Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 16, No. 3, 2025

Vehicle reputation value management scheme based on data uplink rules

Cong Zhang *, Peiqian Liu, Shan Ao

College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China

* **Corresponding author**

Abstract: Aiming at the security problems caused by the long-standing lack of trust between vehicles in the Internet of vehicles, a vehicle reputation-value management scheme based on data uplink rules is designed. value management scheme based on data uplink rules is designed. First, users release specific tasks according to their needs. First, users release specific tasks according to their needs. The blockchain generates smart contracts and conducts broadcast transactions within the scope of RSU to find vehicles to complete the tasks. The blockchain generates smart contracts and conducts broadcast transactions within the scope of RSU to find vehicles to complete the tasks. Finally, the credibility of the vehicle is comprehensively evaluated through multi-type vehicle weight, peripheral recommendations, rewards and punishment meschanisms, and the smart contract updates the reputation value of the vehicle in real time. Experiments show that the application of reputation management scheme in the Internet of vehicles is necessary, and the information trust evaluation and reputation integral algorithm are effective. Experiments show that the application of reputation management scheme in the Internet of vehicles is necessary, and the information trust evaluation and reputation integral algorithm are effective.

Keywords: Blockchain; Data uplink rules; Reputation value; Reputation integral algorithm; Smart contracts.

1. Introduction

In recent years, with the rapid development of Telematics technology makes the interaction between vehicles and the surrounding environment more and more close, realizing the comprehensive integration of intelligent vehicles and the surrounding environment, and integrating the public infrastructure, sensors, computing nodes, pedestrians and other diversified elements into a unified network system [1]. By building a comprehensive information exchange platform between vehicles and heterogeneous networks, it not only strengthens the safety and security of users, but also promotes the significant improvement of the public environment and spatial quality. However, this open access environment also brings serious security challenges such as vehicle information reliability and vehicle trust, and it is urgent to find effective solutions [2, 3]. The nodes in vehicular networking are large and widely distributed, and highly dynamic. In this environment, the information received by vehicles often comes from many unfamiliar vehicles, which are inevitably mixed with some malicious vehicles. These malicious vehicles may intentionally spread false messages, thus interfering with the normal driving of other vehicles and bringing potential security risks to the whole transportation system [4]. The traffic system is potentially a safety hazard.

Blockchain technology, with its decentralization, anonymity and strong trust mechanism, has been widely used and promoted in many industries [5, 6]. Smart contracts deployed in blockchain, as an automatically executed computer program, can ensure the transparency and fairness of the contract execution process, thus providing users with a more reliable and efficient contract execution mechanism [7]. The smart contracts deployed in blockchain, as an automatically executed computer program, can ensure the transparency and fairness of the contract execution process, thus providing users with a more reliable and efficient contract execution mechanism.

For the management of vehicle reputation, many scholars have proposed different schemes.Liu et al[8]. proposed a scheme for a blockchain-based reputation system, in which the reputation of a vehicle is constructed based on the ratings with the consent of the rating provider, and the ratings are not abused by any other unauthorized entity in the process of use, and are well protected in the process of transmission and storage.Liu et al[9] proposed a blockchain security-assisted reputation management scheme. In the vehicle sharing process, factors such as familiarity, timeliness, and trajectory similarity are taken into account, opinions are fully weighted, and the SL trust model is used to compute the reputation value combining both direct and indirect opinions, which improves the multiscale and accuracy of reputation value computation.Lu et al[10] proposed an anonymous blockchain based reputation system using two blockchains (CerBC and RevBC) for authentication which is used to break the link between real identity and public key, design reputation management algorithms for trusting communications to prevent the propagation of forged messages and to incentivize vehicles to expose misbehavior. Adnan M et al[11] proposed a distributed trust management system that maintains the trust of all reputation segments in an IoV network. The reputation segments are considered collectively to determine the outcome of direct interaction between the principal and trustee and by obtaining suggestions from the neighboring vehicles of the said trustee in order to accurately determine their trust scores, which are evaluated by subjective logic approach, similarity and timeliness to determine the weights of all the reputation segments.Tang et al[12] Design a lightweight reputation-based mechanism for hybrid vehicular networks that enables real-time reputation updates and synchronization in the device-edge cloud continuum.

Comprehensively, the above studies, blockchain technology is applied to the vehicle reputation management system to realize the protection of vehicle privacy information. However, when constructing the blockchain, the

computational and storage capacity of the vehicle is not considered, and some of the studies produce a large amount of computational overhead, and the frequency of data transactions and the size of the data volume in the process of data transmission are the key elements of reputation management. In the judgment of information credibility, most of them ignore the influence of other factors on the credibility of vehicle information, and there may also be information sending vehicles that obtain high credibility value through normal operation, so the weight allocation of credibility value is also a key influencing factor. In order to solve the above research problems, a vehicle reputation value management scheme based on data uplink rules is proposed. Main Contributions:

A vehicle reputation value management scheme based on data on-chain rules is designed. In this scheme, the user completes registration through SM2 elliptic curve public key cryptography algorithm, releases specific tasks, the blockchain generates a smart contract and broadcasts the transaction within the RSU, looks for information to send the vehicle to complete the task, and updates the reputation value of the vehicle in real time according to the quality of task completion.

Introduce data uplink rules. Determine the type of data, choose the data uplink method (real-time uplink or batch uplink), store it on the blockchain, ensure the integrity and authenticity of the data with the help of technologies such as hash algorithms and digital signatures, and finally, determine the authority and access control mechanism for data uplink to protect the privacy of the users and the security of the data.

According to different vehicle types, different data trust weights are assigned, reference is made to the recommended trust values of the recommended vehicles in the neighborhood, a reward and punishment mechanism is introduced to comprehensively assess the trustworthiness of the vehicles, and the reputation values of the vehicles are updated in real time according to the smart contract.

The remaining sections are organized as follows. In Section II, the system model of this scheme is designed. In Section III, the vehicle reputation value management scheme based on data uplink rules is described in detail. Section IV, introduces the data uplink rules and details the data uplink process. Section V, analyzes the average vehicle speed affected by obstacles, sets up a control experiment to compare the changes in the reputation value of message-sending vehicles with the increase in the number of message interactions, and analyzes the effectiveness of the message trust assessment, and the effectiveness of the reputation points algorithm. Finally, section VI summarizes the whole scheme.

2. System Model

The model of the vehicle reputation value management scheme is shown in Fig. 1, which is composed of four main parts, including RSU (Road Side Unit, RSU), blockchain, smart contract and vehicle.

RSU: It has a large coverage area and abundant computing resources. It is mainly responsible for the registration of vehicle users, providing the basic information of vehicles when they release tasks, broadcasting transactions within its coverage, and synchronizing information for each user.

Blockchain: distributed ledger technology with features such as decentralization, security, transparency and traceability.

Smart Contract: It can automatically execute the conditions and terms specified in the contract. Deployed on the RSU, it is mainly responsible for selecting the best vehicle to send the message, assigning the task, and uplink the task data to the designated location to ensure that the whole process is smooth and error-free.

Vehicles: divided into vehicles for receiving information and vehicles for sending information.

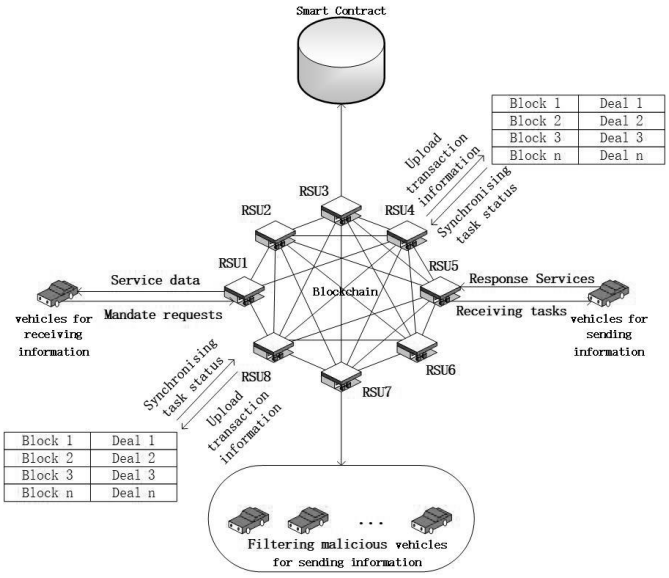

Figure 1. System model

3. Vehicle reputation value management scheme based on data uplink rules

3.1. User registration

Table 1. Vehicle registration

Inputs: user type VehType, vehicle user V, roadside unit R, vehicle arithmetic CP, real position of roadside unit Lrsu(xi,yi)

Output: block and user database DBu

1)if V or R ∉DBu then initialize the registration information block

2)SM2 generates {PK, CK}

3)if VehType = R then{PK, CK}→R

4)DBu append (IDrsui, Lrsu(xi,yi) , PK) and blockappend (IDrsui, PK)

5)Return to block

6)end if

7)if VehType = V then

8) Initialize reputation value RepValue = 60

9){PK, CK}→V

10)DBu Append (IDrsui, RepValue, CP, PK) and Block Append (VehIDi, PK)

11)Return to block

12)end if

When the RSU registers, the RSU needs to provide the

information IDrsu and the real location Lrsu(xi,yi) to the blockchain to obtain the public-private key pairs used to complete the registration, the method of which is the SM2 elliptic curve public key cryptography algorithm[13]. The method is SM2 elliptic curve public key cryptography algorithm. When the vehicle is registered, the information receiving vehicle needs to provide the vehicle information VehIDi to the RSU, which sends the public-private key pair {PK, CK} according to the requirements of the SM2 algorithm and synchronizes it with the vehicle information VehID, initializes the vehicle reputation value to RepValue=60, and the vehicle arithmetic is set to CP, which is synchronized in the blockchain.

3.2. Vehicle release specific tasks

Blockchain is used to track and record key information about vehicles including their status, attributes, and for publishing and receiving tasks related to vehicles. When the information-receiving vehicle publishes a task, the blockchain is required to query the RSU with the shortest distance and provide the vehicle information VehIDi, Reward and Punishment RP, Reputation Value RepValue, Public Key PKi, Task Deadline Dt, and Privacy Protection Level K,i.e.,News.when the RSU receives the information sent by the vehicle, it first queries the blockchain based on the VehID and PKi provided by the vehicle user data on the chain to verify whether these information match and whether they are legitimate. After the user is recognized as a legitimate user, the RSU will further evaluate whether the vehicle's reputation value RepValue meets the minimum reputation value requirement set by the system 60. If the vehicle's reputation value meets this requirement, the RSU will trigger its smart contract mechanism. The smart contract will generate a new task Wi based on the parameters provided by the requesting vehicle and append the task to the task database DBt[14] .

Table 2. Vehicle release specific tasks

Input: News={VehIDi, PKi, RepValue, RP, Dt, K}

Output: Task database DBt

1)if VehIDi∈DBu then

2) if {VehIDi, PKi} belongs to the blockchain then

3) if RepValue > 60 then

4) Generating Smart Contracts and Tasks Wi

5) DBt Append (IDrsui,Wi,Dt,VehIDi,K,RP)

6) end if

7) end if

8)end if

3.3. Reputation Points Algorithm

In Telematics, the behavior and performance of vehicles may change with time, environment, road conditions and other factors, and the reputation evaluation process is a dynamic process that can reflect the actual condition of vehicles in real time. A reputation evaluation algorithm is designed to update the reputation evaluation model in real time[15] .

Given the fast and dynamic moving nature of vehicle interaction, the state of vehicles in their surroundings is always changing, which makes it difficult to stabilize the security of vehicles that interact with information. Therefore, when a vehicle receives information from other vehicles, it must assess the trustworthiness of this information so that the value of the trust relationship between vehicles can be determined. Doing so helps to ensure the security and validity of the information, which in turn improves the reliability and security of the entire transportation system. In detail, the current moment is denoted as t, the vehicle receiving the information is denoted as i, and the vehicle sending the information is denoted as j, as expressed in equation (1).

$$Trust_j^i(t) = \alpha PreTrust^j(t-1) + \beta Trust^j(Rank_t) + \gamma NeiTrust^j(t) \quad (1)$$

Where, $Trust_j^i(t)$ denotes the trust relationship value between the information receiving vehicle i and the information sending vehicle j at the current moment t; $PreTrust^j(t-1)$ denotes the historical reputation value of the information sending vehicle j at the previous moment t-1; $Trust^j(Rank_t)$ denotes the trust value of the data sent by the information sending vehicle j at the current moment t; $NeiTrust^j(t)$ denotes the current recommended trust value; α , β , γ are the weighting factors, and $\alpha+\beta+\gamma=1$.

3.3.1. Multi-type vehicle weights

Vehicle interaction scenarios are different, and different data trust weights can be assigned according to different vehicle types (high trust for special vehicles, general trust for public transportation vehicles, and low trust for private vehicles) [16]. High-trust vehicles Vh: police cars, fire trucks, ambulances, etc. General trust vehicles Vm: public transportation vehicles, cabs, etc. Low trust vehicle Vl: private car, etc. The priority is Vh>Vm>Vl. When the message-receiving vehicle receives a sent message vehicle with different vehicle types, it is prioritized to find out whether there is a high-trust vehicle type interaction. Specifically.

$$Trust^j(Rank_t) = \begin{cases} 1.0, v \in vh \\ 0.8, v \in vm \\ 0.6, v \in vl \end{cases} \quad (2)$$

3.3.2. Recommended trust values for neighboring recommended vehicles

The recommendation trust of a recommended vehicle is categorized as positive or negative, when the recommendation trust value is greater than the trust threshold Thv (administrator-defined threshold)[17], it will be considered as a positive rating and vice versa.

$$NeiTrust^+ = \frac{1}{n}\sum_{k=1}^{n} NeiTrust_k^j(t) \quad (3)$$

$$NeiTrust^- = \frac{1}{m}\sum_{k=1}^{m} NeiTrust_k^j(t) \quad (4)$$

$$NeiTrust^j = \begin{cases} NeiTrust^+, Trust_i^j(t) - Thv \geqslant 0 \\ NeiTrust^-, Trust_i^j(t) - Thv < 0 \end{cases} \quad (5)$$

3.3.3. Mechanisms for incentives and penalties

Introduce a reward and punishment mechanism if the message sent by the message sending vehicle j is verified as valid by the majority of the vehicles (EI.Effective

information), then the vehicle is rewarded accordingly[18] , specifically as expressed in equation (6):

$$rewardTrust = (1+\frac{PreTrust^{j}(t-1)}{Trust_{max}}) * rewardRank \quad (6)$$

Among them, $PreTrust^{j}(t-1)$ indicates the original credibility value of the vehicle j to which the message was sent; $Trust_{max}$ indicates the maximum credibility value of the vehicle; $rewardRank$ indicates the credibility value of this reward; $rewardTrust$ indicates the credibility value after the reward.

On the contrary, if the message sent by the message sending vehicle j is invalid or malicious information (NI,Noneffective information), the vehicle will suffer the corresponding punishment, as expressed in equation (7):

$$punishTrust = (1+\frac{PreTrust^{j}(t-1)}{Trust_{max}}) * punishRank * \delta \quad (7)$$

Among them, δ is the penalty coefficient, which controls the penalty value to be δ times of the reward value ($\delta \geq 1$), $punishRank$ indicates the reputation value of this penalty, and $punishTrust$ indicates the reputation value after the penalty.

The reputation value of the message sending vehicle j after passing the reward and punishment mechanism is denoted as:

$$PreTrust^{j}(t) = \begin{cases} rewardTrust, Trust^{j}(Rank) = EI \\ punishTrust, Trust^{j}(Rank) = NI \end{cases} \quad (8)$$

3.3.4. Vehicle reputation value updates

Vehicle reputation value update i.e. sending valid message reputation value update grows slowly and sending malicious message reputation value update decreases rapidly by comparing the current vehicle trust relationship value with the relationship threshold value Thv, as expressed in equation (9):

$$\Delta Rep(j) = \begin{cases} \frac{Trust_i^j(t) - Thv}{3i+1}, Trust_i^j(t) - Thv \geqslant 0 \\ 1 - e^{|Trust_i^j(t) - Thv|}, Trust_i^j(t) - Thv < 0 \end{cases} \quad (9)$$

The reputation of the message sending vehicle j is updated to:

$$RepValue^{j}(t) = \min\left\{ Rep^{j}(t-1)\left[1+\frac{2}{\pi}\arctan\left(\Delta Rep(j)\right)\right], 1\right\} \quad (10)$$

Table 3. Algorithm for updating vehicle reputation value

Input:trust threshold Thv

Output: $RepValue^{j}(t)$

1)Determine vehicle type and vehicle priority

2)Calculate the trust value of the data sent by the information sending vehicle j at the current moment t $Trust^{j}(Rank_t)$

3)Calculate the recommended trust value of the neighboring recommended vehicles to the information sending vehicle j at the current moment t $NeiTrust^{j}(t)$

4)Calculate the value of trust relationship between information receiving vehicle i and information sending vehicle j at the previous moment t $Trust_j^i(t)$

5) if $Trust_i^i(t) - Thv \geqslant 0$ do

6) $\Delta Rep(j) = \frac{Trust_i^j(t) - Thv}{3i+1}$

7) else do

8) $\Delta Rep(j) = 1 - e^{|Trust_i^j(t) - Thv|}$

9) end if

10) Calculate the reputation value of the message sending vehicle j $RepValue^{j}(t)$

3.4. Blockchain Smart Contract Design

After the RSU generates a smart contract, it broadcasts a transaction request based on its coverage area, with the aim of finding a message sending vehicle that can receive and perform the task. This broadcast message can be received by all users in the coverage area of the RSU. When the information sending vehicle receives the broadcast message, if it intends to participate in the task, it can send relevant information including its own reputation value RepValue, arithmetic CP, and the current location point Lv(xi,yi) to the smart contract according to the task requirements of the information receiving vehicle in the request. The smart contract selects the best information sending vehicle according to the data uplink rules. Once selected, the message sending vehicle will start to execute the task. During the execution process, the smart contract will synchronize the status of the task in real time to ensure that all relevant parties can obtain the latest progress of the task in a timely manner. When the task is completed, the message sending vehicle will submit the task data to the smart contract for verification. The smart contract will reward or penalize the message sending vehicle according to the quality of the task completion. Finally, the smart contract will update the RepValue of the message sending vehicle according to the quality of the task and upload this update to the blockchain so that subsequent transactions and verification can refer to the latest Reputation Value [19].

Table 4. Smart contract design in blockchain

Input:WiDBt, message-receiving vehicle, task database, message-sending vehicle database DBwu

Output: message sending vehicle VehIDj

1) Announcement of mission information Wi and information-receiving vehicles VehIDi

2) Information sending vehicle query blockchain {VehIDi,Ci,PKi}

3)if {VehIDi, PKi} belongs to a blockchain and RepValue> 85 then

4)The message sending vehicle sends {VehIDj, CPj, PKj, Lv(xi,yi)} to the smart contract

5) end if

6) Smart contract to verify the legitimacy of the vehicle to which the information is sent

7) if the vehicle to which the message is sent is legal then

8)The message is sent to the vehicle database DBwu append(VehIDj,CPj , PKj,Lv(xi,yi))

9)if DBwu< K then

10)Continue to add information to send vehicles

11) else if DBwu= K

12)Smart contract filters the best message from DBwu to send the vehicle

13)end if

14) end if

15) Return the best message to send the vehicle VehIDj

3.5. Blockchain message synchronization

To avoid malicious message-sending vehicles from completing their bookkeeping in the blockchain, it is stipulated that message-sending vehicles have only query access to the blockchain, while RSUs have full operational access to the blockchain[20]. After each task is completed, the RSU must update the information of the message receiving vehicle and the message sending vehicle in the blockchain. In addition, the RSU must synchronize the information of each user with its identity information VehID.

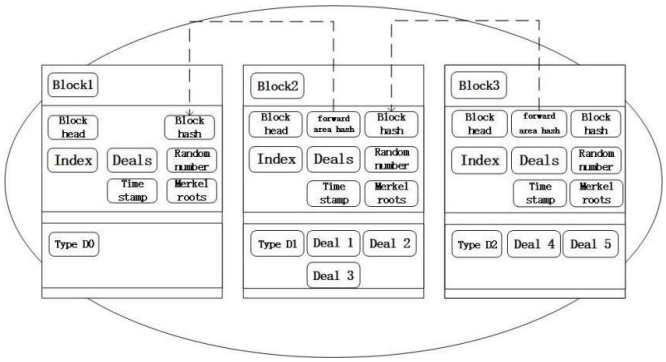

Figure 2. Blockchain structure

3.6. Smart Contract Implementation

The smart contract needs to be written according to the pre-set reputation points algorithm to ensure that the reputation value can be accurately calculated based on the vehicle's behavior and data. The design of the reputation points algorithm should take full account of the diversity and complexity of the vehicle's behavior in order to better assess the vehicle's reputation. The fairness and accuracy of the reputation value can be ensured through the automatic execution of the smart contract [21] .

Smart contracts can define and enforce data uplink rules to ensure that only eligible data can be uplink, preventing false data or malicious tampering from entering the system. This ensures the authenticity of information and the traceability of transactions in the reputation value program[22].Verify and confirm interactions between vehicles to ensure that each interaction complies with the rules and requirements of the reputation value scheme. Through the implementation, it avoids the impact of malicious behaviors or bad interactions on the system and enhances the degree of mutual trust between vehicles[23].The program is implemented to avoid malicious behaviors or undesirable interactions from affecting the system and to enhance mutual trust between vehicles.

The construction of the smart contract involves three core function components, each of which performs specific trust management tasks.The SetRep() function is responsible for setting the initial trust value of a vehicle when it is connected to the network. The function sets the initial trust value for specialized vehicles (e.g., fire trucks, ambulances, police cars, etc.) to a high value of 90 points to reflect their high reliability and priority. For other vehicles, the function will set a relatively low initial trust value of 60 points. Next, the UpdateReputation( ) function assumes responsibility for updating the vehicle's trust value. As network interactions take place, the behavior and performance of the vehicle will affect its trust value. This function calculates the trust offset based on the predefined rules and algorithms and dynamically adjusts the vehicle's trust status accordingly. Finally, the QueryTrust() function provides a query interface for other entities in the network to retrieve the current trust value of a specific vehicle. By querying the trust value of the target vehicle, participants in the network can more accurately determine the authenticity and reliability of the message and thus make more informed decisions [7] .

3.7. Uplink mission data

After the message sending vehicle completes the task, it needs to encrypt the data with the RSU public key in the smart contract and uplink it. If the time spent on the task exceeds the time limit, the contract will be automatically terminated and the task will fail. If the vehicle uplink the task data on time, the RSU decoder the data and encrypts it with the receiving vehicle's public key and sends it, and the receiving vehicle decoder it with its private key and verifies the data quality.

4. Data uplink rules

In the Internet of Vehicles, in order to ensure mutual trust between vehicles and system security, it is necessary to select and determine what types of data should be recorded and stored on the blockchain. This includes vehicle identification information, driving records, violation records, and reputation assessment results.

The mode and frequency of data uplink are key to ensuring efficient system operation and data accuracy. The way of data uplink, real-time uplink or batch uplink, is determined according to the frequency of transactions and the size of data volume. For high-frequency transactions or critical data, real-time uplink can be used; while for low-frequency or large amount of data, batch uplink can be chosen.

The verification rules and mechanisms for data uplink are crucial links. This process, the hash algorithm can effectively verify whether the data have been tampered with during transmission or storage, ensure the integrity of the data, and confirm the source and authenticity of the data through digital signatures. The hash algorithm, by transforming the original data into a unique hash value, can ensure the integrity of the data and has not been tampered with, and any minor changes to the data will lead to significant changes in the hash value, which can be easily recognized by the system. At the same time, digital signature technology can verify the authenticity of the data and achieve authentication. By adding a digital signature to the data, it ensures that the source of the data is

trusted and that the data has not been tampered with during transmission. By combining verification rules and techniques such as hash algorithms and digital signatures, it is ensured that the data undergoes strict verification before being uplink to the chain, so as to guarantee the data quality and system security. Finally, it is necessary to determine the authority and access control mechanism for data uplink. Data in the blockchain should be managed in accordance with certain permissions and access control rules to protect user privacy and data security [24].

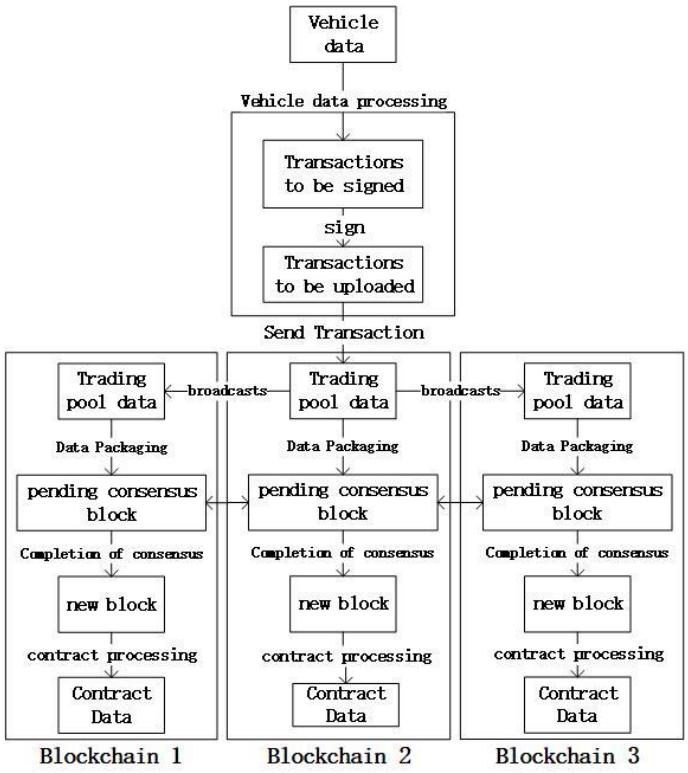

Figure 3. Data uplink process

4.1. Pre-uplink processing stage

Vehicle data needs to be processed and the information signed before the vehicle data can be uplink.

4.1.1. Vehicle data processing

The vehicle data is processed through the server and then the information from the calling function plus the chain data is put into the transaction structure. The pre-signature transaction structure is determined by the chain and typically contains the calling contract, timestamp, random number and information about the calling function plus data. After putting together the pre-signature data, it is further serialized for messaging.

4.1.2. Message signatures

The pre-signature vehicle data is processed to ensure its accuracy and completeness. This data is then hashed once to generate a hash value that is tightly bound to the data. Next, a signature operation is performed on the generated hash value. Signature is an authentication method based on asymmetric encryption that allows to verify whether the sender holds the corresponding private key by means of a public key and a signature message. In this way, the identity of the sender can be confirmed without revealing the sender's private key. At the same time, signing the hash value can also tightly bind the sender's identity with the information sent, effectively preventing others from impersonating the sender and ensuring the authenticity of the information and the authentication of the sender. In the processing stage before the data is uplink to the chain, professional tools are mainly used to convert the vehicle data into a format readable by the blockchain network. Through the signature operation, the identity of the sender and the information sent are tightly bound, which realizes the functions of authentication and prevention of repudiation. Finally, the processed information is sent to the blockchain node in preparation for the uplink operation. It is worth noting that the processing before uplink is centralized and does not involve the participation of blockchain nodes. This stage is mainly accomplished by relevant tools and systems to ensure the accuracy and credibility of the data and provide strong support for the subsequent uplink operation.

4.2. Upstream processing stage

Once the processed vehicle data is sent to the blockchain node, a blockchain transaction is formed and enters the on-chain processing phase.

4.2.1. Transaction broadcasting

Transactions in the system, once received by each node, are quickly broadcast to other nodes, thus building a transaction pool that centralizes all pending transactions and lays the foundation for the subsequent consensus mechanism. After the transactions are broadcast, there is a significant difference in the way transactions are processed by alliance chains and public chains. Public chains and coalition chains use different strategies in processing transactions to adapt to their respective characteristics and needs. Public chains focus more on openness and decentralization, while coalition chains place more emphasis on trust and cooperation among partners.

4.2.2. Block consensus

At the heart of blockchain technology are blocks, unique block hashes, block headers containing important information, and detailed transaction data. Core data such as details of the consensus mechanism, the timestamp of the transaction record, and the block's position on the chain (i.e., block height) are stored in the block header. To ensure continuity and security between blocks, each block records the hash value of its predecessor, and this linkage ensures the integrity of the chain. Inside the block, the Transaction Data section then details all the transactions contained in that block, which are summarized by a hashing algorithm and arranged in a specific order. Once the block header and the transaction data within it have been verified and validated, the system uses a cryptographic algorithm to calculate a hash value for the entire block. Through this mechanism, each block is closely linked to the previous block, not only by recording the hash value of the previous block, but also by its own unique hash value. This design makes the blockchain a virtually tamper-proof chain of data, and any modification to the data immediately results in a change in the hash value that can be recognized by other participants in the network. Blockchain technology thus provides a secure and reliable way to record and manage data.

Consensus mechanism is a key process to ensure that different nodes in a blockchain network can generate the same block, thus maintaining data consistency. For public chains, as the communication status of nodes is not controllable, network problems may lead to inconsistent blocks or even forks. For coalition chains, on the other hand, the consensus algorithm needs to ensure that when some nodes have network problems, other nodes can still maintain the consistency of block data, and may adopt the strategy of

suspending block issuance to prevent forking.

On-chain processing is the process of actually writing business data to the block, which is a decentralized operation that requires the participation and processing of nodes. Prior to the uplink processing phase, the business data can be modified according to the sender's wishes, but once it enters the uplink phase, this data is permanently recorded and cannot be changed. Despite the possibility of uplink failure, once the consensus phase is completed and the blocks of each node are consistent, the business data is recognized by each node and becomes traceable and reliable.

4.3. Smart Contract Processing Phase

4.3.1. Contract Logic Processing

In many cases, the business data completed on the chain need to be further processed logically, because the process of creating smart contracts and calling smart contracts are on the chain, i.e., the executed program and the called functions and parameters are all agreed upon, so the output results of the data of the final called smart contract are also the same. The processed results will be written into the contract's state database, which contains not only the latest state but also the historical state, which is convenient for tracing and querying[25].This database will also contain the historical status in addition to the latest status, which is convenient for traceability and query.

4.3.2. Modifying the State Merkel Tree

The Merkel tree, as a special binary tree structure, is designed to achieve tamper-proof and efficient indexing of data. Through layers of hash calculations, different data blocks (leaf nodes) are progressively aggregated in the Merkel tree until a unique root hash value is formed. Through the indexing mechanism, it is possible to quickly locate snapshots of data in different historical states of the contract[26, 27] .

5. Experimental results and analysis

The experimental simulation processor is Intel(R) Core TM i5-9500 with 8 GB of RAM in Win10 operating system environment using Python language.

5.1. Analysis of average vehicle speed as affected by obstacles

To set up the experiment, a random obstacle is placed between the start and end points, the reputation values of the vehicles are generated uniformly and randomly from 0-100, and all vehicles share messages truthfully according to their reputation values, e.g., a vehicle with a reputation value of 60 points has a 60% probability of sending a truthful message. The average vehicle speed is negatively affected by obstacles in the form of decreasing and then increasing until the normal speed is restored. The experiments show that the recovery time of the average vehicle speed for the received messages is significantly improved, proving that the application of reputation management schemes in vehicular networks is necessary and beneficial, especially in heavy traffic situations.

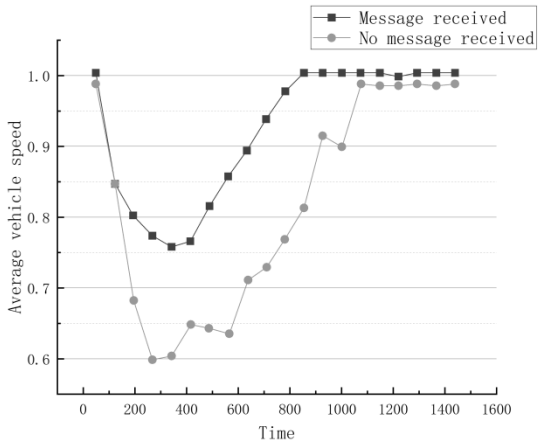

Figure 4. Analysis of average vehicle speed as affected by obstacles

5.2. Changes in message-sending vehicle reputation values with increasing number of message interactions

Figure 5 represents the changes in the reputation value of the malicious information sending vehicle with the increase in the number of information transactions, from the point of view of the percentage of the malicious information sending vehicle, as the percentage of the malicious information sending vehicle decreases, its reputation value decreases faster. As the malicious information sending vehicle participates in more transactions, its reputation value score becomes lower, and the reputation value decreases from 75 points to less than 60 points on average only need to carry out 5 transactions, which fully proves that the reputation points algorithm penalizes the invalid or malicious information of the malicious information sending vehicle.

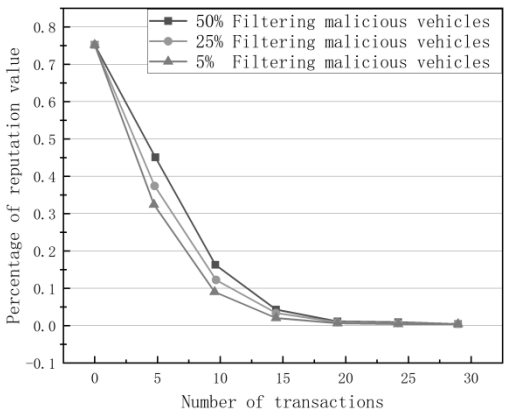

Figure 5. Changes in the reputation value of vehicles sending malicious messages with the increase in the number of message transactions

Figure 6 represents the changes in the reputation value of normal information sending vehicles with the increase in the number of information interactions, from the point of view of the percentage of malicious information sending vehicles, with the decrease in the percentage of the intended information sending vehicles, their reputation value rises slowly. The vehicle reputation value grows slowly with the increase of the number of transactions, and the recovery of the

reputation value of the malicious information sending vehicle to more than 60 points requires hundreds of effective information transactions, which fully proves the professional effectiveness of the reputation points algorithm.

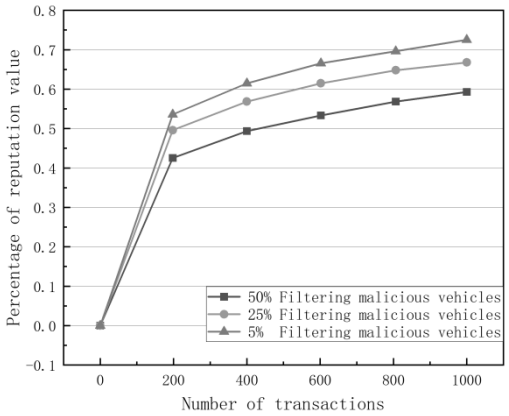

Figure 6. Changes in the reputation value of vehicles sending normal messages with the increase in the number of message interactions

5.3. Analysis of the validity of information trust assessments

In order to verify the effectiveness of the message accuracy rate, comparative experiments are set up to introduce a combined assessment of message trustworthiness based on direct trust of vehicle entities and indirect trust of neighboring vehicles[28] and a false information recognition strategy combining Bayesian inference modeling[29]Comparison experiments are conducted. In the experiment, the total number of vehicles is 500, and the percentage of vehicles sending malicious messages is between 5% and 50%, and multiple experiments are executed to take the mean value to reduce the error. The experimental results are shown in Fig. 7, with the increase of the proportion of vehicles sending malicious information information accuracy rate slowly decreases, the program accuracy rate can be maintained at more than 85%, the verification rules and mechanisms of data uplinking to ensure the legitimacy and accuracy of the data.

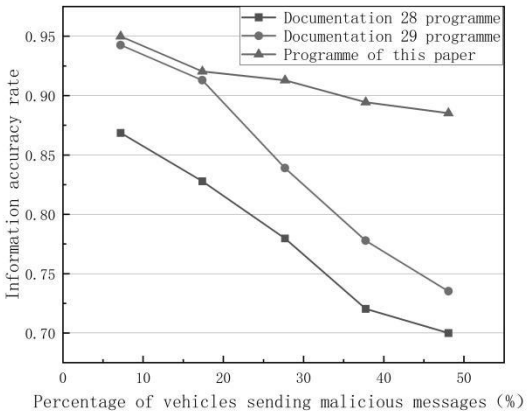

Figure 7. Information Trust Assessment Validity Analysis

5.4. Analysis of the effectiveness of the credit score algorithm

In order to verify the change in reputation value caused by vehicle behavior, a comparison experiment is set up to introduce the use of reputation thresholds to identify malicious vehicles[30] (with an initial reputation value of 50 points and an initial reputation value of 60 points for this experiment) for comparison experiments. The vehicle's reputation value grows normally from 0 to 50 transactions, and is penalized and decreases rapidly as malicious behavior occurs. When the reputation value is lower than normal, the vehicle sending malicious messages will have its reputation value growth limited and grow slowly even if it resumes normal behavior due to its previous malicious behavior. The experimental results are shown in Fig. 8, where the vehicle's reputation value is updated according to the vehicle's behavior and the malicious behavior of the malicious message sending vehicle is penalized to a greater extent.

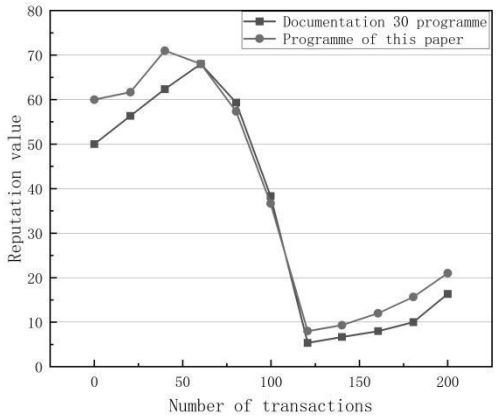

Figure 8. Effectiveness analysis of credit score algorithm

6. Conclusion

According to the trust problem between vehicles that may occur in the car networking scenario, a vehicle reputation value management scheme based on data uplinking rules is designed. First, the user completes registration through the SM2 elliptic curve public key cryptography algorithm and releases a specific task according to the demand, the RSU queries the blockchain according to the user's information to verify whether the data matches to determine whether the user is legitimate, and the smart contract selects the best information to send the vehicle to perform the task according to the data uplinking rules. Further, the data is stored on the blockchain according to the data uplinking rules, and the data in the blockchain should be managed according to certain permissions and access control rules to protect the user's privacy and data security. Finally, the trustworthiness of vehicles is comprehensively evaluated through multi-type vehicle weights, neighborhood recommendations, and reward and punishment mechanisms, and the smart contract updates the reputation value of vehicles in real time. The results show that the scheme can effectively detect the information sending vehicles with malicious behavior and make corresponding punishment, which effectively protects the safety of vehicles.

References

[1] Vishwakarma,L.,Das,D.(2022).‘SmartCoin:A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain’,Vehicular Communications, Vol. 33, 100429.

[2] Hu,C.,Fan,W.,Zeng,E.,Hang,Z.,Wang,F.,Qi,L.,&Bhuiyan,M. Z. A.(2021).‘Digital twin-assisted real-time traffic data prediction method for 5G-enabled internet of vehicles’, IEEE Transactions on Industrial Informatics, 18(4), 2811-2819.

[3] Xu, C., Ding,Y., Lu,L., Liu,S., Liu,L & Zhao,G. (2022). ‘Personalized Location Privacy Protection for Location-based Services in Vehicular Networks’,Journal of Software (02), 699-716.

[4] Liu,J.,Zhang,S.,Sun,W.,&Shi,Y.(2017).‘In-vehicle network attacks and countermeasures: Challenges and future directions’,IEEE Network, 31(5), 50-58.

[5] Li,C.,Fu,Y.,Yu,F.R.,Luan,T.H.,&Zhang,Y.(2020).‘Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework’,IEEE Transactions on Intelligent Transportation Systems, 22(2), 898-912.

[6] Xie,Y.,Zhang,J.,Wang,H.,Liu,P.,Liu,S.,Huo,T,&Ye,Z.(2021). ‘Applications of blockchain in the medical field: narrative review’,Journal of Medical Internet Research, 23(10), e28613.

[7] Zheng,Z.,Xie,S.,Dai,H.N.,Chen,W.,Chen,X.,Weng,J.,& Imran, M.(2020).‘An overview on smart contracts: Challenges, advances and platforms’,Future Generation Computer Systems, 105, 475-491.

[8] Liu,Y.,Xiong,Z.,Hu,Q.,Niyato,D.,Zhang,J.,Miao,C,&Tian,Z. (2022). ‘VRepChain: A decentralized and privacy-preserving reputation system for social Internet of Vehicles based on blockchain’, IEEE Transactions on Vehicular Technology, 71(12), 13242-13253.

[9] Liu,Q.,Gong,J.,&Liu,Q.(2023).‘Blockchain-assisted reputation management scheme for internet of vehicles’,Sensors, 23(10), 4624.

[10] Lu,Z.,Wang,Q.,Qu,G.,&Liu,Z.(2018,August).‘BARS:A blockchain-based anonymous reputation system for trust management in VANETs’,In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 98-103). IEEE.

[11] Mahmood,A.,Sheng,Q.Z.,Zhang,W.E.,Wang,Y.,&Sagar,S. (2023).‘Toward a distributed trust management system for misbehavior detection in the internet of vehicles’,ACM Transactions on Cyber-Physical Systems, 7(3), 1-25.

[12] Tang,C.,Wu,H.,&Xiao,S.(2023).‘Lightweight Reputation Management for Multi-Role Internet of Vehicles’,IEEE Internet of Things Magazine, 6(2), 38-42.

[13] He,Y.,Quan,J. & Liu,Y.(2024).‘A Location Privacy Protection Scheme Based on Hybrid Blockchain’,Netinfo Security(02),229-238.

[14] Byberg, F. (2024). Implementation of multiple collaborative agents using reinforcement learning (Master's thesis, Universitat Politècnica de Catalunya).

[15] Pan,D.,Zhu,G.& Yang,Q.(2022).‘Consensus mechanism of blockchain based on contribution value and credit value’,Journal of Computer Applications(S1),166-172.

[16] Wijesekara,P.A.D.S.N.,&Gunawardena,S.(2023).‘A Review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges’, Network, 3(3), 343-421.

[17] Gupta,M.,Patel,R.B.,Jain,S.,Garg,H.,&Sharma,B.(2023). ‘Lightweight branched blockchain security framework for Internet of Vehicles’,Transactions on Emerging Telecommunications Technologies, 34(11), e4520.

[18] Avin,S.(2019).‘Exploring artificial intelligence futures’, Journal of AI Humanities, 2, 171-193.

[19] Kumar,S.,Velliangiri,S.,Karthikeyan,P.,Kumari,S.,Kumar,S., &Khan,M.K.(2024).‘A survey on the blockchain techniques for the Internet of Vehicles security’, Transactions on Emerging Telecommunications Technologies, 35(4), e4317.

[20] Yang,L.,&Long,W.(2023).‘Blockchain-based trust mechanism in VANET’,Application Research of Computers(07),1957-1963.

[21] Das,D.,Banerjee,S.,Chatterjee,P.,Ghosh,U.,&Biswas,U. (2023).‘Blockchain for intelligent transportation systems: Applications, challenges, and opportunities’,IEEE Internet of Things Journal, 10(21), 18961-18970.

[22] Negara,E.S.,Hidayanto,A.N.,Andryani,R.,&Syaputra,R. (2021).‘Survey of smart contract framework and its application’, Information, 12(7), 257.

[23] Mohanta,B.K.,Panda,S.S.,&Jena,D.(2018, July). ‘An overview of smart contract and use cases in blockchain technology’, In 2018 9th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-4). IEEE.

[24] Zhu,X.,&Shen,G.(2010).‘Review of association rules mining in data streams’,Application Research of Computers(09),3201-3205.

[25] Gao,T.,Yao,Z.,Jia,M&Si,X.‘Overview of on-chain and off-chain consistency protection technologies’,Journal of Computer Applications 1-13.

[26] Kuznetsov,O.,Rusnak,A.,Yezhov,A.,Kuznetsova,K.,Kanonik, D.,&Domin,O.(2024).‘Merkle Trees in Blockchain: A Study of Collision Probability and Security Implications’,Internet of Things, 101193.

[27] Liu,Z.,Ren,L.,Feng,Y.,Wang,S.,&Wei,J.(2023).‘Data integrity audit scheme based on quad Merkle tree and blockchain’,IEEE Access, 11, 59263-59273.

[28] Li,F.,Chen,M.,Wang,L.,Li,P.&Ju,X.(2024).‘Research on Trust Management Mechanism of Internet of Vehicles Based on Blockchain’,Computer Science(04),381-387.

[29] Zhang,H.,Cao,Y.,Liu,K.&Wang,R.(2023).‘Distributed trust management scheme based on blockchain in Internet of vehicles’,Journal on Communications(05),148-157.

[30] Zhang,H.,Wang,D.,Wang,R.&Wang,D.(2023).‘Collusion node detection method based on fuzzy evaluation density clustering in Internet of vehicles’,Journal on Communications(07),114-123.