certificates. It is important to first register the admin before enrolling it. Creating the MSP is also necessary. The CA's admin will issue a username and password for the entity. After being issued to the identity, these credentials can be used for enrollment. Two certificates are generated by the CA. One public certificate is used by other members, and the private certificate is used to sign messages and identities. The CA generates the Membership Service Provider (MSP). This is a set of folders that contains the CA's public certificate and

root of trust for the CAs. MSPs assign roles to the identities, i.e., the node is either a peer node, an orderer node, or a CA. The MSP is created after the creation of the node identity. After configuring the CAs and MSPs, peers and ordering nodes must be deployed. There are different ways to deploy the nodes but the configuration file must be configured before deployment. The peer's configuration file is called "core.yaml", and that of ordering nodes is "orderer.yaml". The roles of peers and orderers must be understood before deployment. The main difference between them is that the channel's "ordering service" comprises nodes that function together to form the OS.

4.1. Performance Evaluation and Results

In the performance and evaluation phase, we tested the proposed model with existing models and evaluated the efficiency regarding different performance parameters. The performance parameters were used to evaluate the proposed architecture and were helpful in generating the results. We used MATLAB for performance and evaluation.

4.2. Security and Privacy Analysis

High-availability systems span multiple global networks. Although firewalls and physical security measures are used, it is essential that those networks are secured and do not allow an attacker to attack a vehicle's data. The compromised server cannot be used to compromise other parts of the system. Hence, some schema is needed to create trust between the vehicles in the network. The proposed system supports secure communication among vehicles using TLS. Vehicles can assign their cryptographic operations to a Hardware Security Module. This secures the secret keys and executes cryptographic functions, enabling vehicles and RSUs to sign and endorse transactions without revealing the secret keys.

4.3. Scalability

Any system must grow with the growth of the users. This requires more computational power. The system must handle short spikes and short periods of high demand. If the system is unable to respond in a sensible time, transaction flow will be affected and delayed. Hyperledger Fabric is scalable, and comprises a channel system enabling new channels to be created without disturbing the previous architecture. New nodes can be added and deleted without causing any disturbance to the existing environment. Figure 4 shows the latency in the enhanced Fabric transactions. Latency refers to block time, which is the time required to generate the next block of the transaction. Latency is the amount of time a user has to wait for its transaction to be validated and included on the blockchain.

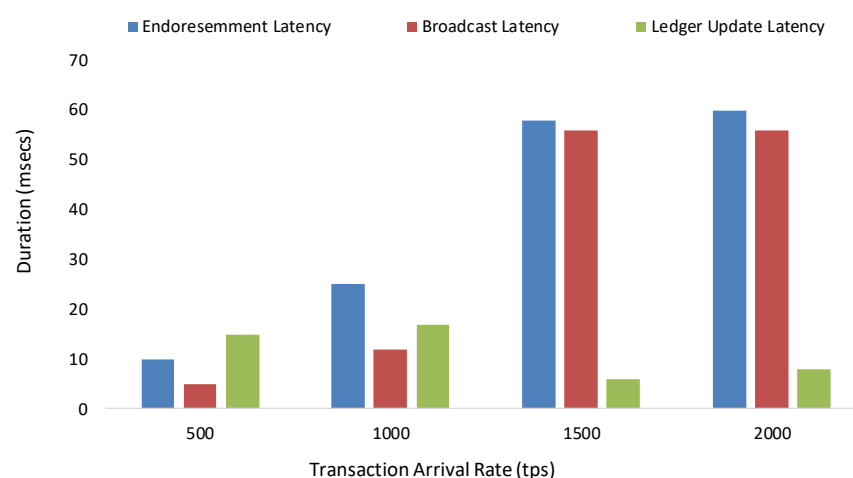


Figure 4. Latency in enhanced Fabric transactions.

4.4. Anonymity and Unlinkability

The Fabric enables advanced cryptographic algorithms and includes privacy features such as anonymity, unlinkability, and small disclosure of attributes. The Fabric uses Idemix, which is a cryptographic protocol that ensures strong features of privacy preservation and authentication. It allows users to prove their authentication without disclosing their real identities. It also enables users to send multiple transactions that are unlinkable. In addition, it is also not possible to identify multiple transactions that are sent by a single user. The actors who are involved in this protocol suite are the user, issuer, and verifier. Figure 5 shows the performance of the enhanced Fabric transactions with different block sizes.

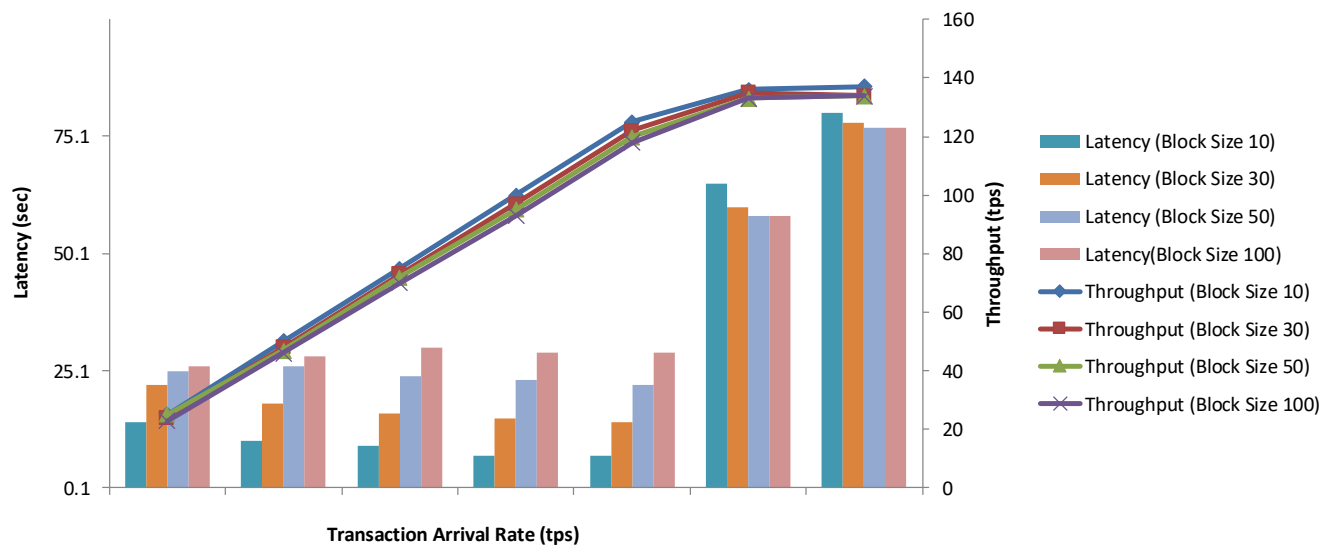


Figure 5. Performance of enhanced Fabric transactions with different block sizes.

4.5. Authentication

The Fabric utilizes access control lists (ACLs) by defining the policies to control the access to the network. These ACLs are very useful for Hyperledger Fabric because they allow only those identities that are linked with a request to be checked. Different types of policies are associated with the network for different purposes, such as endorsement policy checks to determine whether a transaction is properly endorsed. Similarly, modification policies are defined for the configuration of channels that access control and are specified in the configuration of the channel itself. In our proposed system, all the peers in a network are authentic and authorized through the MSP. Roles are defined in the MSPs to access the channels: who are you and what is your role? The system cannot be secured without certainty regarding the user's identity. The MSP gives permission to the vehicles and RSUs regarding the operations that can be executed and the data that can be accessed.

4.6. Traceability

The proposed scheme of IoV provides a conditional-privacy scheme that discloses the real identity of the vehicle if any malicious activities in the network are detected. The most significant feature of our proposed scheme is that the identity of the compromised entity must be traced by the law enforcement department (LED) to punish the intruder. Currently, including traceability and privacy preservation together in the blockchain is a challenging task. Therefore, traceability must be considered in the proposed scheme to avoid any malicious activities in the network. Hyperledger Fabric provides an audit feature. If any malicious activity is noticed, the LED can detect the vehicle's id and time stamp. The Fabric enables "ZKP" to manage privacy preservation with asset management using an auditing feature, which is also called ZKAT. This enables senders to send transactions without disclosing any information to the public. This feature differentiates Hyperledger

Fabric from other schemes available for privacy preservation. A specific auditor, who has full access to transactions of the user, is assigned to each user in a network. Subsequently, auditors are also able to check all of the history and extract the information of users who are assigned to that auditor. Auditors are not able to audit the users who are not assigned to them. In IOV, auditing is the most required feature. Unlike other privacy-preserving blockchain solutions, Fabric fulfills the requirements of the permission network by providing long-term credentials to vehicles. Hence, Fabric supports nonrepudiation, strong accountability, and a strong and secure auditing mechanism for vehicles in the blockchain network.

Figure 4 shows the different latencies of transactions, such as endorsement latency, broadcast latency, and ledger update Latency. We note that latency increases with the increase in the number of transactions per second.

Figure 5 shows the number of transactions per second, which is known as transaction throughput. The time it takes for a transaction to commit is known as transaction latency. The throughput increases linearly as the transaction arrival rate rises. The throughput becomes saturated at roughly 140 tps, and the latency rapidly increases. The latency will be the same for all block sizes. A smaller block size is faster when the transaction rate rises before the saturation point

Figure 6 shows the average delay of the BESA scheme and Ethereum with a varied number of transactions. It clearly shows that our proposed scheme has low latency compared to the Ethereum network.

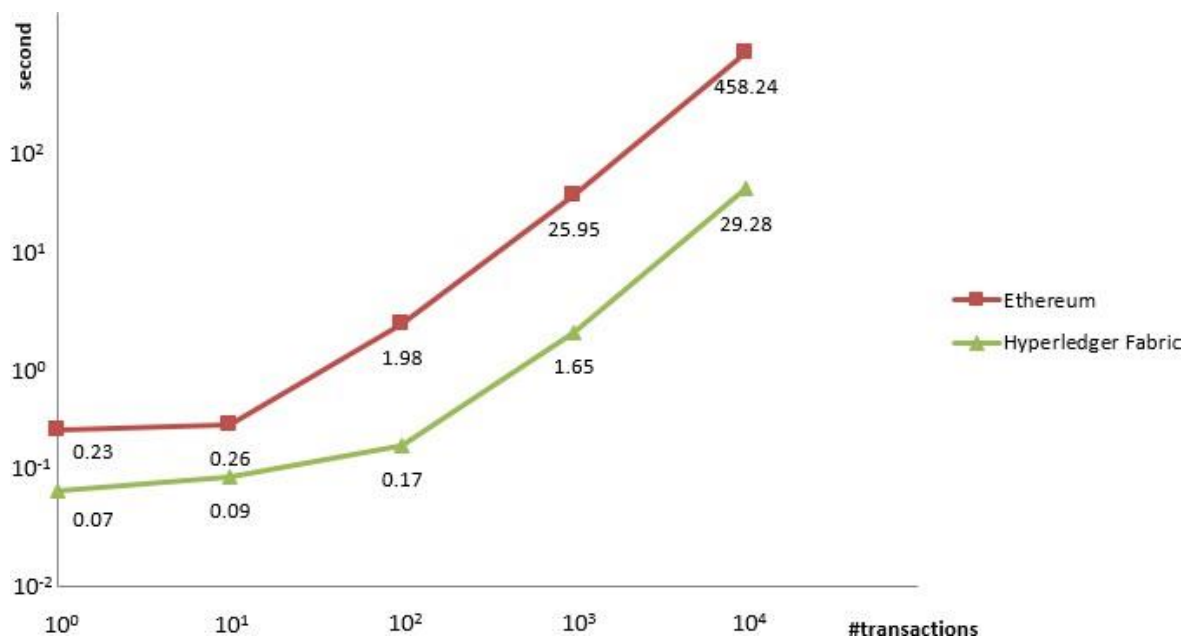


Figure 6. Comparison of enhanced Fabric with Ethereum.

Figure 7 depicts the correct probability that a data block will be verified for several successful detection reputation levels. We note that when the reputation threshold is 0.25, then the accurate probability of our BESA scheme is more than 75% higher than that of the TSL scheme. This shows that the BESA scheme based on the multi-weight subjective logic (MWSL) model can ensure secure block verification even when attackers use internal active miner cooperation. Figure 7 shows the probability of corrected data blocks whereas the Figure 8 compares the resource utilization in PBFT and SBFT.

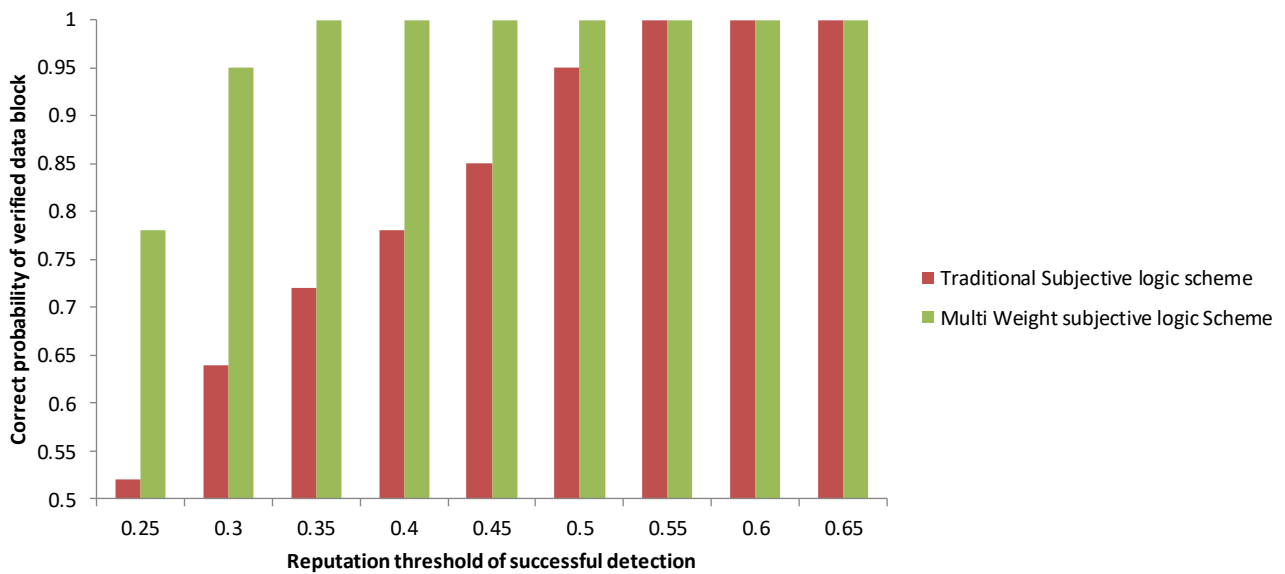


Figure 7. Probability of corrected data blocks.

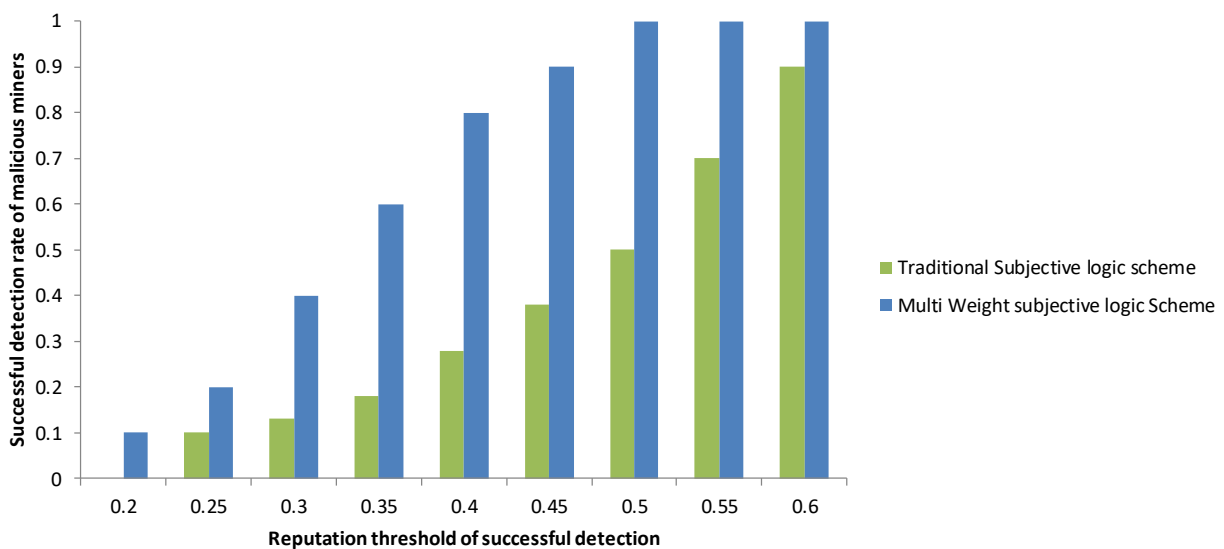


Figure 8. Detection rate of malicious miners.

We used the traditional subjective logic scheme and the proposed BESA solution based on the multi-weight subjective logic scheme to track the detection rate of 10 malicious miner candidates for 1 h. The MWSL technique had a substantially greater successful detection rate of malicious miners than the TSL scheme. We note that when we set the value of the reputation threshold to 0.5, the proposed scheme has a detection rate that is approximately 99 percent higher than that of the traditional subjective logic scheme. Because the MWSL scheme has a greater detection rate, possible security threats can be discovered and prevented more effectively, resulting in a more secure blockchain-enabled IoV.

We calculated the computation cost of the proposed BESA scheme with state-of-the-art schemes to evaluate the scheme overrun of a real-time processor. Computational cost is the execution time per time step during simulation. To estimate this time, we executed the scheme in a simulation, and measured the execution time and determined the average execution time per time step on a real-time target. It is clearly shown in Figure 9 that the computation cost of message verification of the proposed solution is lower than that of the

existing schemes of CPPA [8], ATAAP [22], and EAAP [9]. Figure 10 shows the comparison of BESA communication cost with that of existing schemes.

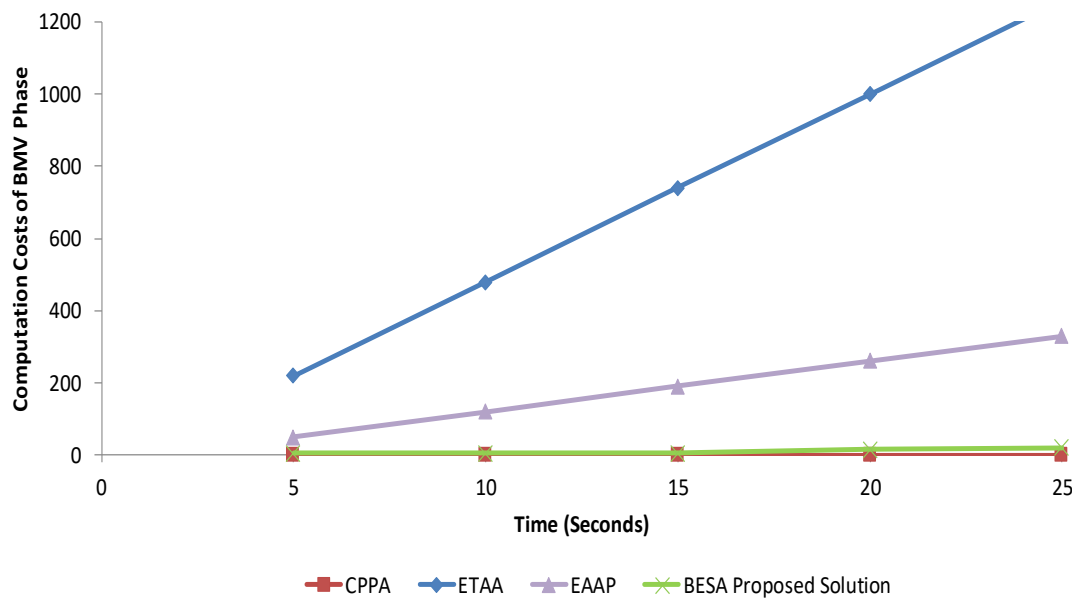


Figure 9. Comparison of BESA computation cost of message verification with that of existing schemes.

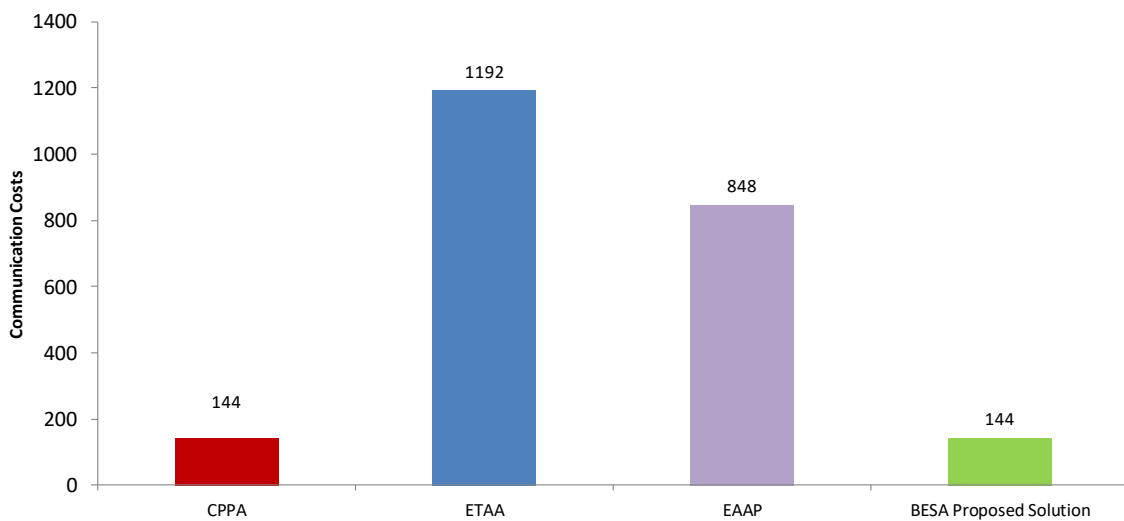


Figure 10. Comparison of BESA communication cost with that of existing schemes.

A graphic representation of the comparison results in Figure 10 is provided. In comparison to the three other approaches—CPPA [8], ATAAP [22], and EAAP [9]—the BESA solution has a lower communication cost.

Figure 11 depicts the reputation of a malicious miner candidate as seen through the eyes of a well-behaved vehicle in three scenarios: the traditional Hyperledger Fabric scheme, the traditional subjective logic scheme, and our BESA scheme. In the standard Hyperledger Fabric scheme, because there is no reputation element, vehicles are unable to identify the malicious vehicles, and thus the vehicle’s evaluation of malicious candidates increases. The traditional subjective logic scheme and our BESA scheme are both based on the reputation values of vehicles; thus, we note that opinions from other well-behaved vehicles decrease the reputation of malicious vehicles in both schemes. Reputation values are below the reputation value of 0.50. It is also clear that the MWSL is more efficient

because it is based on different weights. As result, our BESA scheme has a more precise reputation calculation than the TSL, which leads to a more secure leader selection process.

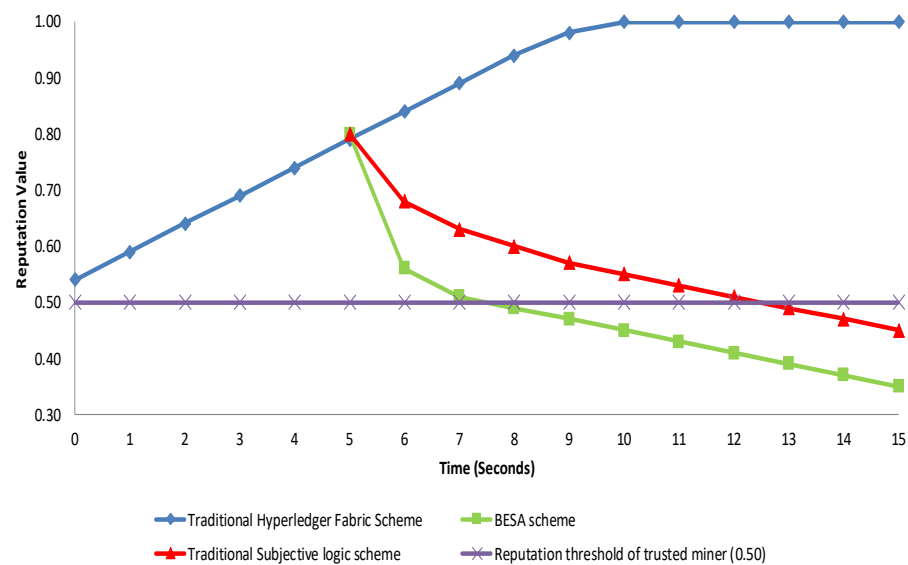


Figure 11. Reputation of a malicious miner.

5. Conclusions

In this paper, we introduced a hard security solution, i.e., the improved Hyperledger Fabric, to implement a blockchain-enabled IoV for safe vehicle information sharing. This paper comprehensively highlighted the issues related to IoV. The literature review concluded that most of the security services can be achieved by the implementation of blockchain. Hyperledger Fabric is one of the major implementations of blockchain for achieving security services. This paper provides a brief introduction to IoV, Hyperledger Fabric, consensus algorithms, privacy, and anonymization techniques, in conjunction with the additional terminology necessary to understand the problem statement and proposed scheme. Then a critical analysis is undertaken of existing consensus algorithms and conditional privacy schemes in the context of the IoV environment. The paper also discusses the non-applicability of existing schemes to the IoV environment. Thus, there is a requirement for an efficient decentralized scheme for IoV that can address security issues and fulfill the latest security requirements of vehicular communication. Hyperledger Fabric appears to be the most suitable emerging solution for a resource-constrained environment, and addresses some of the functionality issues of IoV. The security analysis indicates the proposed scheme will address some of the limitations of existing schemes and fulfill the security criteria of CPPA schemes for IoV. The two main contributions of this research relate to the manner in which it addresses the issue of the leader selection process. The first is to select leaders based on their reputation. A reputation-based scheme is utilized to calculate the accurate reputation of RSUs. Second, this paper presents an anonymous and traceable CPPA approach that can be utilized in a vehicular network. We also evaluated the performance of the proposed solution. In future work, we will choose a more effective and scalable consensus algorithm, and a more efficient scheme to increase the accuracy of the leader's reputation. We will also create a version of the suggested approach for real-world experimentation in a permissioned system, enabling us to analyze and modify the scheme to make it more realistic.

Author Contributions: Conceptualization, K.N.Q. and L.S.; methodology, A.A. and T.A.E.E.; software, T.A.E.E.; validation, A.A.-D.; writing—original draft preparation L.S.; and K.N.Q.; visualization, I.T.J.; writing—review and editing, I.T.J. and B.A.; supervision, N.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Research Groups under grant number (R. G. P. 1/127/42).

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

References

1. Qureshi, K.N.; Bashir, F.; Abdullah, A.H. Provision of Security in Vehicular Ad hoc Networks through An Intelligent Secure Routing Scheme. In Proceedings of the 2017 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 18–20 December 2017; pp. 200–205.
2. Qureshi, K.N.; Din, S.; Jeon, G.; Piccialli, F. Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges with Future Aspects. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 1777–1786.
3. Zhang, C.; Lin, X.; Lu, R.; Ho, P.-H. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 1451–1457.
4. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 11–14 December 2017; pp. 557–564.
5. Javed, I.T.; Alharbi, F.; Margaria, T.; Crespi, N.; Qureshi, K.N. PETchain: A Blockchain-Based Privacy Enhancing Technology. *IEEE Access* **2021**, *9*, 41129–41143.
6. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 104–121.
7. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. *Healthcare* **2021**, *9*, 712.
8. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691.
9. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476.
10. Li, J.; Choo, K.-K.R.; Zhang, W.; Kumari, S.; Rodrigues, J.J.; Khan, M.K.; Hogrefe, D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.* **2018**, *13*, 104–113.
11. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A distributed solution to automotive security and privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125.
12. Zhang, X.; Li, R.; Cui, B. A security architecture of VANET based on blockchain and mobile edge computing. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 17–19 August 2018; pp. 258–259.
13. Arora, A.; Yadav, S.K. Block chain based security mechanism for internet of vehicles (IoV). In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), Jaipur, India, 9–10 May 2018; pp. 26–27.
14. Zhang, L.; Luo, M.; Li, J.; Au, M.H.; Choo, K.-K.R.; Chen, T.; Tian, S. Blockchain based secure data sharing system for Internet of vehicles: A position paper. *Veh. Commun.* **2019**, *16*, 85–93.
15. Yuan, Y.; Wang, F.-Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
16. Kchaou, A.; Abassi, R.; Guemara, S. Toward a distributed trust management scheme for vanet. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 1–6.
17. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220.
18. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J.* **2018**, *6*, 4660–4670.
19. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920.
20. Schwartz, D.; Youngs, N.; Britto, A. The ripple protocol consensus algorithm. *Ripple Labs Inc White Pap.* **2014**, *5*, 151.
21. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; pp. 357–388.
22. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720.

23. Forestiero, A. Metaheuristic algorithm for anomaly detection in Internet of Things leveraging on a neural-driven multiagent system. *Knowl.-Based Syst.* **2021**, *228*, 107241.
24. Ghanem, T.F.; Elkilani, W.S.; Abdul-Kader, H.M. A hybrid approach for efficient anomaly detection using metaheuristic methods. *J. Adv. Res.* **2015**, *6*, 609–619.
25. Alamri, B.; Javed, I.T.; Margaria, T. A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021; pp. 1–5.
26. Huang, X.; Yu, R.; Kang, J.; Xia, Z.; Zhang, Y. Software defined networking for energy harvesting internet of things. *IEEE Internet Things J.* **2018**, *5*, 1389–1399.