IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 1 December 2019; revised 20 June 2020; accepted 11 October 2020.
Date of publication 2 November 2020; date of current version 16 September 2021.

Digital Object Identifier 10.1109/TETC.2020.3033532

Blockchain-Based Trust Management for Internet of Vehicles

HAIBIN ZHANG, (Member, IEEE), JIAJIA LIU, (Senior Member, IEEE), HUANLEI ZHAO, (Student Member, IEEE), PENG WANG, (Student Member, IEEE), AND NEI KATO, (Fellow, IEEE)

Haibin Zhang and Jiajia Liu are with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an Shaanxi 710072, China
Huanlei Zhao and Peng Wang are with the School of Cyber Engineering, Xidian University, Xi'an Shaanxi 710071, China
Nei Kato is with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan
CORRESPONDING AUTHOR: J. LIU (liujiajia@xidian.edu.cn)

ABSTRACT The Internet of Vehicles (IoV) greatly improves the traffic environment and life efficiency using messages shared between vehicles. However, due to its complex network structure and high mobility, the messages shared between vehicles are not always reliable. To this, we propose a trust management system of IoV based on blockchain, which formalizes a complete vehicle reputation value calculation scheme to deal with the problem of calculating the credibility of messages. The proposed scheme can detect vehicles that send malicious messages and reduce their reputation values for punishing according to the rating mechanism. In addition, we design a blockchain-based data storage system that can prevent attackers from tampering with the reputation values stored in roadside units (RSUs). In view of the lack of calculation basis when roadside units verify the block, we also store the rating list it. Finally, we use the consensus mechanism that combines PoW and PoS to ensure that vehicles with a large change in reputation can be updated to the blockchain first. The simulation results show that the proposed scheme has an obvious limitation on malicious vehicles, and improves the accuracy of the vehicles' judgment of events based on the received messages.

INDEX TERMS Internet of vehicles, trust management, blockchain, credibility, reputation value, smart contract

I. INTRODUCTION

In recent years, the vehicle industry has developed rapidly with the number and quality of vehicles increasing steadily. At the same time, the automation process of vehicles is also steadily advancing [1] with the development of on-board sensors, computing modules and communication modules. In addition, the recently proposed 5G communication protocol greatly speeds up the data transmission speed of IoV and greatly reduces the delay of the system [2]. IoV provides a platform for messages sharing which can provide road information, weather information and traffic accident information in many other locations in a timely manner and make our life extremely convenient.

Trust management is one of the most significant concerns in IoV. Due to the distributed network architecture of IoV, the high mobility and wide range of vehicles, messages transmitted between vehicles are not necessarily reliable [3]. Trust management can realize the credibility calculation of the messages in IoV, and then improve the accuracy of vehicles' judgment of event based on the received messages. It can also assign, calculate and update reputation values for vehicles with its reputation values being stored in the cloud server or stored in RSUs. Storing data in RSUs has lower latency and is more suitable for IoV [4]. However, RSUs are deployed in the external public space near roads, so they are easily illegally controlled by malicious attackers to tamper with the vehicles' reputation values. Therefore, the security of RSUs is very important for the reliability of trust management in IoV.

Blockchain is useful for ensuring the security of data in RSUs [5], which naturally has the function of data tamper resistance due to its own characteristics. An obvious feature of the blockchain is decentralization which is a peer-to-peer distributed database in line with the architecture of IoV [6]. There are many works for the blockchain of IoV. Liu *et al.* in [7] designed an efficient debt-credit mechanism based on blockchain to support efficient data-trading in IoV. Leung *et al.* in [8] stored trust values on the blockchain, and proposed a trust management scheme.

However, there are some problems in the current research for blockchain of IoV. First, the existing consensus mechanisms of blockchain waste a lot of computing resources, which cannot meet the requirement of IoV. Second, the other RSUs cannot verify the correctness of the internal reputation values when verifying the block if only the reputation values information is stored in the block. To this, we propose a trust management system for IoV based on blockchain. The specific contributions of this paper are summarized as follows.

1) We consider a blockchain-based IoV scenario where messages can be shared between vehicles. Due to the existence of malicious vehicles and malicious RSUs, we formalize a trust management mechanism that uses blockchain to save reputation values, which effectively limits the impact of malicious vehicles and malicious RSUs on the system.
2) We propose a complete reputation value update algorithm including message credibility calculation, rating mechanism, and reputation value calculation based on ratings. Using this algorithm, we can effectively detect those vehicles that send false messages and ratings, reduce their reputation value, and weaken their impact on the system.
3) We use a consensus mechanism combining PoW and PoS to realize that vehicles with large changes in reputation value will be updated to the blockchain first. We write the reputation value update algorithm into the smart contract which can guarantee that RSUs can only calculate the reputation values according to the proposed algorithm. In addition, we add ratings to the block body to provide a calculation basis for the block verification.
4) We evaluate the performance of the proposed scheme by simulation experiments which show that the proposed system can effectively improve the accuracy of vehicle's judgment of the event based on the messages, the proposed reputation value update algorithm is effective in detecting and limiting malicious vehicles, and the update delay of the reputation value in the proposed system is also lower than that of the traditional blockchain.

The rest of this paper is arranged as follows. Section II introduces the related work. In Section III, we give a brief description of the application scenario and system model. Section IV proposes the trust management system. In Section 5, we conduct the data storage system based on blockchain. Section VI gives the security analysis. In Section 7, we evaluate the performance of the proposed scheme and present the simulation results. Finally, Section VIII concludes this paper.

II. RELATED WORK

In this section, we mainly discuss related work from IoV with edge computing, edge computing combined with blockchain and trust management in the Internet of things (IoT).

A. IOV WITH EDGE COMPUTING

Due to the high latency of previous IoV architecture based on cloud computing, many scholars invest a lot of research energy in the combination of IoV and edge computing. Tan *et al.* in [9] proposed a kind of IoV architecture based on edge caching and computing of deep reinforcement learning which reduced the computational complexity caused by high data dimension. Gard *et al.* in [10] gave a threat detection model based on the structure of probability data which distributed or collected data from different places using edge computing to make the computing time and storage space reduce greatly. Zhou *et al.* in [11] studied three kinds of mobile edge computing architectures supporting UAV, pointed out the future research direction and great significance. Liu *et al.* in [12] put forward an edge computing network framework which took wireless transmission as the cost, made full use of the computing power of edge nodes, and greatly optimized system performance. Rodrigues *et al.* in [13] proposed an IoV energy-saving scheduling framework based on mobile edge computing to minimize the energy consumption of RSUs under task delay constraints. However, all these researches focused on improving the data processing speed, reducing the delay and energy consumption of the IoV.

B. EDGE COMPUTING COMBINED WITH BLOCKCHAIN

As edge computing is vulnerable to malicious attacks such as data tampering, many scholars have a strong interest in the combination of blockchain and edge computing. Gai *et al.* in [14] proposed a smart grid model based on blockchain and edge computing technology, PBEM-SGN, enhanced data privacy. Bhargava *et al.* in [15] proposed a blockchain-based swarm intelligence ecosystem framework, which used edge nodes as servers, used reward and punishment models to adjust stakeholder incentives, and demonstrated the feasibility of the method. Niyato *et al.* in [16] gave a resource for edge computing and a blockchain system based on mobile edge computing to optimize resource consumption. Leung *et al.* in [17] formalized a wireless blockchain framework for mobile edge computing, which offloaded computing intensive tasks to nearby edge computing areas. Zhang *et al.* in [18] proposed a computing offload scheme based on blockchain to ensure data integrity.

C. TRUST MANAGEMENT IN IOT

The traditional password management system is not suitable for the IoT architecture. To this, the trust management is introduced into the IoT. Hamid *et al.* in [19] proposed a trust-based service management technology which could calculate the credibility level for recommender and quickly select the best service provider. Kamran *et al.* in [20] formalized a trust management system for cross-domain which solved the problem of trust management for cross-domain communication. Ikram *et al.* in [21] gave a trust management model based on a multi-tier central agency and calculated the reliability of each device by introducing a trust server. Iuliana

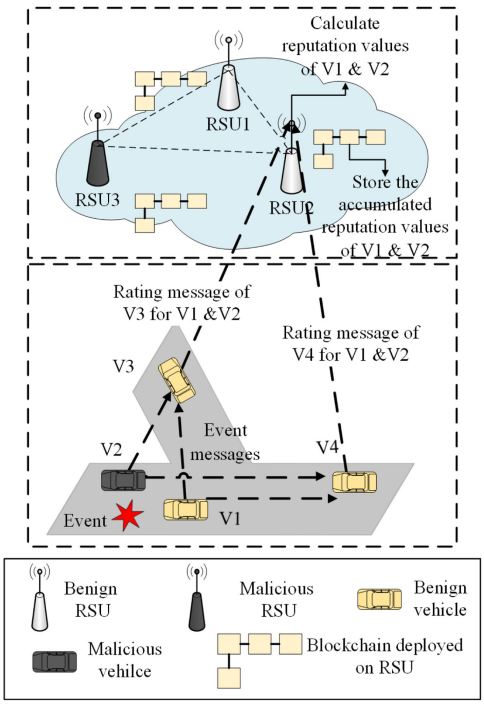


FIGURE 1. An example of blockchain-based IoV. Vehicles can share the messages of an event with each other. The vehicles that received the messages will rate them and upload the ratings to a nearby RSU. The RSU is responsible for calculating the reputation values of the vehicles that sent the event messages based on the ratings, and storing them on the blockchain deployed inside it.

et al. in [22] designed a trust management model for the learning management system of the university of Romania by introducing user trust. Panneerselvam *et al.* in [23] proposed a trust calculation scheme based on collaborative filtering which obtained the global trust value by calculating the direct trust value and the indirect trust value.

At present, most of the related researches of IoV based on blockchain used the tamper resistance of blockchain to achieve the security storage of vehicle information. But none of them considered the real-time nature of the blockchain update and the high mobility of the vehicle. Although [8] also considers this problem, it does not consider the possibility that RSU will upload false data.

III. APPLICATION SCENARIO AND SYSTEM MODEL

A. APPLICATION SCENARIO

Figure 1 illustrates a blockchain-based IoV scenario, which is composed of RSUs and vehicles equipped with various onboard sensors. When some vehicles (such as $V1$ and $V2$) sense an event (such as a car accident), they will broadcast the event messages to surrounding vehicles. Vehicles (such as $V3$ and $V4$) receiving the messages will make a decision (such as whether to detour) based on the actual situation of the event or their judgment of the event, and upload the ratings to a nearby RSU. The RSU will response for calculating the reputation value of the vehicle based on these ratings and store the calculated reputation value in the blockchain deployed inside it. Once the reputation values are stored in the blockchain, they cannot be changed.

We consider that there are n vehicles and k RSUs in IoV. Each vehicle and each RSU has its own unique ID. We use $\mathbb{V} = \{1, 2, \ldots, n\}$ to denote the set of all vehicles, use i to represent the vehicle receiving event messages and j to represent the vehicle sending event messages. The set of all RSUs is represented as $\mathbb{R} = \{1, 2, \ldots, k\}$. Vehicle i's rating for the message sent by the vehicle j can be expressed as γ_i^j. The RSU is responsible for calculating the authenticity of message according to the γ_i^j. If the authenticity of the message is too low, other vehicles will not consider it when judging the event [24].

However, not all vehicles and RSUs are benign, which makes the information in IoV not entirely credible. In this paper, we divide the threats into two categories: malicious vehicles attack and compromised RSUs attack.

Malicious Vehicles Attack. Vehicles deliberately send false messages in order to deceive other vehicles. According to the type of false message, malicious vehicles attack can be divided into the following two types:

1) *Information spoofing attack:* Vehicles send false event information to other vehicles which can lead to the vehicles making wrong judgments.
2) *Malicious rating attack:* Vehicles send false ratings to RSUs which causes RSUs to generate incorrect reputation values to affect the credibility of vehicles.

Compromised RSUs Attack. Attackers maliciously invade RSUs and cause them to behave incorrectly. According to the type of RSUs error behavior, this kind of attack can also be divided into the following two types:

1) *Data tampering attack:* The attacker tampers with the vehicle reputation values stored in RSUs after intruding into them.
2) *Algorithm tampering attack:* Attackers modify the algorithm for updating reputation values after invading RSUs, and make them produce incorrect results.

B. SYSTEM MODEL

To deal with the problem of malicious vehicles and compromised RSUs, we propose a blockchain-based trust management system of IoV. The system model is divided into two parts, one is a trust management model based on reputation value, the other is a blockchain-based data storage system. Then we briefly introduce the system model proposed in this article from these two parts.

1) TRUST MANAGEMENT MODEL BASED ON REPUTATION VALUE

To deal with the problem of malicious vehicles sending false messages, we introduced the concept of reputation values for vehicles.

Definition 1. *$r_j = F_1(\gamma_1^j, \gamma_2^j, \ldots, \gamma_i^j)$ represents the reputation value of the vehicle j at the current moment, which is*

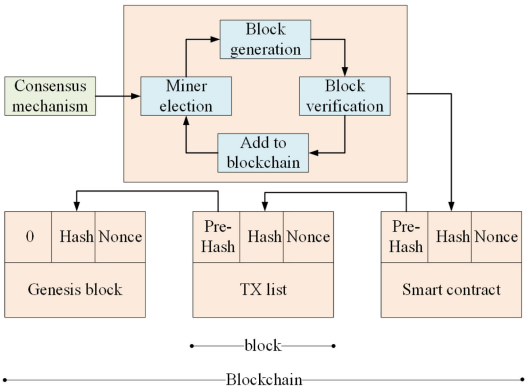


FIGURE 2. **Blockchain structure and workflow.**

the only criterion for the integrity of the vehicle j in this paper.

The vehicle reputation value cannot be calculated directly from the vehicle itself, which needs to be calculated by referring to the ratings of other vehicles on this vehicle, that is, it can be obtained by cross-verification method. During the cross-verification procedure, the vehicle needs an accurate judgment of the authenticity of the received message, so we introduced the concept of message credibility.

Definition 2. *$c_j = F_2(d_j, r_j)$ represents the credibility of the message sent by the vehicle j. d_j is the distance between the vehicle j and the event location. r_j represents the reputation value of the vehicle j.*

Taking the process of updating the reputation value of vehicle j as an example, we briefly introduce the trust management model in this paper. First, vehicle j broadcasts an event message to surrounding vehicles. After receiving the message, the vehicles will calculate the credibility c_j of the message, and each of them will generate a rating for the message from vehicle j in combination with the messages of the event sent by other vehicles. Then these vehicles will upload these ratings to a nearby RSU, and the RSU will calculate the reputation value of the vehicle j. At the same time, our model can also detect those false ratings, and will reduce the reputation values of the vehicles that send them.

2) BLOCKCHAIN-BASED DATA STORAGE SYSTEM

We design a blockchain-based data storage system to deal with the problem of attackers tampering with the data and algorithm in RSUs. Blockchain is a decentralized, peer-to-peer distributed storage system, whose specific structure is shown in Figure 2. Our blockchain-based data storage system has properties as follows.

Unforgeability. Blockchain supports users to add digital signature when uploading data, which can prevent malicious users from forging their data. By this, we can control malicious vehicles and RSUs cannot forge messages of benign vehicles.

Tamper Resistance. An ordered Hash list and a Merkel tree structure are used in the blockchain to ensure that the information is not tampered with. In our system, once the reputation values are recorded in the blockchain, it is impossible for an attacker to change them in the blockchain.

Uniformity. The smart contract is a program code written in the blockchain, which is automatically triggered when the input meets the conditions. Due to the immutable nature of the blockchain, the smart contract is unalterable. We write the reputation value update algorithm into the smart contract to ensure that all RSUs implement an unified reputation value update algorithm.

Verifiability. Before a block is added to the blockchain, it must go through a verification process. We change the content of block storage so that RSUs can monitor and verify each other to prevent malicious RSUs from stigmatizing the vehicles for each reputation value update.

Change-Sensitivity. We adopt a consensus mechanism combining PoW and PoS, so that vehicles with large changes in reputation will be updated to the blockchain first.

IV. TRUST MANAGEMENT SYSTEM BASED ON REPUTATION VALUE

Reputation value is an important standard to measure vehicle honesty. At present, most of the reputation value updating algorithms are based on the behavior records of the evaluated vehicles, most of which are obtained from other vehicles. But these records also have the possibility of counterfeiting, and it is easy for malicious vehicles to improve their reputation through several honest actions. Therefore, we design a new trust management scheme to solve these problems. The specific process of trust management is shown in Figure 3, and the specific steps are as follows:

Step 1: *Message Credibility Calculation.* When vehicle i receives the event messages sent from surrounding vehicles, it needs to calculate the credibility of the event messages c_j based on the reputation values of the surrounding vehicles, the distance between the surrounding vehicles and event location. The specific algorithm can be seen in Section IV-A.

Step 2: *Messages Summary.* After the vehicle i finishes the credibility calculation of all messages, it will get a credibility set $\mathbb{C} = \{c_1, c_2, \ldots, c_j\}$. Then the vehicle i will use this set to summarize all messages based on Bayesian inference, which can be seen in Section IV-B.

Step 3: *Rating Messages and Uploading.* After the vehicle i has the judgment of the event, it can choose to go to the event location to obtain the real value, and then rate the messages according to the real value, or rate the messages according to the judgment. Finally the vehicle i needs to upload the ratings to a nearby RSU, which is shown in Section IV-C.

Step 4: *Reputation Value Update.* After collecting the ratings, RSU uses a weighted aggregation algorithm based on the reputation value of the vehicles sending ratings to calculate the reputation value of the rated vehicles. In addition, RSU will punish the reputation values of vehicles that send false ratings, which can be seen in Section IV-D.

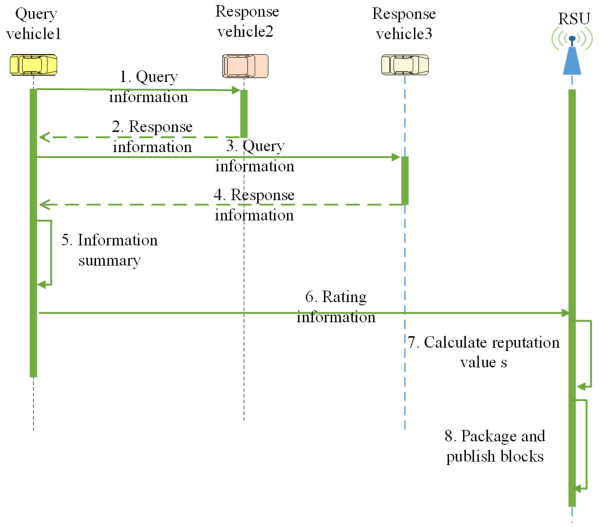


FIGURE 3. The reputation value update procedure. Vehicle 1 sends information query request to vehicle 2 and 3. 2 and 3 will send road condition information to 1 after receiving the request. After receiving the information, 1 will summarize it and rate the information according to the summary result. Then 1 will send the ratings to the RSU, which is responsible for collecting and calculating reputation values of vehicles, packaging it into blocks and releasing it.

By this, we realize the real-time update of the vehicles' reputation values, implement detection and punishment measures for vehicles with malicious behavior, and greatly improve the security of the IoV messages transmission.

A. MESSAGE CREDIBILITY CALCULATION

Due to factors such as the vehicle's own reputation value and the distance from the event, the information sent by the vehicle is not always true. In order to clarify the authenticity of each message, we define the information credibility and design the information credibility calculation method.

When a vehicle i needs to know the occurrence of the event E in a certain place, it will send a query message to other vehicles nearby. The vehicle j receiving the query message needs to send a response message about E to the vehicle i. We adopt the following formula to calculate the credibility of message sent by the vehicle j:

$$c_j = r_j \cdot e^{-\omega_1 d_j}, \tag{1}$$

where c_j is the credibility of information sent by vehicle j, r_j is the reputation value of the vehicle j which can be queried in RSUs, e is the natural constant, d_j is the distance between vehicle j and the location of E which can be obtained by calculating the position distance between them under GPS positioning, ω_1 is the weight coefficient used to control the weight of d_j in calculation.

Remark. By this method, we can get the authenticity of each piece of information, achieve the effect that r_j and c_j are higher when d_j is the smaller, which provides the calculation basis for the later messages summary.

B. MESSAGES SUMMARY USING BAYESIAN INFERENCE

Query vehicles will receive several messages about a common event from multiple vehicles, and they need to get the judgment of the event according to these messages. We formalize a messages summary scheme based on Bayesian inference, which can get the judgment result of the event more accurately.

After calculating the credibilities of all messages received about E, vehicle i will store them in $\mathbb{C}$, such as $\mathbb{C} = \{c_1, c_2 ... c_j ...\}$. Finally, it will summarize the information according to the following formula:

$$P(e|\mathbb{C}) = \frac{P(e) \cdot \Pi_{j=1}^{N} P(c_j|e)}{P(e) \cdot \prod_{j=1}^{N} P(c_j|e) + P(\bar{e}) \cdot \prod_{j=1}^{N} P(c_j|\bar{e})}, \tag{2}$$

where e and $\bar{e}$ refer to the positive and negative states of event E, N is the number of elements in $\mathbb{C}$, $P(c_j|e)$ and $P(c_j|\bar{e})$ are actually the credibility c_j of the information sent by the vehicle j, $P(e)$ and $P(\bar{e})$ are the prior probability of E, $P(e|\mathbb{C})$ is the aggregate credibility based on the credibility set $\mathbb{C}$, that is, the final probability of the possible occurrence of E, and $P(e|\mathbb{C}) \in [0, 1]$. When $P(e|\mathbb{C})$ exceeds the preset threshold Θ, vehicle i will consider the event E to be in the e state, otherwise, it will consider the event E in the $\bar{e}$ state.

Remark. By this, we realize messages summary considering credibility, which can reduce the influence proportion of low credibility messages in the process and improve the accuracy of judgment on event E.

C. RATING INFORMATION AND UPLOADING

To detect and punish vehicles that send malicious messages, we adopt a rating mechanism. The rating mechanism is based on whether the vehicle has a real value. It plays an important role in limiting malicious vehicles, because vehicles that send ratings do not necessarily have the true value of the event.

There are two ratings in the proposed mechanism, namely the initial rating and the final rating. The initial rating is divided into two types: positive rating and negative rating. The specific formula is

$$rate = \begin{cases} +1 & \text{Information is positive} \\ -1 & \text{Information is negative} \end{cases}. \tag{3}$$

The value of the final rating depends on the initial rating and whether the vehicle has a real value. The process of determining the final rating is described as follows.

Without Real Value. If vehicle i doesn't have a real value, it will rate the messages according to the summary result. The message consistent with the judgment result will be given a positive rating, otherwise a negative rating. As vehicle i has no real value, so it cannot guarantee that its initial rating is absolutely correct, whose grasp of the initial rating depends on the value of $P(e|\mathbb{C})$. So i's final rating for j is

$$\gamma_i^j = P(e|\mathbb{C}) \cdot rate. \tag{4}$$

With Real Value. If vehicle i has a real value, it will rate the messages based on the real value. The message consistent with the actual result will be given a positive rating, otherwise a negative rating. As vehicle i has the real value, so it can guarantee that its rating is absolutely correct, and the initial rating can be used as the final rating.

When vehicle i completes the messages rating, it needs to send the ratings to the nearby RSU, which is responsible for the collection of rating information and the update calculation of vehicle reputation values. In addition, all vehicles in our system are registered in the central government agency (such as vehicle administrative office). Each vehicle has its identity information including vehicle ID and a pair of public and private key, e.g., the identity information of vehicle i is $\{i, PK_i, SK_i\}$. When vehicle i needs to send ratings to RSU, it must sign the them with its private key. This cannot only ensure the traceability of the message, but also that the message will not be tampered and forged. In this paper, our signature method is elliptic curve digital signature algorithm (ECDSA) [25].

D. CALCULATING REPUTATION VALUES OF VEHICLES

After collecting ratings, we need to update the reputation values of vehicles. The vehicles that we update the reputation value are mainly divided into two categories, one is the rated vehicles, the other is the vehicles that send malicious ratings.

1) CALCULATING REPUTATION VALUES FOR RATED VEHICLES

As there are malicious vehicles, we need to calculate the vehicles reputation values according to the ratings as soon as possible after collecting the ratings, so as to achieve the purpose of punishing malicious vehicles and prevent them from causing more serious consequences. Therefore, we design a calculating method for reputation values, and realize the unified management of the reputation values of vehicles.

The RSU stores ratings in groups according to the ID of rated vehicles. For example, if there are multiple messages being rated for vehicle j in a RSU, they will be grouped and stored together. In each group, there will be a certain number of positive ratings, and a inevitable certain number of negative ratings. For example, for vehicle j's rating messages, there are 6 positive ratings and 4 negative ratings.

Because of the presence of malicious vehicles, we design a rating summation algorithm based on weighted aggregation of the reputation value sending ratings. At the same time, we formalize an inverse trigonometric function that maps the cumulative sum of ratings to a value in the range 0 to 1, and use it as vehicle reputation value. The specific formulas are

$$\Delta o_j = \sum_{i=1}^{N} r_i \cdot \gamma_i^j, \tag{5a}$$

$$o_j' = \begin{cases} o_j + \omega_2 \cdot \Delta o_j & \Delta o_j > 0 \\ o_j + \omega_3 \cdot \Delta o_j & \Delta o_j < 0 \end{cases}, \tag{5b}$$

$$r_j = \frac{1}{\pi} \arctan\left(\omega_4 \cdot o_j'\right) + \frac{1}{2}, \tag{5c}$$

where Δo_j represents the rating change sum of the vehicle j, N denotes the number of ratings about the vehicle j, r_i is the reputation value of vehicle i that rates vehicle j, γ_i^j is the rating given by the vehicle i. o_j' is the rating cumulative sum of the vehicle j at the latest time, o_j represents the rating cumulative sum of vehicle j at the previous moment, ω_3 and ω_4 are weight parameters, $\omega_2 < \omega_3$ means that the punishment intensity is higher than the reward intensity, r_j represents the latest reputation value of the rated vehicle j, and ω_4 is a parameter for adjusting the change rate of reputation value.

Eq. (5c) is a monotonically increasing function with a range of 0 to 1, which just guarantees that rating sums of the vehicle can have the same trend as the reputation value. In addition, it has a large rate of change when the function value is around 0.5 due to the inherent characteristics of the function. When the function value is close to 0 or 1, the rate of the function change will become very small. This is consistent with our actual life, that is, when the system is initialized, the reputation value caused by the behavior of the vehicle changes the fastest, and when it is accumulated for a long time, the change of the reputation value will become slower.

2) PUNISHING VEHICLES SENDING MALICIOUS RATINGS

Due to the presence of malicious vehicles in IoV, there are also false ratings stored in RSUs. We design a scheme for judging false ratings, and also provide a method for punishing the reputation value which further improves the security of IoV.

After Δo_j is calculated, we compare Δo_j with each rating for vehicle j, and consider the rating to be malicious if the positive and negative of them are inconsistent. For example, if Δo_j is positive and γ_i^j negative, then γ_i^j is a malicious rating and we need to adjust the reputation value of vehicle i that issued γ_i^j, update its rating cumulative sum. We perform a penalty for the reputation value reduction of these maliciously-sending vehicles according to the prescribed penalty coefficient whose value is 0.9, and obtain the updated rating cumulative sum according to the inverse function of Eq. (5c) at the same time. Then these vehicles can participate in the next round of reputation value update.

Remark. In order to limit the spread of false information in IoV, we design a new trust management scheme, the specific algorithm steps are shown in Algorithm 1. Lines 9-16 represent the update process of the reputation values of rated vehicles. We add the reputation values as the weight for ratings, reducing the possibility of ratings fraud. In addition, we have specially increased the punishment of vehicle evildoing,

which makes it difficult to improve the reputation value rapidly. Lines 17-26 represent the reputation values update process for vehicles that send false ratings. We set penalty parameters for the behavior vehicle, reducing the possibility of rating fraud.

Algorithm 1. Reputation Value Updating Algorithm

Input: Rating information list ***Rating_List***; reputation value adjustment parameters ω_2, ω_3, ω_4
Output: Reputation value dictionary of each vehicle *r_dict*; rating sum dictionary of each vehicle *o_dict*.
Initialize $r\_dict = \phi$, $o\_dict = \phi$;
Create a empty list of rated vehicles ***rated_list***;
repeat
  if v_j not in ***rated_list*** **then**
    $rated\_list \leftarrow v_j$;
  end
until v_j *not in* ***Rating_List***
repeat
  Query the sum of current vehicle ratings o_{last}
  repeat
    if $v_j == v_r$ **then**
      Query reputation value r_i of rating vehicle v_i;
      Calculate rating change sum Δo_v according to Eq. (5c);
      Calculate cumulative rating sum o_v according to Eq. (5b);
      Calculate reputation value r_j of rated vehicle v_j according to Eq. (5c);
    end
  until v_r *not in* ***Rating_List***
  repeat
    if $v_r == v_j$ **then**
      if $rate * \Delta o_v < 0$ **then**
        $r_i = 0.9 * r_i$;
        Calculate vehicle rating sum o_i according to the inverse function of Eq. (5c);
        $r\_dict \leftarrow v : r_i$;
        $o\_dict \leftarrow v : o_i$;
      end
    end
  until v_r *not in* ***Rating_List***
  $r\_dict \leftarrow v : r_j$;
  $o\_dict \leftarrow v : o_j$;
until v_j *not in* ***rated_list***
Return *r_dict* and *o_dict*.

V. BLOCKCHAIN-BASED DATA STORAGE SYSTEM

To prevent attackers from maliciously tampering with data, we design a blockchain-based system of IoV. In addition, we adopt a consensus mechanism combining PoW and PoS to update the vehicles with great changes in reputation value first. Then, we store the reputation value and rating list inside the block body, so that RSUs have a calculation basis when verifying the reputation values in the blocks. Finally, we write the reputation value update method into the smart contract to ensure that RSU calculates the vehicle reputation value according to the correct method.

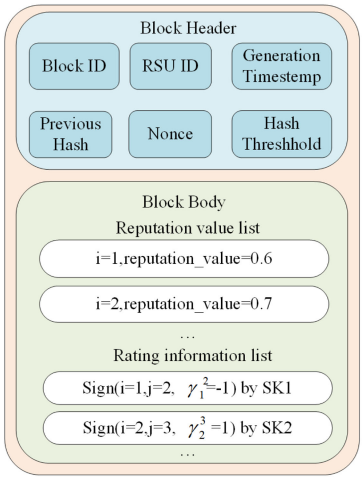


FIGURE 4. **Structure of generated blocks.**

A. REPUTATION VALUE UPDATING BASED ON SMART CONTRACT

To prevent the attacker from controlling its behavior by invading the RSU and make it calculate the reputation value according to the wrong algorithm, we write the update algorithm of the reputation value into the smart contract and deploy it on the blockchain. The smart contract cannot be changed once it is deployed on the blockchain. When the RSU needs to calculate the reputation value, it only needs to call the smart contract, and the algorithm in the contract will be automatically executed.

Besides ensuring consistency in the calculation of reputation values, smart contract can also simplify the verification process of blocks. Other RSUs only need to call the smart contract when verifying the block, substitute the rating in the block into the smart contract and execute it once. As long as the result is consistent with the reputation value in the block, the block is considered to be correct.

B. BLOCK STORAGE CONTENT

To make the RSUs have the data basis when verifying the block, we modify the storage content of the block shown in Figure 4, which shows a general structure of the block. In the block header, we store the hash value of the previous block, the hash value of current block, the height of current block, the random number and other information. We store the vehicle reputation values and ratings in the block body as transactions. We store the transactions in the form of Merkle tree.

In previous studies, rating list is not saved on blocks. Therefore, when an RSU broadcasts a block to other RSUs, the correctness of the block cannot be fully verified. In addition, because we designed a malicious rating detection mechanism

(see Section IV-D2) in trust management, the mechanism does not need to view the road condition information sent by vehicles. Therefore, we remove the road condition information from the block, which will make the same size block can store more transactions than before. We take 10 KB for each transaction, so the traffic information may account for 5 KB. If each block contains 500 transactions, then our scheme can reduce 2.4 MB memory for each block, which will bring good memory scalability for the whole blockchain.

C. CONSENSUS MECHANISM OF COMBINATION OF POW AND POS

The authenticity of the information of the vehicles whose reputation value changes greatly also changes greatly. Therefore, it is important for the security of IoV to ensure that these vehicles with large reputation value changes are updated first. In other words, we need an RSU that contains a larger amount of vehicle reputation value change to be able to more easily obtain the right to publish a block.

We use a consensus mechanism that combines PoW and PoS, which proposed in [8]. It uses the sum of the absolute values for all vehicles' average rating change stored in the RSU as stake to design mining difficulty. The specific process of the consensus mechanism is very similar to PoW. First, all RSUs will calculate according to the mining difficulty. When one RSU is the first to calculate the hash value satisfying the difficulty, it can broadcast the block to other RSUs. When the block passes the verification of most RSUs, it can be added to the blockchain. The only difference from PoW is that the mining difficulty of each RSU is different. Next, we introduce the design of mining difficulty in detail. The mining formula is

$$\text{Hash}(\text{Header}\ ) \leq D_k, \tag{6}$$

where D_k is the mining difficulty threshold of RSU k, RSU k needs to change the random number *Nonce* in block header until it is consistent with the above formula. The first RSU completing the task can obtain the right to publish the block.

The specific calculation formulas of D_k are

$$\overline{\Delta o_j} = \frac{\Delta o_j}{\sum_{r_i \in G_j} r_i}, \tag{7a}$$

$$O_k = \sum_{\overline{\Delta o_j} \in RSU_k} \left|\overline{\Delta o_j}\right|, \tag{7b}$$

$$N_Z = \text{int}\left(e^{-(\omega_5 O_k + \omega_6)}\right), \tag{7c}$$

$$D_k = 2^{N_M - N_Z} - 1, \tag{7d}$$

where $\overline{\Delta o_j}$ is the weighted average rating change for each vehicle in RSU k, G_j is the rating group for the vehicle j in RSU k, O_k represents the sum of $\overline{\Delta o_j}$ of all vehicles in the RSU k, $int(\cdot)$ is a downward rounding function, N_M represents the total number of bits of D_k, The hash algorithm we use here is $SHA-256$ algorithm, so N_M takes 256 here, N_Z represents the number of consecutive zeros in the beginning of D_k. The larger O_k is, the fewer zeros are. The fewer zeros are, the lower mining difficulty is, and the easier it is for RSUs to obtain the right to publish blocks.

Remark. In order to ensure that vehicles with large reputation value changes can be updated to the blockchain preferentially, we use a consensus mechanism combining PoW and PoS, the details can be seen in Algorithm 2. Lines 2-9 represent the calculation process of the sum of the rating changes of all vehicles included in each RSU. Lines 10-11 indicate that we design targets with different difficulty according to the sum of ratings within each RSU. The larger the sum, the less difficult the target is. Lines 12-18 represent the process of RSUs mining. In order to verify the efficiency of the consensus mechanism, we have simulated it, and the simulation result is placed in Section 7.

Algorithm 2. Consensus Mechanism Algorithm

Input: Rating information list ***Rating_List***; mining difficulty parameters ω_5, ω_6
Output: Random number ***Nonce*** meeting mining conditions
Initialize Cumulative sum of ratings $\boldsymbol{O_k}$ in RSU_k, random number ***Nonce***, number of consecutive 0 digits in mining difficulty $\boldsymbol{N_Z}$ and number of total bits of mining difficulty $\boldsymbol{N_M}$, list of rated vehicles from **Algorithm 1** *rated_list*;
repeat
  repeat
    if $v_j == v_i$ **then**
      Query reputation value r_i of rating vehicle v_i;
      Calculate O_k according to Eqs. (7a) and (7b);
    end
  until v_i *not in* ***Rating_List***
until v_i *not in* ***Rating_List***
Calculate $\boldsymbol{N_Z}$ according to Eq. (7c);
Calculate $\boldsymbol{D_k}$ according to Eq. (7d);
repeat
  Nonce $= 0$;
  repeat
    Nonce $=$ ***Nonce*** $+ 1$;
    Replace ***Nonce*** in block header;
  until $Hash(Block\_Header) >= \boldsymbol{D_k}$
until *one RSU mining successfully*
Return *Nonce*

D. BLOCK VERIFICATION

Block verification is the last line of defense to ensure that the data is correct. When a RSU packs a block and broadcasts it after successfully mining, other RSUs receiving the block are responsible for verifying it. Because we use the smart contract to write the reputation value update algorithm, the RSUs only need to re-invoke the smart contract when

verifying the block, and re-run it with the ratings in the block. If the result is consistent with the block, then the block passes the verification. Otherwise, the block will not pass verification. Only when the block passes the verification of most nodes can it be published in the blockchain and become the data that can never be tampered with.

VI. SECURITY ANALYSIS

In this section, we conduct security analysis from the following two aspects.

A. DEFENSE AGAINST MALICIOUS VEHICLES ATTACKS

Defense Against Information Spoofing Attack. When a vehicle i sends false road condition information, we can judge it by Eq. (2) and the real road condition. When confirming that the information of i is false, we can reduce its reputation value by Eqs. (5a), (5b), (5c). Assuming that there has been malicious behavior in i for a period of time T, its reputation value can be expressed by the following formula:

$$r_i = \frac{1}{\pi} arctan(\omega_4(o_i + \omega_3 \sum_{t}^{T} \Delta o_i^t)) + \frac{1}{2}, \tag{8}$$

where ω_3 and ω_4 are default parameters, o_i is the sum of current ratings of i, Δo_i^t is the sum of the ratings of other vehicles on i in time slot t. Because the information of i is false, other vehicles have negative rating on it, so $\Delta o_i^t < 0$. Therefore, with the passage of time, the sum of ratings of vehicle i will be lower and lower, and its reputation value will also be reduced. It is obvious that there must be a value of T, which makes the following formula hold:

$$\sum_{t}^{T} \Delta o_i^t < \frac{tan((\theta - \frac{1}{2})\pi) - \omega_4 o_i}{\omega_3 \omega_4}, \tag{9}$$

where θ is the minimum limit of reputation value. At this time, the reputation value r_i of i is less than θ, it will be forbidden to participate in the IoV. So our scheme can defend against the information spoofing attack.

Defense Against Malicious Rating Attack. When receiving false rating information for some vehicles, RSUs use a weighted aggregation scheme for ratings to calculate vehicle reputation values. When vehicle i sends false ratings within a period of time T, its reputation value will be adjusted according to the following formula:

$$r_i = \frac{1}{\pi} arctan(0.9^t \omega_4 o_i) + \frac{1}{2}, \tag{10}$$

where t represents the number of rounds of reputation value update in time T. Obviously, with the increase of the number of update rounds, the reputation value r_i of I will gradually decrease. Moreover, there must be a value of t, which makes the following formula hold:

$$\lambda^t o_i < \frac{tan((\theta - \frac{1}{2})\pi)}{\omega_4}, \tag{11}$$

where λ is the penalty coefficient of sending malicious rating vehicle reputation value. At this time, $r_i < \theta$, vehicle i will be forbidden to participate in the IoV. So our scheme can defend against malicious rating attack.

B. DEFENSE AGAINST MALICIOUS RSUS ATTACKS

In this paper, we set that the total number of all RSUs must be more than three times that of malicious RSUs. Through this setting, we can ensure the consistency of honest RSUs. We take four RSUs as an example, one of which is malicious. For the convenience of proof, we label them with 1, 2, 3 and 4, in which 1 is responsible for issuing blocks and the others are responsible for receiving blocks.

If 1 is a malicious RSU, it will send different blocks to other RSUs. We label the blocks with A and B. The process can be expressed as:

$$1 \rightarrow 2 : A,$$
$$1 \rightarrow 3 : B,$$
$$1 \rightarrow 4 : A.$$

At this time, 2, 3 and 4 will ask each other about the content of the block, and they will not lie to each other. After that, the block content obtained by each RSU is (A, A, B). They will add A (larger scale block) to the blockchain to ensure consistency.

If one of 2, 3 and 4 is a malicious RSU, take 2 for example, 1 will send the same block to them, assuming it is A. The process can be expressed as:

$$1 \rightarrow 2 : A,$$
$$1 \rightarrow 3 : A,$$
$$1 \rightarrow 4 : A.$$

Then, 2, 3 and 4 will ask each other. Since 2 is malicious, it will tell 3 and 4 that block is B, while 3 and 4 will both say block is A. Finally, the block list obtained in each RSU is:

$$2 : (B, A, A),$$
$$3 : (A, A, B),$$
$$4 : (A, A, B).$$

At this point, honest 2 and 3 will add A to the blockchain. Through the above analysis, it is proved that our scheme can resist the malicious RSUs attack.

VII. EXPERIMENTAL PERFORMANCE EVALUATION

To verify the feasibility and efficiency of the model built in this paper, we performed the system simulation using the Ethereum platform. In this experiment, we simulate the real environment of IoV including benign vehicles and RSUs, as well as malicious vehicles that send false information and

TABLE 1. Key parameter value table.

Parameters	Values
ω_1	0.001
d_j	$d_j \sim U(0, 500)$
Θ	0.5
λ	0.9
ω_2	1
ω_3	4
ω_4	0.02
ω_5	0.01
ω_6	-3

malicious RSUs that publish false blocks. The values of the parameters used are given in Table 1. The simulation results are divided into the following four aspects.

A. EVENT INFORMATION SUMMARY ACCURACY RATE

We simulate the accuracy of the vehicle's judgment of the event condition based on the received information. We take 20 vehicles as information receiving vehicles. Each vehicle receives information from 10 vehicles and judges the event situation based on it. There are different numbers of malicious vehicles in the 10 vehicles sending false event information. We conduct a study on the accuracy of event situation judgments for these 20 vehicles. To show the accuracy of event judgment more clearly, we introduce the method proposed in [8] as the benchmark. This method takes the distance between vehicles as the main reference for its information credibility. This kind of method is widely used in the information judgment process of IoV, so this method has a good representativeness and is very suitable as a benchmark. The result is shown in Figure 5.

The solid lines in Figure 5 represent the simulation results of the proposed scheme, and the dotted lines are the simulation result of the proposed scheme in [8]. We conducted 20 experiments on each proportion of malicious vehicles, and took the maximum, minimum and average values of the correctness of the event situation. It can be seen from Figure 5 that the lower the proportion of malicious vehicles, the higher the accuracy of the vehicle receiving the information to determine the road condition, especially when the proportion of malicious vehicles is 60 percent, the accuracy of the event situation obtained by the proposed scheme still guaranteed at around 70 percent. The scheme proposed in this paper is higher in the accuracy of road condition judgment than the scheme in [8], because the scheme in the reference only considers the distance factor for information credibility, which does not consider the vehicle reputation values, so the information credibility may produce relatively large errors.

B. VEHICLE REPUTATION VALUE RESTRICTIONS ON MALICIOUS VEHICLES

To show the deception prevention of the proposed trust management scheme, we simulate the change of reputation value

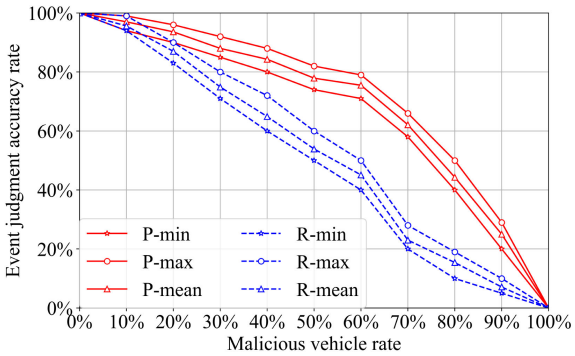


FIGURE 5. Event judgment accuracy rate (P:Proposed method R: Reference method [8]).

caused by vehicle behavior. To show it more clearly, we introduce Trust Management based on Evidence Combination (TMEC) scheme in [23] as the benchmark. This scheme is a combination of direct reputation and indirect reputation, based on the historical interaction records, and has a good representativeness in the application of the IoV. The simulation results are shown in Figure 6. In time slot 0-6, the vehicle interacts honestly. In both schemes, vehicle reputation value increases. In time slot 6-12, the vehicle interacts maliciously. It can be seen that the punishment intensity of our scheme is higher than the benchmark, and the reputation value drops faster. In time slot 12-20, the vehicle reacts with honest interaction. It can be seen that the recovery speed of reputation value in our scheme is significantly slower, which can prevent vehicles from deliberately increasing their reputation value in a short time. Therefore, our scheme has higher deception prevention on malicious behavior of vehicles.

Then we mainly study the limitation of reputation value on the two types of malicious vehicles: vehicles with malicious event information (VMEI) and malicious rating information (VMRI). We take 50 vehicles as research objects with 50 percent being VMEI. Based on the correctness of the event occurrence information they send, the system evaluates their reputation values and identifies vehicles with reputation values below 0.3 as malicious vehicles and excludes them. At the same time, the evaluation process is divided into two

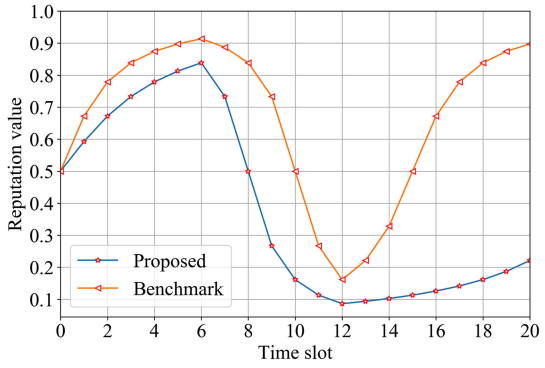


FIGURE 6. Reputation value change trend.

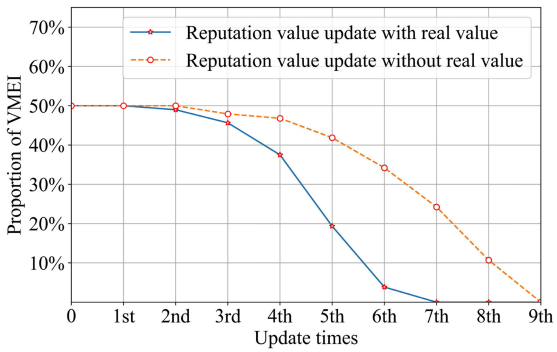


FIGURE 7. Restriction of reputation value to VMEI (vehicles with malicious event information).

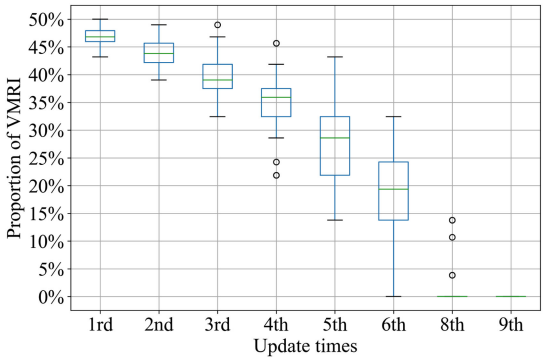


FIGURE 8. Restriction of reputation value to VMRI (vehicles with malicious ratings information).

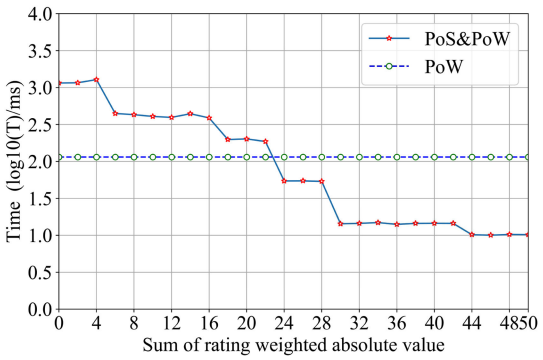


FIGURE 9. Block generation time.

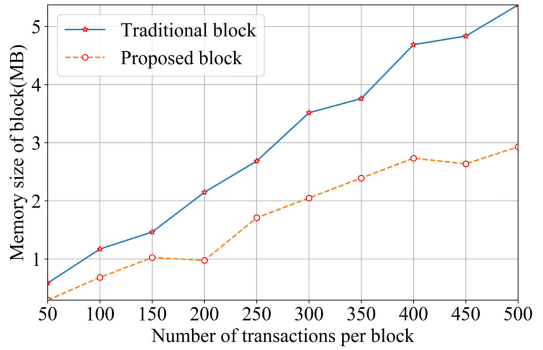


FIGURE 10. Block occupied memory.

categories according to whether the vehicles sending ratings have real values, which is shown in Figure 7. The solid line indicates the evaluation effect with the true value, and the dotted line indicates the evaluation effect without the true value. It can be seen that the malicious vehicles are all eliminated after 7 rounds of reputation value update in the case of real value, and the effect of the reputation value on the malicious vehicle is relatively poor in the absence of real values. After 9 rounds of reputation value update, all malicious vehicles will be excluded.

After that, we still take 50 vehicles as research objects including 50 percent of VMRI. We conducted 50 experiments and the results are given in Figure 8. The box diagram clearly shows the maximum, minimum and average values of the proportion of remaining VMRI in each of the 50 vehicles after the update of reputation value of all 50 experiments. After the 8th round of the update of reputation values, there were only a few VMRI remaining in the 3 experiments. In other cases, all malicious vehicles have been eliminated. In the 9th round of the update of reputation values, all the malicious vehicles in the 50 vehicles of all 50 experiments are eliminated.

C. DELAY IN UPDATE OF REPUTATION VALUE

When RSUs pack the calculated reputation values into blocks and upload them to the blockchain, the reputation values are updated. Therefore, the update delay of the reputation values mainly depends on the time taken by RSUs to mine according to the consensus mechanism. This paper adopts the consensus mechanism of PoW and PoS. The mining time is determined by O_k, the sum of the absolute values of the rating changes of all vehicles in RSUs. We compare the mining time of this model with the mining time using the PoW consensus mechanism with the results in Figure 9. As can be seen from Figure 9, when the O_k exceeds 24, our scheme will have a smaller delay in updating the vehicle reputation value. Therefore, we will try to keep the total change of rating in RSU more than 24, such as increasing the number of internal storage vehicles in each RSU, so as to ensure the low delay characteristics of the system.

D. MEMORY SCALABILITY

In the current research of IoV based on blockchain, most of the work adds the road information sent by vehicles to the block. And road information is much more memory than reputation value and rating. We delete the traffic information from the block, which greatly reduces the block memory. Because we use message signature mechanism and design malicious rating detection mechanism (see Section 4.4.2), we can avoid the risk of tampering with road information. From Figure 10, we can see that the memory of the block in our scheme is much smaller than that of traditional

block, so we can conclude that our scheme has better memory scalability.

VIII. CONCLUSION

In this paper, we proposed a trust management system of IoV based on blockchain. The system could help vehicles to calculate the credibility of the received information and improve the accuracy of the vehicles' judgment on the event situation information. At the same time, it provided a vehicle reputation value update algorithm, which played a good role in limiting malicious vehicles. The blockchain was used for data storage and sharing, which made the security of the data to be greatly guaranteed. We adopted a consensus mechanism so that vehicles with large changes in reputation would be updated preferentially. There are still some areas for further study in this paper, such as designing a new consensus mechanism to make mining time shorter and reduce the delay of trust management system of IoV while ensuring data security. It is believed that the trust management system of IoV based on blockchain plays a very important role in the security and stability of IoV.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (61771373, 61771374, 61801360, and 61601357), in part by Natural Science Basic Research Program of Shaanxi (2020JC-15 and 2020JM-109), in part by Fundamental Research Funds for the Central Universities (3102019PY005, 31020190QD040, and 31020200QD010), in part by Special Funds for Central Universities Construction of World-Class Universities (Disciplines) and Special Development Guidance (06390-20GH020114).

REFERENCES

[1] R. Silva and R. Iqbal, "Ethical implications of social internet of vehicles systems," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 517–531, Feb. 2019.

[2] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for vehicle-to-everything services," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 38–45, Dec. 2017.

[3] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep. 2017.

[4] I. Garcia-Magarino, S. Sendra, R. Lacuesta, and J. Lloret, "Security in vehicles with IoT by prioritization rules, vehicle certificates, and trust management," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5927–5934, Aug. 2019.

[5] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[6] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[7] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9098–9111, Oct. 2019.

[8] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[9] L. T. Tan and R. Q. Hu, "Mobility-aware edge caching and computing in vehicle networks: A deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10 190–10 203, Nov. 2018.

[10] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart vehicles," *IEEE Netw.*, vol. 32, no. 3, pp. 42–51, May/Jun. 2018.

[11] F. Zhou, R. Q. Hu, Z. Li, and Y. Wang, "Mobile edge computing in unmanned aerial vehicle networks," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 140–146, Feb. 2020.

[12] G. Liu, Y. Xu, Z. He, Y. Rao, J. Xia, and L. Fan, "Deep learning-based channel prediction for edge computing networks toward intelligent connected vehicles," *IEEE Access*, vol. 7, pp. 114 487–114 495, 2019.

[13] Z. Ning, J. Huang, X. Wang, J. J. P. C. Rodrigues, and L. Guo, "Mobile edge computing-enabled internet of vehicles: Toward energy-efficient scheduling," *IEEE Netw.*, vol. 33, no. 5, pp. 198–205, Sep./Oct. 2019.

[14] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[15] J. Xu, S. Wang, B. K. Bhargava, and F. Yang, "A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3538–3547, Jun. 2019.

[16] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[17] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11 008–11 021, Nov. 2018.

[18] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "Become: Blockchain-enabled computation offloading for IoT in mobile edge computing," *IEEE Trans. Ind. Inform.*, vol. 16, no. 6, pp. 4187–4195, Jun. 2020.

[19] H. Al-Hamadi, I. Chen, and J. Cho, "Trust management of smart service communities," *IEEE Access*, vol. 7, pp. 26 362–26 378, 2019.

[20] K. A. Awan, I. U. Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, "Robusttrust–A pro-privacy robust distributed trust management mechanism for internet of things," *IEEE Access*, vol. 7, pp. 62 095–62 106, 2019.

[21] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things," *IEEE Access*, vol. 7, pp. 52 191–52 201, 2019.

[22] I. Dorobat, A. M. I. Corbea, and M. Muntean, "Integrating student trust in a conceptual model for assessing learning management system success in higher education: An empirical analysis," *IEEE Access*, vol. 7, pp. 69 202–69 214, 2019.

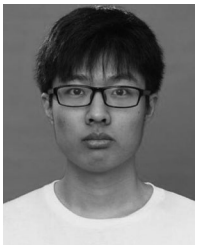
[23] J. Chen, T. Li, and J. Panneerselvam, "TMEC: A trust management based on evidence combination on attack-resistant and collaborative internet of vehicles," *IEEE Access*, vol. 7, pp. 148 913–148 922, 2019.

[24] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[25] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

HAIBIN ZHANG (Member, IEEE) received the BS degree in applied mathematics from the Ocean University of China, in 2003, and PhD degrees in computer science and technology from Xidian University, in 2007. He is currently a professor with the School of Cyberspace Security, Northwestern Polytechnical University. His research interests include concentrate on formal verification, artificial intelligence, IoT. He has published more than 30 peer-reviewed papers in various pre stigious journals and conferences, including the *IEEE Internet of Things Journal* and *IEEE Systems Journal*.

JIAJIA LIU (Senior Member, IEEE) is currently a full professor with the School of Cybersecurity, Northwestern Polytechnical University. His research interests include cover wireless mobile communications, FiWi, IoT, and more. He has published more than 180 peer-reviewed papers in many prestigious IEEE journals and conferences, and currently serves as an associate editor for the *IEEE Transactions on Wireless Communications* and *IEEE Transactions on Vehicular Technology*, an editor for the *IEEE Network*, and a guest editor the *IEEE Transactions on Emerging Topics in Computing* and *IEEE Internet of Things Journal*. He is a distinguished lecturer of IEEE ComSoc.



HUANLEI ZHAO (Student Member, IEEE) received the BS degree in computer science and technology from the Xidian University of China in 2018. He is currently working toward the MS degree in the School of Cyber Engineering, Xidian University, Xian, China. His research interests include blockchain, trust management, Internet of things.

PENG WANG (Student Member, IEEE) received the BEng degree in software engineering from the Harbin Institute of Technology, Harbin, China, in 2017. He is currently working toward the PhD degree in cyber engineering at Xidian University, Xi'an, China. His research interests include blockchain, access control, and Internet of things.

NEI KATO (Fellow, IEEE) is a full professor (deputy dean) with the Graduate School of Information Sciences (GSIS) and the director of Research Organization of Electrical Communication (ROEC), Tohoku University, Japan. He has been engaged in research on computer networking, wireless mobile communications, satellite communications, ad hoc & sensor & mesh networks, smart grid, AI, IoT, big data, and pattern recognition. He has published more than 400 papers in prestigious peer-reviewed journals and conferences. He is the vice-president (Member & Global Activities) of IEEE Communications Society (2018–2019), the editor-in-chief of the *IEEE Transactions on Vehicular Technology* (2017–), and the chair of the IEEE Communications Society Sendai Chapter. He served as the editor-in-chief of the *IEEE Network Magazine* (2015–2017), a Member-at-Large on the Board of Governors, IEEE Communications Society (2014–2016), a vice chair of fellow Committee of IEEE Computer Society (2016), and a member of IEEE Communications Society Award Committee (2015–2017). Heis a distinguished lecturer of the IEEE Communications Society and Vehicular Technology Society. He is also a fellow of The Engineering Academy of Japan and IEICE.