Blockchain-enabled Privacy-preserving Internet of Vehicles: Decentralized and Reputation-based Network Architecture

Xinshu Ma, Chunpeng Ge *Member, IEEE,* and Zhe Liu*, *Senior Member, IEEE*

***Abstract*—With the rapid growth of the transportation systems, Internet of Vehicles (IoV) has evolved as a new theme in both industry and academia from traditional vehicular ad hoc networks (VANETs). However, the multi-sources and multi-domain information disseminated over the network has brought huge security issues for the communications in the IoV system. In this paper, we present a lightweight blockchain-based framwork for IoV to meet the requirements of security, privacy and high availability. We propose a novel hierarchical data sharing framework where two types of sub-blockchain are formed allowing for flexible access control. In addition, we propose a reconfigured blockchain structure to acclimatize itself to the vehicular network which is composed of a number of lightweight and low-energy IoT devices. Moreover, we design a lightweight reputation-based consensus algorithm with a multi-weight reputation evaluation mechanism to prevent internal collusion of network nodes. Based on the proposed architecture, security analysis is illustrated to show the security, privacy-preserving of the proposed framework.**

***Index Terms*—Blockchain, IoV, Privacy preserving, Lightweight consensus**

I. Introduction

The concept of Internet of Vehicles (IoV), one of the revolutions driven by Internet of Things (IoT), has evolved from the conventional Vehicle Adhoc Networks (VANETs) where the limited capacity for handling all the information that is aggregated by numerous vehicles and other actuators (such as sensors and mobile devices) in their vicinity has become the most primary problem with the sustainable growth of the number of connected vehicles [1]–[4], to attain the vision of "smart vehicles". A recent report conducted by a renowned organization revealed that the number of cars sold worldwide is expected to 0.5 billion by the end of 2019 [5], and it's projected that we will have 2 billion motorized vehicles including cars, trucks, and buses by 2030 [6]. Such growth has opened a conspicuously challenging but lucrative market for both industry and academia [3].

The IoV is defined as a comprehensive platform integrating IoT technology with the intelligent transportation systems (ITSs), which could support multifold functions such as dynamic information services, intelligent traffic control, intelligent vehicle management [7]. The IoV is anticipated to cope with the in-depth intelligent integration of human, vehicles, things (such as sensors) and the environment, boost the efficiency of transportation, and improve the quality of municipal services to make humans content with their vehicles [4].

However, as IoV involves the myriad of different participants such as numerous vehicles, various sensors, passengers, drivers, Road Side Units (RSUs), cloud servers, etc., it is a challenging issue to realize data sharing and ensure the interoperability in the context of IoV. Namely, the multi-domain and multi-sources data disseminated among the vehicular network usually contains some sensitive information (such as vehicle identification, personalization information, and navigation information) [1], and thus participants are unwilling to share information with each other owing to a sizable lack of trust on each part. Specially, this problem will get worse if there exists malicious vehicles or RSUs in the system spreading incredible messages or spam messages to destroy the availability of the whole network. Hence, it is of extraordinary significance to ensure the security and privacy of data sharing as well as support mitigating techniques to the malicious attacks.

Recently, the Blockchain technology, the core technology of Bitcoin [8] and other cryptocurrencies [9], is being considered as a powerful tool for enabling trusted interactions between various devices in a decentralized, efficient way. The integration of blockchain technology with IoV has drawn increasing attentions of a large number of researchers and developers, the reasons are fourfold: (i) blockchain, in substance, is an immutable, replicated and tamper-evident distributed ledger where each item cannot be deleted or tampered once a consensus is reached and thus enables IoV to conduct *audits* if necessary; (ii) it adopts multiple cryptographic algorithms such as hash functions, asymmetric cryptography and digital signature could protect the *security and privacy* of the information and support the *anonymity* of the users; (iii) it could achieve a *rough consensus* based on designated distributed consensus algorithm where nodes do not have to confide in each other. Despite all these advantages stemming from the blockchain, some challenges might emerge during integrating IoV with the existing blockchain technology such as high resource consumption and high memory overhead. So far, BC has been applied in a number of non-financial scenarios [10], [11], such as healthcare data [12], [13], government democracy and legal enforcement [14], smart home [15]–[17] and so on.

With this in mind, in this paper, we present a lightweight blockchain to meet the requirements of IoV to cope with the

* Zhe Liu is the corresponding author.

Xinshu Ma, Chunpeng Ge, and Zhe Liu are with College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics. E-mail: maxinshusu@gmail.com, {gecp, zhe.liu}@nuaa.edu.cn.

data sharing problem aforementioned and a detailed decentralized IoV system framework based on a novel reputation evaluating scheme is presented. The main contributions of this paper are summarized as follows:

1) A hierarchical structure is adopted to optimize the resource consumption and provide flexible access control for the IoV devices and their data, where two kinds of blockchains *IntraChain* and *InterChain* are employed in the intravehicular network and interwehicular network respectively by default and both blockchains are reconstructed to mitigate the devices' pressure of storage and calculation.
2) A novel consensus protocol akin to Delegated Proof of Stake (DPoS) [18] is proposed in the intervehicular network to reach an agreement with the aggregated data and manage the fluctuation of reputation values of each node among IoV. To evaluate the reputation value of a node (i.e., a vehicle or an RSU), we consider the integration of the direct observations and indirect observations in order to acquire a final value.
3) We show that our proposed blockchain-enabled decentralized framework for IoV is secure by throughly analyzing its security with respect to the adversary model.

The paper is organized as follows. Section II reviews the related works in the literature. Section III presents the system model, adversary model of the new architecture. Section IV illustrates the methodology behind the proposed BC-based IoV framework including the architecture overview and the reconstructed blockchain structure. Section V presents the detailed working mechanism of two chains respectively, especially the novel reputation-based consensus algorithm. Section VI elaborates the security analysis and discusses the disadvantage of the proposed framework. Ultimately, Section VII concludes the paper.

II. Related Work

A. IoV Security

In IoV, heterogeneity and the large number of vehicles increases the security requirements for the communication and data sharing. A demonstration [19] at Black Hat cybersecurity conference showed how to control a Jeep Cherokee on the move via some softwares, which shows the potential risks on the road for IoV. Compared to IoT security which has been studied by numerous previous survey works comprehensively, IoV security is less studied but is analogical to IoT security to some extent. Thus a number of security solutions developed for IoT could also be implemented in IoV. Porambage et al. [20] introduces a pervasive authentication protocol for the resource limited wireless sensor networks (WSNs). Sharaf et al. [21] proposed a novel scheme for authentication procedure in IoT by generating a unique fingerprint for each device. Zhang et al. [22] proposed a method to measure and defend against DDoS attack over IoT network. Some works focusing on the privacy-preserving approaches when the devices transmitting sensitive data via the untrusted channel. Yao et al. [23] proposed an anonymous privacy-preserving data reporting mechanism for IoT applications. The secure communication schemes for vehicular networks has been studied in several previous works [24], [25].

B. Blockchain for IoV

With the advances in networking technologies, embedded processors, and artificial intelligence, the trend of harnessing the blockchain technology to create a decentralized, secure and efficient IoV network is increasingly inexorable. Yang et al. [26] proposed a decentralized trust management mechanism based on blockchain for IoV, employing a joint Proof of Work and Proof of Stake consensus algorithm to reach an agreement about the trust level of each devices. Liu et al. [27] proposed an adaptive electric vehicle participation mechanism in smart grid platform using blockchain to minimize the charging cost of electric vehicles. Gao et al. [28] proposed a blockchain-based payment scheme for vehicles to protect the privacy of the user information during the data sharing process. Jiang et al. [29] proposed a a distributed IoV network architecture where several types of nodes are defined and several sub-blockchain networks are formed. Kang et al. [30] proposed an optimizing consensus management mechanism using reputation-based voting scheme and contract theory to ensure the security and traceability of data sharing in IoV. Sharma [31] presented an energy-efficient transaction model for the blockchain-enabled IoV using distributed clustering-mechanism based on stochastic volatility model to reduce the burden of processing transactions on each device. These current works explore the potential of integrating blockchain technology with vehicular networking in various ways. However, these works lack the clear definition of the blockchain structure which is presented in this paper.

III. Problem Definition

A. System Model

As shown in Fig. 2, a decentralized, secure, and privacy-preserving communication framework for the vehicular networks mainly contains multiple vehicles, multiple RSUs (e.g., traffic lights, toll station, gas station, among others), multiple infrastructures (e.g., transport station, cloud computing platform) multiple humans and personal devices (e.g., cell phones), and all the sensors along with actuators within the vehicle. The heterogeneous network architecture of IoV consists of five types of vehicular communications: Vehicle-to-Vehicle (V2V), Vehicle-to-RSU (V2R), Vehicle-to-Personal devices (V2P), Vehicle-to-Sensors (V2S), and Vehicles-to-Infrastructure (V2I), as shown in Fig. 1. We simplify the complex system into two two-level fundamental paradigms:

1) *Intra-vehicular network layer*: including the connections between all the sensors, actuators, and personal devices within the individual vehicle, i.e., V2S and V2R;
2) *Inter-vehicular network layer*: including the information exchange among vehicles, RSUs, and infrastructures, i.e., V2V, V2R, and V2I.

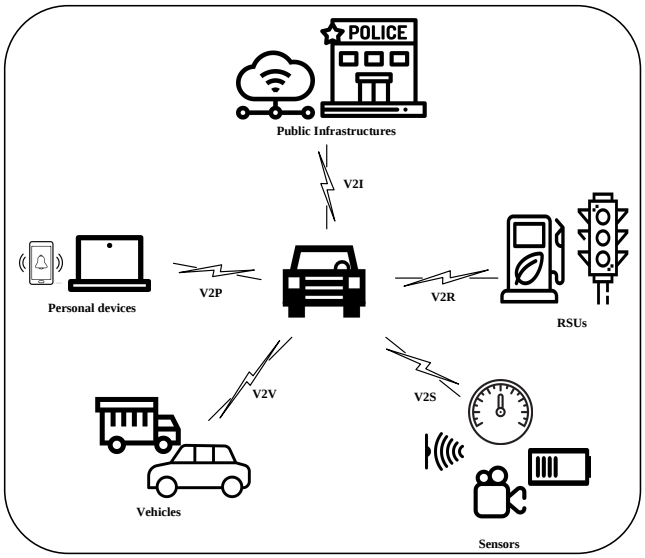

Fig. 1. Five types of vehicular communications of IoV.

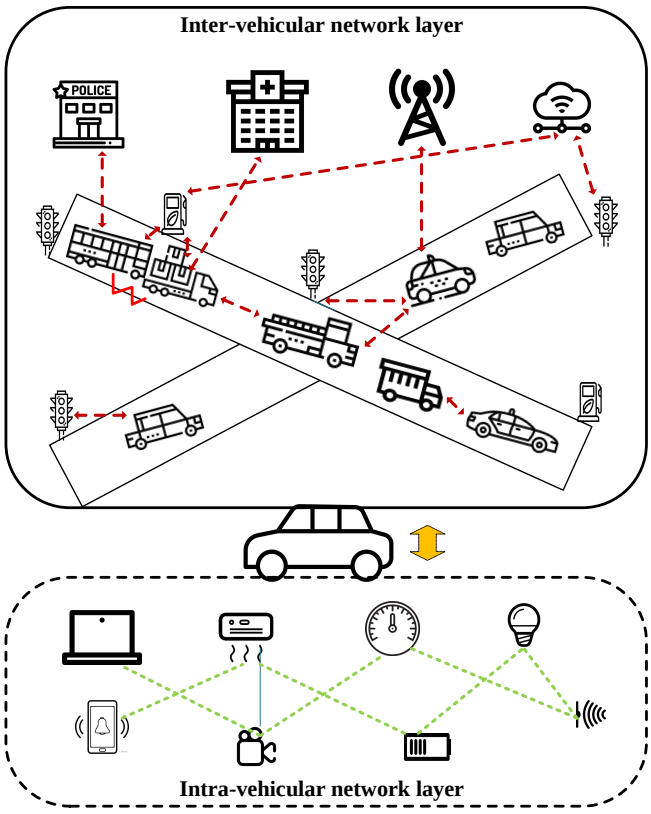

Fig. 2. Overview of our hierarchical system model compromised of two layers: intra-vehicular network layer and inter-vehicular layer.

Note that different type of the aforementioned communications over IoV are enabled utilizing different wireless access technologies (WATs) (such as IEEE Wireless Access in Vehicular Environments (WAVE), GSM, LTE, WiFi, bluetooth, among others), to ensure the seamless connections between all actors. The responsibility of each actor in our framework is listed as follows:

- RSUs: Based on the relatively high data processing and data storage capacity, RSUs take charge of major computing and storage tasks. Namely, RSUs serve as the full node in the conventional Bitcoin network storing the latest version of the entire blockchain, and as the important force for the block generation and reputation consensus. Besides, they ought to monitor the traffic conditions, disseminate the valuable information immediately, and supervise the vehicles operations via collecting and analyzing its behaviors.
- Vehicles: Each vehicle need to interact with other vehicles, RSUs, and infrastructures via sending/responding information to tune with the changing circumstances. Beyond that, vehicles should rate the reputation level of other vehicles/RSUs as the feedback of the service quality and broadcast the rating message to the network to reach an agreement via a certain algorithm. Note that vehicles have the same right to compete for the mining task allowing an increase of its own reputation value.
- Sensors and Actuators: These 'things' are responsible to control the movement of vehicles, gather vehicle situations data such as fuel consumption and car diagnostics, and aggregate environmental data (e.g., temperature, weather conditions, etc.), and report the emergency event to the vehicle when necessary.
- Cloud Server: It is mainly in charge of cloud backup of the blockchain data and other information storage.

B. Adversary Model

We briefly overview three adversarial cases aiming to destroy the availability, data privacy and security of the whole vehicular system:

1) Malicious Vehicles: It is contingent that a few vehicles are manipulated by attackers trying to interfere the normal operation of the whole system. This could bring about severe damages via increasing the traffic crashes and even fatalities. We assume the malicious vehicles mainly destroy the system in three ways: (i) broadcasting false information, packet dropping, packet selective forwarding, e.g., spreading the signal of traffic congestion when the ahead road is clear to make the other vehicles take a detour. (ii) generating unfair reputation values to the other vehicles in the network to damage their reputation and thus acquire the chance to become the miner to alter block content.

2) Compromised RSUs: Analogically, RSUs placed along the road are more susceptible to be compromised by attackers and thus they are assumed as semi-trusted. Since all of the RSUs perform as the full node responsible for storing all blocks in the blockchain, it would be catastrophic if most

of RSUs are under the malicious control. Nevertheless, it is impracticable for the attackers to launch a large-scale intrusion attack due to the limited ability. Thus, we assume that the attack could compromise a few RSUs (i.e., tampering the block content and generating new blocks) within a certain period of time.

3) DoS/DDoS Attack: The object is to prevent some or all legitimate requests/information from being responded/acquired, by sending a mass of requests to the target device causing its computational resources unavailable [32]. Either external device or the individual device within IoV might be manipulated to initiate this attack and we only assume the latter case in our framework.

IV. Methodology

In this section, we briefly introduce the fundamental methodology of our design — blockchain technology, system architecture of the decentralized IoV framework, and the reconfigured blockchain structure tailored for vehicular communication systems.

A. Blockchain Basics

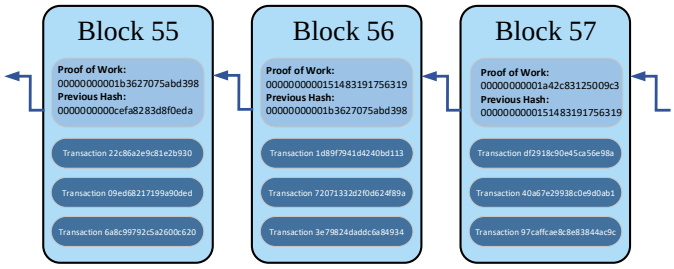

Fig. 3. An illustratioin of blockchain struction.

Satoshi Nakamato [8] invented the concept of blockchain in 2018 which has attracted much attention in the last few years, and is regarded as the fifth disruptive innovation in computing paradigm after the invention of the Internet [33]. It was originally created for recording financial transactions (e.g., Bitcoins and other cryptocurrencies), where multiple transactions will be encoded and saved by all participants in a public ledger. Nowadays, blockchain technology is view as an emerging peer-to-peer (P2P) technology for decentralized data sharing and distributed computing systems that ensures a group of agents are able to reach an agreement in a secure and verifiable manner without the need for a centralized controlling authority [34].

As shown in Fig. 3, the blockchain is composed of a string of blocks linked together by the hash values of the previous block. Each block contains a number of transactions descripting the details of who sent how much money to whom, hash value of the preceding block in the blockchain, and hash value of current block which is the target value to a complex mathematical challenge known as ”proof of work”. All the nodes after receiving new blocks should validate the block and transactions embedded in. The new block would be appended to the blockchain once the it is valid. Otherwise, it will be discarded.

B. Architecture Overview

In this paper, we explore how the blockchain technology could be applied in the vehicular network. As mentioned above, a hierarchical network model is proposed which is illustrated in Fig. 2. Accordingly, *IntraChain* and *InterChain*, these two types of blockchain are adopted to process different transactions and information in *Intra-vehicular network* and *Inter-vehicular network* respectively.

1) IntraChain: Smart sensors, actuators of individual vehicle, and user's personal phones/computers are located within the *Intra-vehicle network* tier and are centrally managed by vehicular central controller (i.e., local miner). In each vehicle, there exists a local private blockchain named *Intra-BC* which keeps tracks of interactions within the vehicle and sticks to a certain policy list for the internal access control and external access control management. Due to the sensitivity of the interaction information inside the vehicle, the encryption algorithm is involved in the internal communications. Each transaction initiated by the ”things” should be tagged with the requester ID and requestee ID that is assigned by the controller at the initialization stage. The central controller each received transaction in accordance with the policy list set by the vehicle's owner.

Besides the block header, the block body contains a number of transactions collected by the local miner within a certain period of time. Since the communication traffic of the intra-vehicular network is not high, it is rational to store the block data in the vehicle locally and all of the transactions are chained together as an immutable ledger. Therefore, all the information related to the present and past conditions of the vehicle (including speed, direction, location, lane, the number of passengers, etc.) will be well preserved, which could be considered as the black-box data in case of emergency.

2) InterChain: Multiple vehicles, and RSUs constitute an *Inter-vehicular network* layer along with public infrastructures (cloud server). All the vehicles want to receive the information from the other vehicles/RSUs in the vicinity, even by accessing the sensors of the neighboring vehicles. Each vehicle in the network could act as either a requester collecting data or a provider sharing its own data while on the road. Since each node even RSUs in the network might perform compliantly or disobediently, it is anticipated that each node could enjoy qualified services. Therefore, a reputation evaluation mechanism is needed to improve the stability and availability of the entire system. It is worth noting that nodes (vehicles or RSUs) might transform the performance between normal and abnormal just as in the real world situations.

We adopt the *InterChain* as a public ledger which records the interactions among *Inter-vehicular network* and the reputation value of each actor, allowing accident prevention, autonomous decision making, and data auditing. These reputation records are persistent and transparent evidence when disputes and destruction occur. However, some compromised

and malicious nodes might provide incorrect feedback to the former service aiming to decrease the service quality and stability of the network. Thus a novel consensus algorithm based on the fusion of the average reputation value is necessary. In the proposed framework, both vehicles and RSUs could compete to be the miner and obtain an increase in reputation as a reward. Due to the constrained resources of the vehicles, only block headers are saved locally which is similar to the Simplified Payment Verification (SVP) nodes in the Bitcoin. Conversely, the RSUs must have a copy of the full *InterChain*, thus every transaction and block that has ever taken place must be saved and upload the data to the cloud server periodically. This ensures that the *InterChain* cannot be controlled by a single entity, and nor can it easily be compromised, as there is not one single point of failure.

C. Reconstructed Blockchain Constitution

Considering IoV is composed of resource-constrained and low-energy devices, it is irrational to require these devices to possess equal computational power to the miners in the conventional blockchain network, which makes the task of supporting distributed storage and security quite challenging. Thus, in our proposed framework, a reconstructed blockchain architecture is proposed for *InterChain*.

1) Block Detail: As shown in Fig. **??**, the structure of a reformatory block, akin to Bitcoin, consists of the block header and the block body. The block header, detailed in Table I, is composed of the current block header's hash, previous block header's hash, root of the reputation tree, policy list, a timestamp, and root of the transaction tree. Here, the item of reputation tree is added into block and the root of the tree is recorded by block header. As shown in Fig. 4, we utilize the modified Merkle Patricia Trie structure to record the reputation values, where only modified data is stored in the new block, efficiently reducing the burden of memory.

Accordingly, the block body is composed of the reputation tree and transactions tree. The reputation value of each vehicle and RSU will be recalculated once the acts in suspicious ways, such as querying privacy data against the access policy which is stored in the block header generated by the administrator, and creating or relaying the invalid blocks or transactions. And the details of reputation evaluation scheme are elaborated in Section V-B. It should be noted that a cryptographically authenticated data structure—modified Merkle Patricia Trie (MPT) applied in Ethereum [35] is adopted to store the reputation value of each UAV as depicted in Fig.4, which could quickly and efficiently identify data that has changed without having to retrieve over all the data in order to make the comparison.

2) Transaction Detail: As for defining transactions, inspired from [16], communications between vehicles, RSUs and the cloud server among the whole system are formatted as transactions. Owing to the constrained storage space of vehicles, a micro-size transaction structure is proposed as shown in TABLE II. The detail information of a transaction includes the transaction type IDs of the requester and requestee

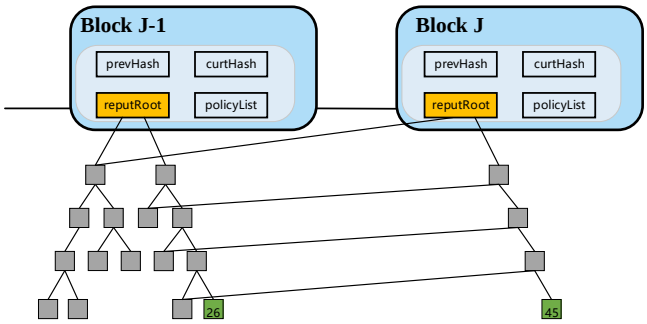

Fig. 4. Example of the modified Merkle Patricia Trie structure for recording the reputation values. Two blocks B_{J-1} and B_J containing two reputation trees, it is shown that the reputation value 26 was changed to 45 in the latter block B_J. Specifically, only the modified data would be stored in the new block and the unmodified data would be linked to the new root without duplication, efficiently reducing the request of memory compared to the original Merkle Tree which is adopted in Bitcoin [8].

(similar to the addresses in the blockchain), the signature of the requester (i.e., sender) and the additional data if necessary. It is worth noting that the length of the additional data is variable ranging from 0 to 1024 bits.

TABLE I
COMPOSITION OF A BLOCK

Contents	Size(bit)	Description
BLOCK_HASH	80	Hash value of current block header
PREV_HASH	80	Hash value of previous block header
TIMESTAMP	24	Unix timestamp of the block
REPUTATION_ROOT	80	Root of the reputation tree
TRANSACTION_ROOT	80	Root of the transaction tree

TABLE II
COMPOSITION OF A TRANSACTION

Contents	Size(bit)	Description
TX_TYPE	4	Transaction type
REQUESTER_ID	8	Device ID of the sender
REQUESTEE_ID	8	Device ID of the receiver
SIGNATURE	1024/2048	Signature/multi-signature
DATA	Maximum 1024	Additional information

3) Transaction Handling: Due to that various weighting factor is embraced into the proposed reputation evaluation algorithm, we define a set of operations to be recorded as transactions with different weighting factors. We briefly elaborate six kinds of transactions as follows:

- **Interest** The requester initiates *Interest* to query specific information from a number of neighboring vehicles/RSUs or one appointed actor.
- **Reply** The vehicle/RSU reply to the *Interest* transaction with the additional information.

- **Report** The vehicle/RSU actively publishes the latest information (related to the road conditions, weather report, etc.).
- **Rating** The vehicle/RSU sends the feedback via this transaction after dealing with the specific devices utilizing the reputation evaluation scheme.
- **Alert** The vehicle/RSU creates an *Alert* transaction to sound a warning once it finds itself under a certain kind of attack thus other nodes could perform corresponding actions towards different attacks.
- **Help** The vehicle/RSU generates such transaction as an emergency call which will be disseminated with the highest priority in order to contact the services (such as police, family, etc.).

4) Periodically Memory Release: With the continuous operation of the vehicular system, there is no doubt that the blockchain distributed ledger would become increasingly larger. For instance, suppose that the size of the block header is 100 Bytes; the block body is 2000 bytes; and the generation rate of the blocks is 1 block every 3 minutes. Therefore, after one day the size of the ledger would be $(2000 + 100) \times 60 \times 24 \div 3 = 1008$ KB. Considering the restricted memory space of RSUs, for these parameters, freeing up memory at a frequency of every 12 hours is sufficient for recycling the memory space. Namely, the distributed ledger of blockchain in the proposed framework needs to be baked up to the cloud server and the physical memory of RSUs is released periodically.

V. Detailed Mechanism of the InterChain

In this section, we elaborate in detail of the working mechanism of our proposed *InterChain* framework which consists mainly of reputation evaluation scheme and the consensus algorithm.

A. Data Processing

Each node (vehicles and RSUs) in the network is assigned a pair of public key and private key as mentioned at the initiate stage. The unique ID of each node is derived from its own public key to ensure the anonymity of the framework. Note that the basic information stored in each vehicle is composed of the public keys of all nodes, its own private key and the consecutive block headers which contains the reputation values of the entire system, while RSUs store the full blocks of *InterChain*. All devices need to perform the hash function and digital signature before sending messages. It is worth noting that Keccak [36], [37], a high-performance hash function in both code size and cycle count [38], [39] compared to other lightweight hash functions (such as Quark [40], PHOTON [41], and SPONGENT [42]), is adopted to generate a *message digest*. To reduce memory usage, the 160-bit output is truncated to 80-bit which saves a mount of space.

All the nodes receiving the transactions need to verify data integrity and consistency via checking if two *digests* match with each other. The transaction is relayed to the neighbors or replied with specific data if validation passes with certain probability $\mathcal{P}$ generalized from the sender's reputation value. Otherwise, the received transaction is considered as false and not transmitted if it lacks data integrity. Particularly, once a node finds that a sender sending the same message with an abnormal frequency, it creates and broadcast an *Alert* transaction immediately. Once this information is confirmed by miner committee, the malicious sender will be flagged via setting reputation value to zero and the message initiated by it would be blocked.

B. Reputation Evaluation Scheme

1) Individual Reputation Calculation: The proposed framework maintains a trust rating for each node based on activities it has performed harnessing the reputation evaluation scheme. Generally, each node is initialized with a fixed reputation value 100 which could be decreased for performing malicious/incredible actions or increased for correctly performing *Alert* and mining task.

Each node in the network evaluate the reputation of other nodes based on the direct historical interactions with them. Considering the characteristics of different transactions, the weighting factor W of each transaction is embraced into the evaluation scheme. Beside, since the timeliness of data should also be considered into out algorithm, we evaluate each record at time t. At time t, the evaluation result $R_{u,v}(t)$ of node v generated by node u from the direct observation is calculate via:

$$R_{u,v}(t) = \sum_{i=1}^{C(u,v,t)} \sigma(t,i) \cdot Q(v,i) \cdot W(v,i) / \sum_{i=1}^{C(u,v,t)} W(v,i) \tag{1}$$

where $C(u,v,t)$ denotes the interaction count of all the transactions between u and v before the specific time t; $Q(v,i)$ represents the quality evaluation of the ith transaction with node v; and $W(v,i)$ represents the significance factor of the ith transaction with node v.

Besides, $\sigma(t,i)$ is proposed as the perish coefficient depicting the timeliness of the ith service. Let $t(i)$ represents the time of ith transaction and we have

$$\sigma(t,i) = 1/(t(i) - t), \tag{2}$$

which shows that the decay of the service quality is inversely proportional to the transaction time length.

2) Reputation Fusion: The miner might receive conflicting reputation values about one specific node. In the proposed framework, weighted reputation fusion is utilized on these ratings to obtain a relatively objective result. Let $R(t_0)$ denote the set of all reputation values last time at t_0, $R_v(t)$ denote the new calculated reputation value of node v at time t, and $\mathcal{R}_v$ denote the latest aggregated reputation values of node v. At first, we abandon the highest reputation value and the lowest reputation value from the aggregated data set R as follows:

$$\mathcal{R}_v^* = \mathcal{R}_v \not\subset \{\max(\mathcal{R}_v), \min(R)_v\}. \tag{3}$$

Then, the weighted average reputation value of node v is calculated via:

$$R_v(t) = \sum_{i=1}^{N} \frac{R_i(t_0)}{\sum_{j=1}^{N} R_j(t_0)} \cdot R_(i,v)(t), \tag{4}$$

where $R_{i,v}(t) \in \mathcal{R}_v^*$ and N denotes the number of rating transactions received by the miner.

C. Consensus Protocol

The consensus algorithm, which ought to be automatically executed by each node (vehicles and RSUs), is presented in this section, involving the regulations of committee selection and block generation.

1) Committee Selection: To relieve the burden of the IoV devices, we adopt the core idea of DPoS electing the committee via certain voting methods where block are generated in turn instead of Proof of Work algorithm that requires lots of computational resources to solve a complex mathematical challenge. Considering the actual situation of IoV system, we propose the following two schemes to select miners.

Strategy 1: Randomly Selected RSU as Miner. Based on the premise that the majority of RSUs are trusted and the computational ability is comparably strong, it is rational to randomly assign a RSU to act as the miner responsible for collecting all the transaction information, verifying the validity of transactions, and managing the changes of reputation values in the block header, which mitigates the computation load of the Vehicles.

Strategy 2: Voted Vehicle/RSU as Miner. Formally, the re-election of the committee is triggered by any omitting of block generation or forks in the blockchain ledger. In that case, the members of committee are selected by their reputation value R and, namely, only top 15% of the nodes could become the candidates. Then, a group of k active miners, three fifths of the miner candidates, are voted by all RSUs which take turn to act as the block generator within a certain time slot. It is worth mentioning that, the members of committee can also propose transactions as other devices in the network, they only exercise their mining rights every fixed period of time T. Formally, the re-election of the committee is triggered by any omitting of block generation or forks in the blockchain ledger.

Strategy 3: Hybrid Miner Selection. It's obvious that both *Strategy 1* and *Strategy 2* have their advantages. With this in mind, we consider node density and network connectivity into our consensus algorithm to propose a hybrid selection strategy by taking advantages of both methods. When the network is unstable and few vehicles are enabled for connection, or the node density is lower than a threshold such as in the middle of the night, *Randomly Selected RSU as Miner* is employed to provide a stable and available service. Otherwise (e.g., in the rush hour), *Voted Vehicle/RSU as Miner* is utilized to get a relatively high-quality service. Based on the observation, we could use different strategy in different time periods.

2) Block Generation: If the rate of block generation is slow, the size of block will be quite large due to the accumulative transactions over time, which could cause the communication delay or slow down the transmission rate among the network. Otherwise, extremely frequent mining could become the computation burden for the each node in the blockchain system. Consequently, the suitable block generation rate is significant for the proposed framework. We propose a hybrid strategy by considering the node density into our model.

Generating Block by Fixed Size Each block is generated with the same size limit, for example, each block including the same number of verified transactions. Thus, the time slot between two blocks is fluctuant. Let α denote the time interval of mining process, β denote the designated block size, t_0 represent the time period that periodically releases the memory (cf. Section IV-C4), and Δ represent the average allocated size of storage space in RSUs. We have the following constraint:

$$\beta \cdot floor(\frac{t_0}{\alpha}) \leq \Delta, \tag{5}$$

where $floor(\cdot)$ represents rounding down to the nearest integer.

Generating Block by Fixed Time Each block is created at a fixed time interval which requires the mining task to be rotated at the same frequency. The next new round of mining process starts instantly after the generation of the previous block. It is adjustable that the stipulating of the time period between two rounds of block generation owing to the diverse communication requirements of different tasks. For an N-UAVs network, let α' denote the time interval of mining process, β' denote the average size of the generated block, t_0 represent the time period that periodically releases the memory (cf. Section IV-C4), and Δ represent the average allocated size of storage space in RSUs. We have the following constraint:

$$\beta' \cdot floor(\frac{t_0}{\alpha'}) \leq \Delta, \tag{6}$$

Clearly, both Eq.5 and Eq. 6 ensure that all collected data in the blockchain could be well stored in each devices before next round of memory release.

VI. Security Analysis

A. Scenario of Malicious Vehicles

As mentioned before, a malicious vehicle might damage the availability of the whole system in two methods. Broadcasting fake information which might cause traffic accidents could be defended by the novel reputation evaluation scheme. It mainly because the activities of each devices in the network are being evaluated to build a trust rating scheme and the receiver accepts or drops the message according to the reputation value of the vehicle. Thus, those fake information and unfair reputation report messages could be blocked with high probability.

B. Scenario of Compromised RSUs

In the proposed framework, it is supposed that only a fraction of RSUs might be compromised in a given period of time. Once the RSU is compromised, the saved data (i.e., blocks) might be deleted or modified and the RSU could tamper the reputation value when generating the new blocks. However, the same version of the latest blockchain stored in all the

RSUs among the whole network according to the fundamental principle of the blockchain technology. Thus there always exits more than half of RSUs compliant to the basic rules and consensus algorithms such that the compromised RSU is prone to be recognized via the detection of deviant behaviors and kicked out of the system using vote transaction in order to prevent it from serving the malicious activities.

In addition, the compromised RSUs also might fabricate and spread fake information. However, the reputation value of RSU should also be evaluated by the same scheme with other vehicles, so the vehicles would give a low credit grade if they do not satisfied with the service provided.

C. Scenario of DoS/DDoS Attacks

Next we analyze the effectiveness of our framework to prevent DoS/DDoS attack launched by the individual vehicle among the vehicular network, aiming to overwhelm a particular target vehicle. In our system, the reputation evaluation scheme allows to reduce the probability of being undermined by DoS/DDoS attack due to that a sender sending the same message within a certain time will be flagged via setting reputation value to zero and the message initiated by it would not be relayed by the neighbor nodes. Overall, each node among the system could supervise the packet flows and send alert transaction to warn the neighbor vehicles to ban all the access permissions of the malicious node.

VII. Conclusion

In this paper, we investigate a blockchained-based decentralized data sharing framework in vehicular networks. Considering the inherent hierarchical architecture of IoV, a hierarchical blockchain-based data sharing framework is proposed where two types of sub-blockchain networks (intra-vehicular network and inter-vehicular network) are formed allowing for flexible access control and reduced data storage consumption. In addition, a reconstructed blockchain structure is illustrated to acclimatize itself to the vehicular network which is composed of a number of lightweight and low-energy IoT devices. Besides, we also design a reputation-based consensus scheme which is akin to the core idea of DPoS consensus algorithm but a multi-weight reputation evaluation mechanism is utilized to prevent internal collusion of network nodes. Based on the proposed architecture, security analysis is illustrated to show the security, privacy-preserving of the proposed framework. In the future, we can further confirm the efficiency of our schema via numerical results produced by simulation experiments and improve the ability of implementation through taking more factors into consideration and finding optimal parameters.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant No.61802180, 61702236, 61872181), the Natural Science Foundation of Jiangsu Province (Grant No.BK20180421), the National Cryptography Development Fund (Grant No.MMJJ20180105), the Fundamental Research Funds for the Central Universities (Grant No.NE2018106).

References

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[2] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *2014 IEEE world forum on internet of things (WF-IoT)*. IEEE, 2014, pp. 241–246.

[3] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[4] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1–15, 2014.

[5] S. Scotiabank, "Number of cars sold worldwide from 1990 to 2019 (in million units)," https://www.statista.com/statistics/200002/international-car-sales-since-1990/, accessed Aug 22, 2019.

[6] L. Bill, "Is our planet ready for 2 billion cars?" http://alert-conservation.org/issues-research-highlights/2016/5/8/are-you-ready-for-a-planet-with-2-billion-cars-hg583, accessed Dec 19, 2017.

[7] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," *IEEE Wireless Communications*, vol. 22, no. 6, pp. 122–128, 2015.

[8] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[9] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 104–121.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[11] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[12] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of internet of things infrastructure for secure and smart healthcare," *arXiv preprint arXiv:1805.11011*, 2018.

[13] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2017, pp. 772–777.

[14] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Available at SSRN 2580664*, 2015.

[15] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 618–623.

[17] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the second international conference on Internet-of-Things design and implementation*. ACM, 2017, pp. 173–178.

[18] "Dpos description on bitshares." [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html

[19] Y. Danny, "Hackers demonstrate how to take control of cars," in *Proc. Black Hat Security Conf., Las Vegas, NV, USA*. Black Hat, 2015, p. 834.

[20] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 357430, 2014.

[21] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the internet of things," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2016, pp. 1–3.

[22] C. Zhang and R. Green, "Communication security in internet of thing: preventive measure and avoid ddos attack over iot network," in *Proceedings of the 18th Symposium on Communications & Networking*. Society for Computer Simulation International, 2015, pp. 8–15.

[23] Y. Yao, L. T. Yang, and N. N. Xiong, "Anonymity-based privacy-preserving data reporting for participatory sensing," *IEEE Internet of Things Journal*, vol. 2, no. 5, pp. 381–390, 2015.

[24] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in vanets," *Computer Communications*, vol. 71, pp. 50–60, 2015.

[25] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for vanet safety applications," *Computer Communications*, vol. 63, pp. 11–23, 2015.

[26] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[27] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25 657–25 665, 2018.

[28] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Network*, vol. 32, no. 6, pp. 184–192, 2018.

[29] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, 2018.

[30] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[31] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled internet of vehicles (iov)," *IEEE Communications Letters*, vol. 23, no. 2, pp. 246–249, 2018.

[32] J. Chen, Z. Feng, J.-Y. Wen, B. Liu, and L. Sha, "A container-based dos attack-resilient control framework for real-time uav systems," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 1222–1227.

[33] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[34] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," in *Proceedings of the Future Technologies Conference*. Springer, 2018, pp. 1037–1058.

[35] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[36] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak specifications," *Submission to nist (round 2)*, pp. 320–337, 2009.

[37] ——, "Keccak sponge function family main document," *Submission to NIST (Round 2)*, vol. 3, no. 30, 2009.

[38] T. Meuser, L. Schmidt, and A. Wiesmaier, "Comparing lightweight hash functions–photon & quark."

[39] J. Balasch, B. Ege, T. Eisenbarth, B. Gérard, Z. Gong, T. Güneysu, S. Heyse, S. Kerckhof, F. Koeune, T. Plos *et al.*, "Compact implementation and performance evaluation of hash functions in attiny devices," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2012, pp. 158–172.

[40] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A lightweight hash," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 1–15.

[41] J. Guo, T. Peyrin, and A. Poschmann, "The photon family of lightweight hash functions," in *Annual Cryptology Conference*. Springer, 2011, pp. 222–239.

[42] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede, "Spongent: A lightweight hash function," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2011, pp. 312–325.