IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 2, 2018, accepted December 18, 2018, date of publication January 3, 2019, date of current version May 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890736

Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network

XIAOHONG ZHANG AND XIAOFENG CHEN
School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China

Corresponding author: Xiaohong Zhang (xiaohongzh@263.net)

This work was supported in part by the National Natural Science Foundation of China under Grant 61763017 and Grant 51665019, in part by the Scientific Research Plan Projects of the Jiangxi Education Department under Grant GJJ150621, in part by the Natural Science Foundation of Jiangxi Province under Grant 20161BAB202053 and Grant 20161BAB206145, and in part by the Innovation Fund for Graduate Students in Jiangxi Province under Grant YC2017-S302.

ABSTRACT A vehicular ad-hoc network (VANET) can improve the flow of traffic to facilitate intelligent transportation and to provide convenient information services, where the goal is to provide self-organizing data transmission capabilities for vehicles on the road to enable applications, such as assisted vehicle driving and safety warnings. VANETs are affected by issues such as identity validity and message reliability when vehicle nodes share data with other nodes. The method used to allow the vehicle nodes to upload sensor data to a trusted center for storage is susceptible to security risks, such as malicious tampering and data leakage. To address these security challenges, we propose a data security sharing and storage system based on the consortium blockchain (DSSCB). This digital signature technique based on the nature of bilinear pairing for elliptic curves is used to ensure the reliability and integrity when transmitting data to a node. The emerging consortium blockchain technology provides a decentralized, secure, and reliable database, which is maintained by the entire network node. In DSSCB, smart contracts are used to limit the triggering conditions for preselected nodes when transmitting and storing data and for allocating data coins to vehicles that participate in the contribution of data. The security analysis and performance evaluations demonstrated that our DSSCB solution is more secure and reliable in terms of data sharing and storage. Compared with the traditional blockchain system, the time required to confirm the data block was reduced by nearly six times and the transmission efficiency was improved by 83.33%.

INDEX TERMS Consortium blockchain, data sharing, data storage, signature verification, vehicular ad-hoc network (VANET).

I. INTRODUCTION

The number of mobile vehicles in mobile ad-hoc networks has increased rapidly and vehicular ad-hoc networks (VANETs) have been formed. In a VANET, vehicles are fitted with wireless communication devices called onboard units (OBUs). Each OBU contains a hardware security module, which is a tamper-proof device for storing security information. The OBU on a vehicle communicates with a roadside unit (RSU) or other OBUs via a dedicated short-range communication [1] protocol. A vehicle is a network node in a VANET and it has the ability to communicate and process information to facilitate distributed traffic control. The traffic management center can distribute the road resources in a reasonable manner through distributed synchronization and coordination. As part of an intelligent transportation system, the VANET aims to improve road safety, enhance traffic flow, and to reduce congestion [2]. Therefore, ensuring the safe and efficient driving of vehicles will play a major role in the development of intelligent transportation systems [3]. However, if the data sent by a vehicle are lost or tampered with while on the road, this will affect the driver's decision, thereby causing a severe deviation from the route and even threatening the safety of the vehicle or the driver. Thus, improving the security and integrity of vehicle data sharing is a focus for researchers.

The associate editor coordinating the review of this manuscript and approving it for publication was Malik Najmus Saqib.

In the traditional VANET network architecture, data sharing mainly occurs via two communication modes comprising vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) units. The vehicle nodes can store sensitive data in a tamper-resistant device [4] according to specific needs, which is considered to be very safe. Sharing non-sensitive data with other vehicles can increase the system's efficiency. However, data are transmitted over non-secure channels and they are readily intercepted or tampered with by an attacker. Traffic data in the coverage area are aggregated by the RSU in the cloud service platform for storage and they form a central database. The RSU is usually placed in positions at each kilometer or less [5] in order to maintain a high data rate in busy traffic. However, this centralized approach to data storage leads to information security issues such as centralized malicious attacks and malicious tampering with intermediate data. After the centralized database is attacked, large volumes of vehicle data leakage can occur and cause uncontrollable security incidents. The growing number of issues such as data privacy and cyberattacks has resulted in three major challenges that hinder the construction of a secure and efficient VANET.

1) Centralization: The traditional VANET relies on a cloud service platform for central database storage and data management. The increasing demand for data sharing among vehicles imposes higher requirements in terms of data storage. Large-scale data leakage may occur after it has been attacked or maliciously tampered with, which can cause a series of uncontrollable events.
2) Efficiency and computational overheads: Due to the rapid growth of internet-connected vehicles, the maintenance of the control center for a central database incurs high costs and is both time and energy consuming. The limited calculation resource size for the RSUs can be overloaded in areas with high vehicle densities, whereas the calculation resources may be idle in areas with low densities. The inability to allocate computing resources in a reasonable manner decreases the efficiency of data sharing.
3) Security threat: Wireless communication in a VANET allows data to be easily monitored and falsified during the sharing process, thereby resulting in severe threats to the safety and privacy of vehicles (e.g., illegal tracking or remote hijacking of vehicles). Illegal vehicles may send falsified data to disrupt the normal transmission of data, and providing an incorrect message is likely to cause a traffic accident or even a serious traffic accident.

To address these challenges, trust and privacy [6] urgently need to be improved to ensure the security and integrity of the communication process. Thus, it is necessary to design a safe and reliable decentralized data storage system to ensure the normal operation of VANETs. According to a previous study [7], 60% of accidents could be prevented if the vehicle warns its driver half a second before a collision.

In recent years, blockchain has generally been considered a subversive technique that is developing rapidly [8]. A blockchain is a decentralized distributed database that generates blocks of data in chronological order and combines them into specific data structures in a chain. A blockchain uses cryptography to ensure that the data are tamper-proof and unforgeable, and can be used for distributed computing and data sharing between network nodes. Each node can verify the validity of the transaction signature based on the public key in the distributed network, so there is no trust consensus between them. Consensus algorithms rely on all nodes to participate in a coherency protocol called proof-of-work (PoW) to complete data validation and storage. In a consortium blockchain, the nodes that participate in the consensus are preselected and the generation of each block is determined by the preselected nodes (PSNs). Other connected sensing nodes (SNs) can participate in information interactions but they do not participate in the consensus process. The blockchain technique can also provide a smart contract [9] scripting system, which enables more advanced distributed applications. This digital form of commitment includes contract execution conditions and digital asset content, and it is automatically executed by the computer once it has been deployed. In addition, the blockchain uses a unique economic incentive mechanism to attract nodes to complete work (i.e., mining), thereby prompting nodes to provide computing power and resources [10]. The incentive mechanism motivates node interactions to improve the system's activity and this allows it to develop steadily. The vehicle nodes in VANETs are similar to the distributed structure of network nodes in a blockchain. Therefore, this technique could provide a solution to the scalability issues that affect data storage for VANETs.

Kenney [11] introduced an effective batch signature verification scheme to cope with the time delay when verifying multiple messages. Lu et al. [12] proposed a scheme that changes the pseudonym to protect the privacy of users with the participation of a trusted authority (TA), but it is not suitable for the real-time nature of vehicle data sharing. In order to address the heavy workload and the trustworthiness of messages, a new VANET authentication protocol was proposed [13] for use in the group model with a new group signature scheme. Azees et al. [14] proposed an effective anonymous authentication scheme to avoid malicious vehicles joining VANETs. Another study [15] proposed a safety solution based on blockchain protection for electric vehicle energy and data interactions. This scheme provides data coins and energy coins for the interactions between vehicles in order to motivate the vehicles to share data. In addition, a lightweight solution was proposed that uses encryption techniques to solve some of the security challenges that affect V2V solutions when creating and disseminating emergency messages [16]. A decentralized privacy protection and blockchain-based security architecture was developed for smart vehicles [17], but this approach does not consider practical issues such as PSN management and high overheads. A point-to-point power transaction model based on the consortium blockchain solves the scalability

problem [18] but we consider that it does not completely guarantee the information transaction process and it is vulnerable to security attacks.

Therefore, a safe and effective solution is needed in order address the security problems related to vehicle transmission data and the scalability of data storage. Thus, we propose a new data security sharing and storage system based on consortium blockchain (DSSCB). In this scheme, a digital signature algorithm based on the elliptic curve bilinear pair property [19] is used to sign the message in the data sharing stage in order to support the vehicle's secure communication and to ensure the non-repudiation and integrity of the message. The use of the consortium blockchain solves the problem of lightweight scalability and improves the overall system efficiency. Consistent algorithms are used to ensure that the whole network reaches a consensus, where it can guarantee the consistency of actions even when a few nodes are malicious. Private data in VANETs can be stored securely in the blockchain so the user behavior does not become unreliable during privacy protection. Smart contracts [20] are used to limit the triggering conditions for the vehicle when transmitting and storing data in order to allocate computing resources within the RSU in a reasonable manner. In addition, the use of data coins according to the frequency of data contribution motivates vehicles to share data. Due to the mobility of the vehicle nodes, the vehicles always experience a transition within the communication range when moving from the current RSU to another RSU, which can lead to delays in data sharing. The soft handover method [21] can be used to correlate the vehicle nodes with different RSUs that are closer to the current position.

The remainder of this paper is organized as follows. In Section 2, we present basic details of the encryption and verification algorithms. In Section 3, we explain the network architecture based on the consortium blockchain system, including detailed descriptions of several entity models. In Section 4, we describe the specific implementation of the DSSCB, including the sender's authentication and digital signature process, and the consensus mechanisms and incentives. We present a safety analysis and performance evaluation of our proposed scheme in Section 5. In Section 6, we give our conclusions.

II. BASIC DETAILS OF ENCRYPTION AND VERIFICATION ALGORITHMS

A. ELLIPTIC CURVE CRYPTOSYSTEM (ECC)

Assuming that F_p represents the finite field of large prime p, an elliptic curve $E_p(a, b)$ is defined as $y^2 \equiv x^3 + ax + b(\bmod p)$, where a, b, x, and y belong to F_p. They also satisfy the equation $4a^3 + 27b^2(\bmod p) \neq 0$. In particular, the addition operation and scalar multiplication operation comprise the Abel group of the elliptic curve $E_p(a, b)$. On the elliptic curve $E_p(a, b)$, we define a special point in the coordinate system, which is infinitely far from the X-axis, and it is called the O-point. When $P(x_1, y_1) \in E_p$, the equation $P + O = O + P = P$ is satisfied. Figure 1(a) shows the addition operation for the Abel group under modulo p on the elliptic curve. If $P(x_1, y_1)$, $Q(x_2, y_2)$ are two different points and $P \neq -Q$, then $P + Q = R = (x_3, y_3) \in E_p$ holds. The scalar multiplication on the elliptic curve is $2P(x_3, y_3) \in E_p$, $P(x_1, y_1) \in E_p$, and $P \neq -P$, which are given by $x_3 = [(3x_1^2 + a)/2y_1]^2 - 2x_1$ and $y_3 = (3x_1^2 + a)(x_1 - x_3)/2y_1 - y_1$, as shown in Figure 1(b).

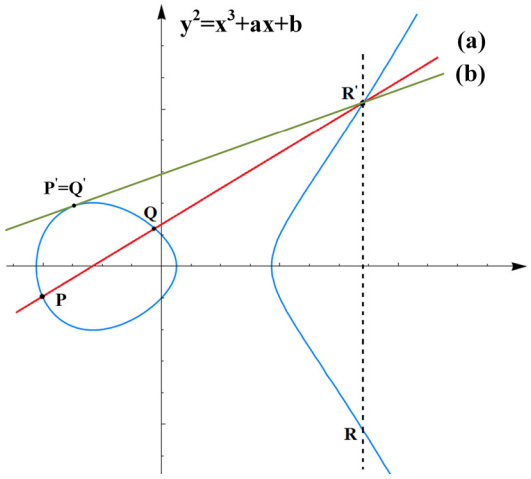

FIGURE 1. Elliptic curve based on (a) addition and (b) scalar multiplication.

The elliptic curve was applied to cryptography in a previous study [22]. After the construction of the ECC based on the elliptic curve discrete logarithm problem (ECDLP), ECC began to be used for encryption protocols and in other security fields [23]. The steps required for generating a public–private key pair in an ECC are as follows.

- Select elliptic curve $y^2 \equiv x^3 + ax + b(\bmod p)$ to construct ellipse group E_p.
- Find the base point $G(x_0, y_0) \in E_p$ and $nG = O$ is satisfied, where n is a large prime number.
- Select an integer $n_B < n$ as the private key and generate the public key $P_B = n_B G$. The public key is (E, G, n, P_B) and the private key is n_B.

B. BILINEAR MAPS

Bilinear mapping [24] is a very important concept in cryptosystems, which can be constructed by Weil pairing or Tate [25] pairing in elliptic curves. Assuming that q is a large prime number, G and G_T are two cyclic groups of order q, which are defined on two cyclic groups with a mapping called a bilinear map, as follows.

$$\begin{cases} G : \textit{Additive group} \\ G_T : \textit{Multiplicative group} \\ \hat{e} : \textit{Bilinear map such that } G \times G \to G_T \end{cases}$$

The bilinear map satisfies the following three properties.

- Bilinearity: If we let $P, Q, R \in G$, we have

$$\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R) \tag{1}$$

and for any $a, b \in Z_q^*$, we have:

$$\hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} = \hat{e}(P, abQ) = \hat{e}(abP, Q) \quad (2)$$

- Non-degeneracy: $P, Q \in G$ exist such that $\hat{e}(P, Q) \neq 1_{G_T}$, where 1_{G_T} is the identity element of G_T.
- Computability: For any $P, Q \in G$, an efficient algorithm can compute $\hat{e}(P, Q)$.

In general, a bilinear map can be constructed by modifying an elliptic curve and it also has the following characteristics of an elliptic curve. Let $P, Q \in G$ and $a \in Z_q^*$, $Q = ap$, and $\{P, Q\}$ are known. Finding the integer a from Q and P is the ECDLP.

C. BATCH VERIFICATION

Assume that for the random selection of $i \in (1, n)$, the RSU can receive verification parameters $Ver_i(AID_i, S_i, M_i, C_i)$, and each step runs normally. AID_i is the pseudonym generated by the vehicle, S_i is the final signature information, M_i is the message, and C_i is the randomization parameter Then, the plurality of the authentication parameters during batch verification for the message shared between the nodes is: $Batch_Ver_n((AID_1, S_1, M_1, C_1), \ldots, (AID_n, S_n, M_n, C_n))$.

Thus, if each of the n signatures are legal, then batch verification [26] is passed. If one or more of the n signatures are invalid, then batch verification fails.

According to a previous study, batch verification can be divided into three types.

- Verifying that a signer signs a different message.
- Verifying that different signers sign the same message.
- Verifying that different signers sign different messages.

III. PROPOSAL OF THE DSSCB NETWORK ARCHITECTURE

The proposed DSSCB scheme is optimized for large-scale data storage in VANETs and the distributed security is used to address the security challenges caused by a centralized database [27]. In the DSSCB, the RSU is a PSN and the vehicle is an SN. PSNs are granted the right to write data and participate in the consensus. The SN can access and synchronize replicas, but it does not participate in the consensus. The local storage device in the PSN is responsible for collecting the sensor data uploaded by the SN and obtaining the data shared by other PSNs, as well as for automatically collating and analyzing the data using the originally deployed smart contract. According to the analysis results, the traffic management center or TA can adjust the traffic conditions for the VANET to improve the traffic efficiency and authenticity of the safety warnings. The historical data that the PSN senses after the data analysis is complete are packaged into blocks for secure storage by the DSSCB. The DSSCB has two major advantages in terms of ensuring the security and reliability of data sharing, and making the data storage more secure and available for querying. In addition, there is an important data auditing process in the DSSCB as a consensus mechanism. The consensus mechanism solves the problem of mutual trust between nodes in the decentralized system, which is crucial for ensuring the continuous operation of the blockchain system. The following entities are included in the DSSCB.

A. DATA SHARING MODEL FOR NODES IN VANETs

Three types of data sharing are allowed in the VANET system comprising V2V, V2R, and sharing between RSU-to-RSU (R2R) through a wired network. The sender signs the message with its own private key before the message is sent and the receiver verifies the signature with the sender's public key. This effectively guarantees the non-repudiation and simple verification of data sharing, thereby allowing nodes to transmit securely. In the proposed method, a digital signature algorithm based on the properties of the bilinear pairing for an elliptic curve is used to verify the identities of the vehicle and the shared message.

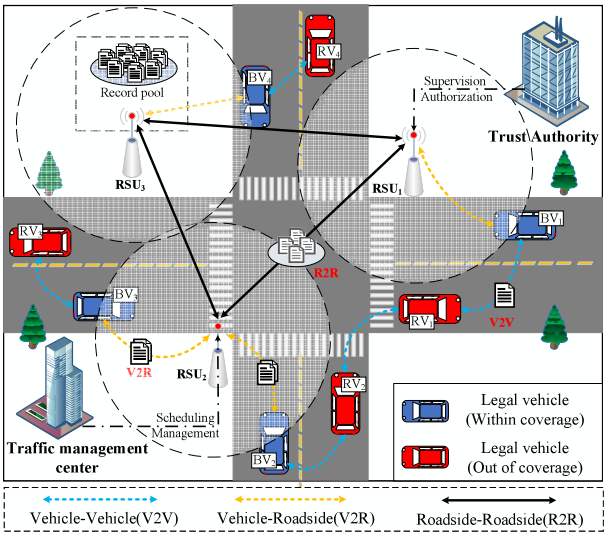

FIGURE 2. Regional model for data sharing.

In Figure 2, the blue vehicle (BV) is traveling within the communication range of the RSU and the red vehicle (RV) is traveling outside the communication range of the RSU. During V2V data sharing, relevant traffic information is transmitted mainly via a unicast or multicast mechanism, and both the sender and receiver of the message are vehicles. There are two main types of information interactions in V2V: regular periodic broadcasting of a vehicle's driving information, including the speed, direction, and traffic congestion data; and purposeful communication when a vehicle sends information to a particular target vehicle that the target vehicle must decrypt. The sent message needs to be digitally signed and validated to ensure the reliability of the data. Other nearby vehicles can then analyze and process the received messages in time to assist the driver with driving safely. The communication range [28] between vehicles is 50–300 m and the communication range of the RSU is limited to about 1000 m. In areas where the vehicle density is not very high, the V2V communication method is subject to problems

such as delayed transmission of the message, and the real-time performance of the current data cannot be guaranteed. In order to solve the V2V communication problem and share information throughout the network, vehicles can communicate with the RSU, i.e., by V2R. For example, data are transmitted to RSU_2 in BV_2 and then forwarded to BV_3 by RSU_2 to achieve long-distance data sharing between BV_2 and BV_3. The computing power and communication capability of the RSU are much larger than those of the vehicle, so it generally acts as a vehicle manager in the communication protocol, where it may assist with the management of vehicles in the area under its jurisdiction, such as key distribution and member revocation. The RSU can also share information with other RSUs via a wired connection network, so data can be sent to target vehicles that are not within the RSU coverage area, e.g., data forwarding between RSU_1, RSU_2, and RSU_3.

The TA and the traffic management center communicate with the PSN via a wired connection secure channel, such as the transport layer secure pool. PSNs are usually supervised and authorized by the TA, and they are scheduled and managed by the traffic management center. Finally, the data in the whole network can be interconnected to form a completely automated data transmission network, thereby ensuring two-way information transfer between every node in the VANET and on-demand data sharing.

B. DISTRIBUTED CONSENSUS

The distributed consensus in the blockchain technique is the core of the system and it is crucial for the correct operation of the entire blockchain system. VANETs and blockchain have similar node distribution characteristics, and their combination can solve some of the problems that affect VANETs. A consensus is reached when all of the distributed network nodes update their ledgers and a consistent statement is made in a copy of the ledger. First, the vehicle sends data to the record pool in the RSU and then packs all of the data in the record pool into blocks after a fixed time. A distributed consensus needs to be established before the data block is written in the digital ledger. In the DSSCB, the PSN with recording rights participates in the execution of this process. The data block requires that all participants verify jointly in order to allow collaborative management in new blocks. Therefore, an efficient distributed consensus is needed to solve the problem of distributed consistency in storage. In order for all PSNs to reach consensus under limited information exchange and in dynamic interactions, cooperative control is required in non-centralized control according to neighbor-based distributed control [29]. The blockchain uses a PoW mechanism that is highly dependent on the node power to ensure consistent accounting for the bitcoin network. In VANETs, the distributed consensus for RSUs is similar to bitcoin, where the RSUs compete with each other to solve a SHA256 math problem that is complex to solve but easy to verify, and the node that solves the problem first has the billing right. The authorized RSU broadcasts the data block to other RSUs and the other RSUs verify the validity of each item of traffic information in the data block, which is added to the DSSCB to form a new data block.

Proof of data contribution: We define the data coin represented by the vehicle data as a new cryptocurrency for the vehicle application. At the time when the information between the vehicles interacts, a distributed consensus mechanism is initiated to allow the network to reach a coherent protocol and the vehicle records are then uploaded to a federated blockchain for secure storage.

The proposed DSSCB is based on the traditional consistency algorithm and it is added to the practical Byzantine fault tolerance [30] (PBFT) security protection mechanism. The PBFT algorithm is executed based on message passing, which significantly improves the transaction confirmation speed and transaction throughput. This algorithm solves the inefficiency of the original Byzantine fault-tolerant algorithm and reduces the complexity of the algorithm from exponential to square. The PBFT consensus algorithm can solve the data loss and data delay problems, and it exhibits good fault tolerance in the VANET environment, thereby ensuring the maintenance of uniform system data. The distributed consensus also includes an incentive mechanism to promote the efficient operation of the blockchain system, which is the basis for building trust in the blockchain.

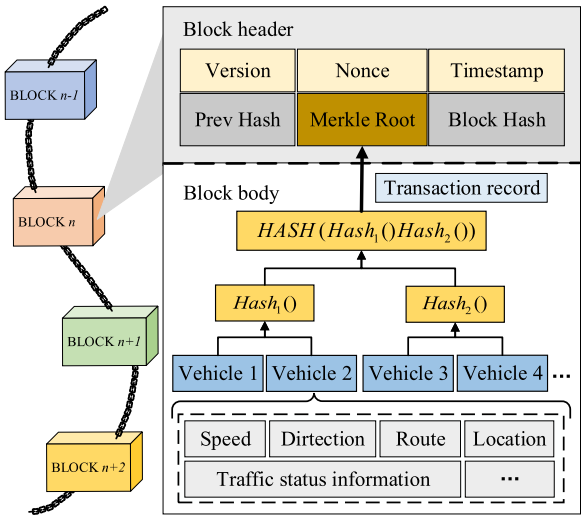

FIGURE 3. Regional model for data sharing.

C. BLOCKCHAIN AND DATA STORAGE

After a new data block is audited by the consensus mechanism, the distributed node links to the current longest main blockchain to increase the block height by one. Data blocks generally comprise block headers and block bodies [31]. As shown in Figure 3, the block header contains the current version number, solution random number for the current block consensus process, timestamp, Prev-Hash, Merkle root, and the hash value of the current block. The Prev-Hash is the hash value of the previous block and it can be used to trace the history information for the data block and to verify the legality of the data block. The block body contains a

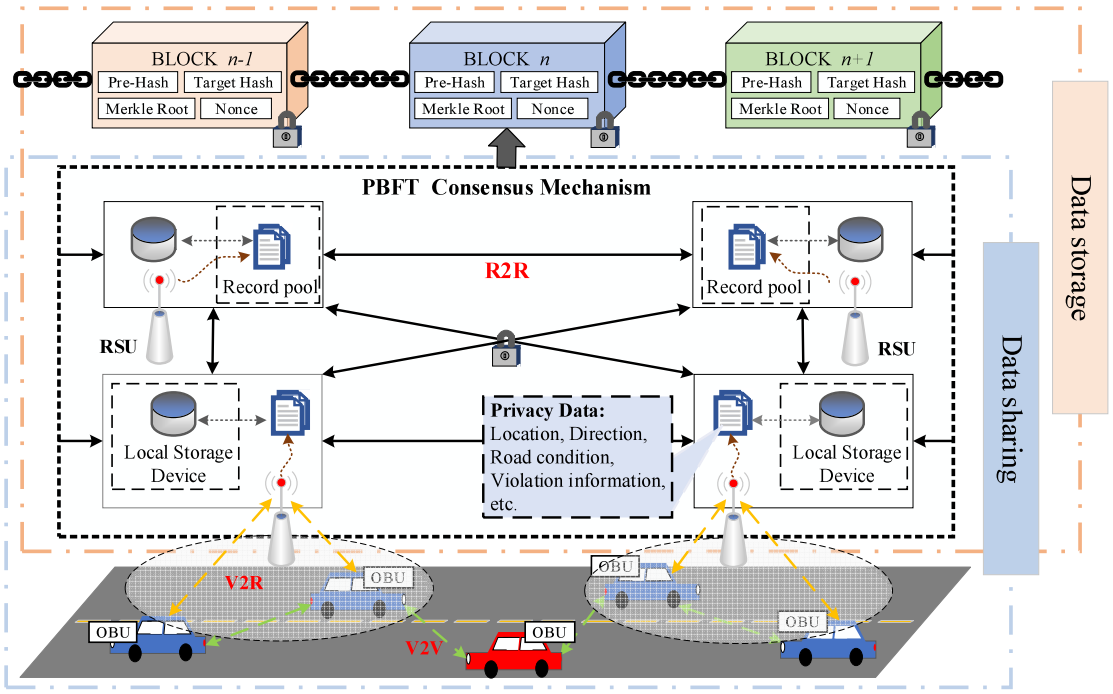

FIGURE 4. Overview of data sharing and the storage architecture in DSSCB.

Merkle tree structure [32] formed by hashing the transaction data records. The Merkle tree is a binary tree used to store transaction information. During a period of time, the received transaction data are paired and hashed separately until a unique Merkle root is generated and recorded in the block header.

Due to the limited computational power and storage space of the vehicle nodes, it is impossible to directly store all of the sensor data in the proposed DSSCB. Instead, the data are stored in an indexed list of sensor data, which indicates the specific locations of the metadata. This shared list is distributed across all the local storage devices in the RSU. The traffic management department and the vehicle node can access the data records after their authentication.

IV. IMPLEMENTATION OF THE DSSCB

Next, we discuss the specific implementation of DSSCB for secure data sharing and storage in VANETs. Figure 4 shows the system architecture based on the consortium blockchain. Record pools and local storage devices are located in the PSN in the consortium blockchain system. The record pool stores data for the consortium blockchain, including some private data uploaded by the vehicle such as location, direction, road condition, and violation information. The local storage device management employs smart contracts to control access to data sharing and it preserves the sensor data for SNs.

First, the vehicle needs a TA to grant the vehicle a legitimate identity authentication before joining the network, and it then obtains the corresponding authentication information and system parameters. The SN uploads sensor data to the PSN. The PSN verifies the identity and requests information about the SN, before determining its legitimacy and proceeding to the next step. The PSN sorts and collects the data from a certain period of time into blocks, and then signs the data and broadcasts them to the entire network. All of the PSNs engage in the distributed consensus process to compete for the permission for data writing. The SN that grants the accounting authority obtains a certain system reward and the whole network PSN synchronously updates the blockchain ledger. Finally, data sharing between PSNs can be managed by smart contracts, such as the scope for data sharing, time periods, and objects. The specific details of the operation of the DSSCB system are as follows.

A. DIGITAL SIGNATURE AND VERIFICATION OF VEHICLE DATA

The vehicles share data by wireless communication, so it is easy to monitor and forge the data during communication. Therefore, the data transmission vehicle requires a safe privacy protection method to ensure that the information is accurate and tamper-proof. For example, information from the SN must be authenticated and its integrity should be checked before it can be trusted, or an attacker can replace the information or even impersonate other vehicles to broadcast incorrect information [33]. In a previous study [34], a new anonymous authentication scheme was proposed to improve the authentication efficiency and solve the privacy protection problem in VANETs. Our solution is a further improvement and it is divided into four phases comprising the pre-distribution phase, authentication and signature key generation phase, message signing phase, and message verification phase.

TABLE 1. Units for magnetic properties.

Notation	Description
V_i	The i th vehicle
G	A cyclic additive group
G_T	A cyclic multiplicative group
RID_i	The real identity of the V_i
RID_{R_p}	The real identity of the RSU
AID_i	Pseudonym of vehicle V_i
M_i	Message sent by vehicle V_i
t_1, t_2	Timestamp associated with the transmission time
x_1, x_2	The private master key of RSU
d_i	TA generated n dimensional column vector
C_i	Random attributes generated by RSU
S_i	Final signature information
P	The generators of the cyclic group G
q	The order of G and G_T
$\hat{e}$	The bilinear map $\hat{e}: G \times G \rightarrow G_T$
P_{pub1}, P_{pub2}	The public keys of TA
H	Hash functions such as $H: \{0,1\}^* \rightarrow G$

Table 1 summarizes the notations for the publicly known system parameters used in this study.

1) PRE-DISTRIBUTION PHASE

RSU nodes and vehicle nodes need to be registered with the TA before network deployment. After each RSU and vehicle have been legally authenticated, the TA uses the following steps to generate the system parameters for them.

1) The TA selects a prime number q, two groups G and G_T of order q, a generator P in G, and a bilinear map $\hat{e}: G \times G \rightarrow G_T$.
2) TA randomly generates an $m \times n$ dimensional matrix $A(2 \leq m < n)$ and m dimensional column vector ω that satisfies the linear system of equations $Ad = \omega$ with infinite solutions, $R(A) = R(\overline{A}), \quad R(A) < n$.
3) The TA generates a unique n dimensional column vector d_i for each legal vehicle node, and d_i satisfies $Ad_i = \omega$, such that d_i is a solution of the linear equations $Ad = \omega$. The TA sends the vector d_i to the corresponding vehicle node V_i as its real identity information. TA randomly selects an m dimensional column vector D and then calculates the identity of V_i.

$$RID_i = D^T d_i \tag{3}$$

The TA transmits A, D, and ω to the RSU through a secure channel as a shared secret between the RSU and TA.

4) The RSU generates its own private key x_1 in the unit group of the prime modulus q, the finite field Z_q^*, and calculates another private key x_2.

$$x_2 = \left(D^T \omega\right) \bmod q \tag{4}$$

The corresponding public key dimension is $P_{pub1} = x_1 P$ and $P_{pub2} = x_2 P$, $H : \{0,1\}^* \rightarrow G$ is a one-way hash function. Each RSU and vehicle can publicly access the system parameters $\{G, G_T, q, \hat{e}, P, P_{pub1}, P_{pub2}, H\}$.

2) AUTHENTICATION AND SIGNATURE KEY GENERATION

The vehicle node needs to be authenticated before communicating with the RSU. After preparing to receive the message signature of the vehicle, the vehicle node sends a signature request signal to the signer RSU. The detailed steps are as follows.

1) The RSU randomly selects k, where k belongs to the finite field Z_q^*, and calculates the authentication parameters R and s

$$R = kA \tag{5}$$

$$S = k\omega \tag{6}$$

The authentication information $\left(t_1, R, H\left(s \| RID_{R_p} \| t_1\right)\right)$ is sent to vehicle user V_i, where t_1 is the timestamp associated with the transmission time of the message.

2) V_i receives the message from the RSU and stores it in the tamper-proof device. The tamper-proof device on the vehicle is considered reliable and its information is never disclosed. First, calculate.

$$r = Rd_i \tag{7}$$

and then verify that $h\left(r \| RID_{R_p} \| t_1\right) = h\left(s \| RID_{R_p} \| t_1\right)$ is true. If they are equal, send $\left(t_2, R, H\left(r \| RID_{R_p} \| t_2\right)\right)$ to RSU. t_2 is the timestamp associated with the transmission time of the message.

3) After receiving the message, the RSU verifies that $h\left(r \| RID_{R_p} \| t_1 \| t_2\right) = h\left(s \| RID_{R_p} \| t_1 \| t_2\right)$ is true. If the verification is successful, the communication with V_i will continue; otherwise, the communication will be interrupted. The random parameter y_i is selected, where y_i belongs to the finite field Z_q^*. $\rho_i = y_i P$ is calculated and the parameter ρ_i is sent to the vehicle user. If both ρ_i and RID_i are verified, the tamper-proof device will begin generating anonymous identity and signing keys. The procedure for the tamper-proof device is shown in Figure 5.

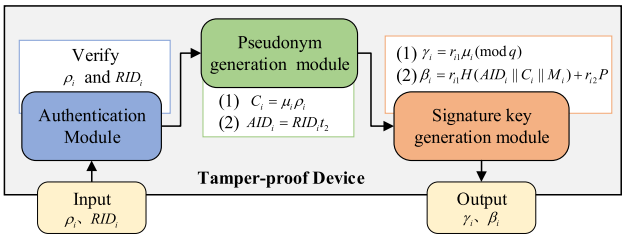

FIGURE 5. Procedure for the tamper-proof device.

4) V_i randomly selects parameters μ_i, r_{i1}, r_{i2}, and sets the randomization parameter C_i to calculate

the pseudonym AID_i:

$$C_i = \mu_i \rho_i \tag{8}$$

$$AID_i = RID_i t_2 \tag{9}$$

and it calculates the signature key β_i and γ_i :

$$\beta_i = r_{i1} H(AID_i \parallel C_i \parallel M_i) + r_{i2} P \tag{10}$$

$$\gamma_i = r_{i1} \mu_i (\mathrm{mod} q) \tag{11}$$

and the tamper-proof device finally outputs (β_i, γ_i). Within the coverage range of the RSU, the vehicle is required to perform two-way anonymous authentication when communicating with the RSU for the first time to complete the receipt of the subsequent message signature. After the certification is completed, when the vehicle communicates with other vehicles and RSU assistance is required to generate the signature, authentication is no longer required between the vehicle and the RSU, thereby reducing the communication and computational overheads of the entire communication process.

3) MESSAGE SIGNING PHASE

In the message signing phase, the RSU and vehicle jointly generate a message signature for authentication between vehicles. After receiving (β_i, γ_i) from the signer RSU, the message sent by the vehicle is signed.

$$T_i = x_1 \beta_i + x_2 y \gamma_i P \tag{12}$$

The signature T_i is calculated and sent to the vehicle user. The vehicle user receives the signature T_i sent by the signer RSU to calculate the final signature information.

$$S_i = r_{i1}^{-1} (T_i - r_{i2} P_{pub1}) \tag{13}$$

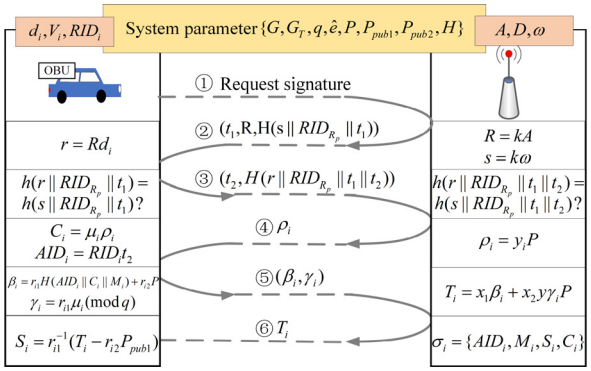

FIGURE 6. Identity authentication and digital signature process.

Finally, the vehicle obtains the signer RSU's signature $\sigma_i = \{AID_i, M_i, S_i, C_i\}$ for the message M_i, The complete identity authentication and digital signature process is shown in Figure 6.

4) MESSAGE VERIFICATION PHASE

There are two versions of the message verification process: single message verification and batch message verification. Detailed descriptions of both versions are provided in the following.

In the single message verification process, the recipient vehicle receives the signature σ_i of the sender's vehicle and checks $\{AID_i, M_i, S_i, C_i\}$ by verifying whether.

$$\hat{e}(S_i, P) = \hat{e}(C_i, P_{pub2}) \hat{e}(H(AID_i \parallel C_i \parallel M_i), P_{pub1}) \tag{14}$$

If Equation (14) is satisfied, the verification process is passed, which indicates that the vehicle identity is legal and the message M_i is received; otherwise, the message is rejected.

In the batch message verification process, RSU or V_i can verify the validity of a number of messages simultaneously, which are denoted as $\sigma_1 = \{AID_1, M_1, S_1, C_1\}$, $\sigma_2 = \{AID_2, M_2, S_2, C_2\}, \ldots, \sigma_n = \{AID_n, M_n, S_n, C_n\}$ where $M_1, M_2, \ldots, M$ may be the same.

$$\hat{e}(\sum_{i=1}^{n} S_i, P) = \hat{e}(\sum_{i=1}^{n} H(AID_i \| C_i \| M_i), P_{pub1}) \hat{e}(\sum_{i=1}^{n} C_i, P_{pub2}) \tag{15}$$

If Equation (15) is satisfied, then it is proved that the message signatures are valid and the verifier receives these messages.

B. BUILDING DATA BLOCKS FOR DSSCB

After ensuring that the node identity and data information in the network are legitimate, the PSN collects the local transaction records after a random time. Establishing a data block is a major part of the blockchain system and it comprises the following steps.

1) Preparation before building a block: The PSN digitally signs and verifies the records, and temporarily stores them in the local record pool in chronological order. When the size of the recording pool is equal to the size of the block, the system packs the information into blocks.
2) Start building data blocks: To ensure traceability and tamper resistance, each block contains the cryptographic hash of the previous block in the DSSCB system. Similar to the bitcoin system, PSNs need to find a hash value that satisfies a certain level of difficulty in order to provide them with a PoW. The PoW is provided after the PSN calculates the hash value of the current block according to the random number φ and the hash value of the previous block, timestamp, Merkle root, etc. (represented as Pre_data), and it calculates the random number φ that satisfies: $Hash\,(\varphi + \mathrm{Pr}\,e\_data) < \theta$. θ refers to the difficulty value used by the system to calculate the correct random number φ for the PSN. The system can adjust the value of θ to control the speed at which a particular φ is found [35].

3) Broadcasting a block to the whole network: The miners (PSNs) who find the target hash value fastest can broadcast the block and the specific random number to other PSNs. Other PSNs review and verify the transaction records and random numbers in the block. If the block is verified, the message records in the block will be added to the end of the main chain in linear and chronological order.

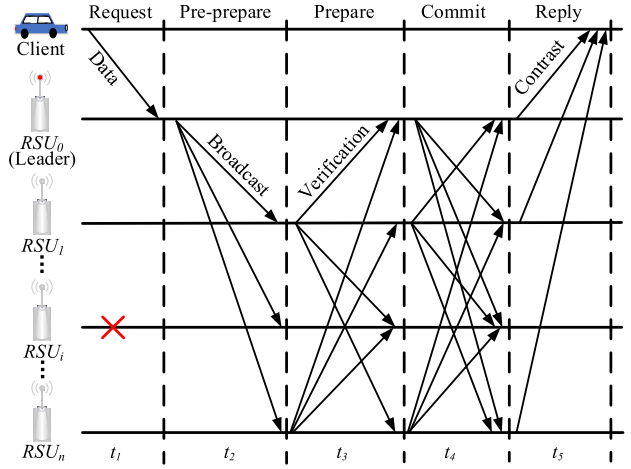

FIGURE 7. Consensus process for data storage in the DSSCB.

C. CONDUCTING THE CONSENSUS PROCESS

The consensus process is performed by the authorized RSU and the primary node (which is assumed to be RSU_0 and labeled as the leader). The leader is the fastest RSU at calculating the valid PoW certificate and the other authorized RSUs act as replica nodes. Figure 7 shows the leader broadcasting its data blocks, PoW, and timestamps to the replica nodes for verification and review. For example, $RSU_1, R\ SU_2, \ldots, RSU_i, \ldots, RSU_{n-1}$ are the replica nodes and RSU_i is the abnormal replica node. An abnormal replica node is generally a malicious node or a faulty node, and it does not respond to requests from other nodes. The total number of nodes in the network is n and the number of abnormal nodes is f. It is known that the PBFT mechanism allows the existence of anomalous nodes where $f = (n-1)/3$ without affecting the consensus result [36]. The detailed consensus steps are as follows.

1) REQUEST STAGE

All SN (i.e., client) data uploaded within the coverage range of the primary node are aggregated into a new data block. In order for their verification by review, the block contains information such as the digital signature of the primary node and the hash value of the block. The requesting end node sends a request to any RSU node, activates the node's service operation, and is called a leader.

2) PRE-PREPARATION STAGE

After receiving the request, the leader broadcasts the order of execution for the transaction to each of the replica nodes comprising $RSU_1, RSU_2, \ldots, RSU_t, \ldots, RSU_{n-1}$. The primary node sorts the multiple transactions that need to be placed in the new block from the SN and stores them in the list, and then broadcasts the list to the entire network. There are two options when receiving a message from a node, where one is normally accepted from the node and the replica node does not accept the exception in the other.

3) PREPARATION STAGE

After each node receives the transaction list, it verifies and audits the integrity and legality of the transaction. The audit result is added to the digital signature of each node and broadcast to other non-primary nodes. If the node receives a message from $2f$ different nodes, this indicates that the preparation phase has been completed for the node. The maximum number of abnormal nodes that can be tolerated by the system is f (where $n \geq 3f + 1$) and the abnormal nodes cannot be broadcast.

4) COMMIT STAGE

The node receives and summarizes the audit results from other replica nodes and compares them with its own audit results. The replica node broadcasts an acknowledgment message to other replica nodes. If the replica node receives $(n-f)$ (including its own message) confirmation messages, it sends feedback results to the client and writes the result to the block.

5) REPLY STAGE

If both the primary node and the replica nodes receive a certain number of identical requests, they are fed back to the client. Provided that the abnormal node value $f \leq (n-1)/3$ is satisfied, the consensus result will not be affected. The basic principles of minority compliance are adopted.

Finally, all of the nodes reach a consensus that the new block can be added to the consortium blockchain. The leader sends the currently audited data block and the corresponding digitally signed record to all of the authorized RSUs for storage. The block is then stored in the DSSCB and the leader receives a reward. The leader further analyzes the audit results for the RSU_i that are not approved in the system in order to determine whether these RSUs are malicious, and processes the abnormal replica nodes in time [37]. The TA will maintain or reject the abnormal replica node according to the feedback result for the replica node participating in the consensus. The proposed DSSCB uses the PBFT consensus algorithm to achieve better fault tolerance for the distributed networks and to guarantee the consistency of the system data more effectively.

The specific DSSCB implementation process is summarized in Figure 8. Data are uploaded from the vehicle node to the RSU and verified by authentication and message signatures to ensure the traceability and security of the data. The RSU then broadcasts to all the RSUs in the entire network to obtain a consistency agreement using the PBFT consensus algorithm. After the data block is verified by the entire network RSU, the block is recorded in the DSSCB.

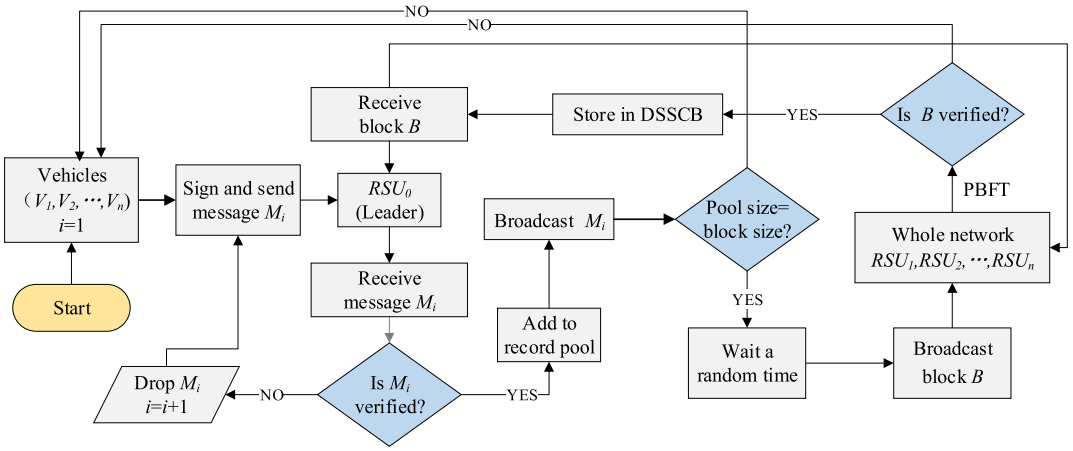

FIGURE 8. Summary of the specific DSSCB application process.

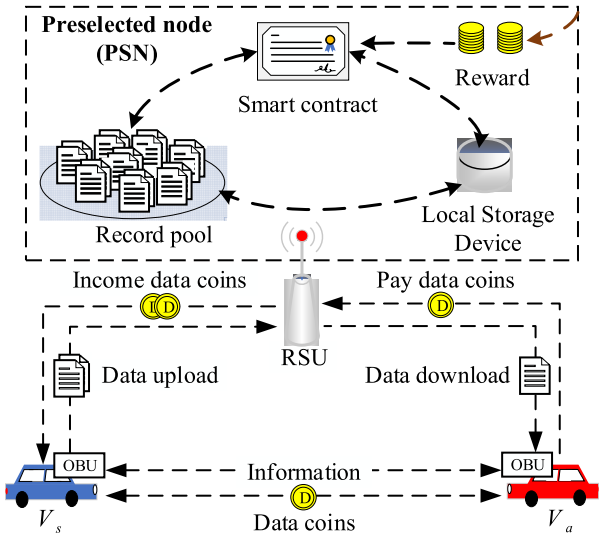

FIGURE 9. Smart contracts and data coin-based reward mechanism.

Blockchain replicas are distributed across each RSU across the network to improve the reliability and scalability of the system.

D. INCENTIVE SCENARIO BASED ON DATA COINS

After the PSN performs the consensus process to obtain the record rights for the data block, the system will provide a specific data coin reward. The PSN assigns rewards based on the ratio of data contributed by each vehicle to the data record pool. The smart contract in the local storage device sets constraints such as the allocation range and time limit for the data coins. The system will complete the operation flow by executing the script file for the smart contract. To ensure the fairness and legitimacy of data sharing, smart contracts are automatically executed when the trigger condition is met by the node joining the consortium blockchain. The incentive to give data coins is used to motivate vehicle data interactions via the DSSCB. As shown in Figure 9, the data sharing vehicle (V_s) can transmit data to the data acquisition vehicle V_a, and V_a transfers a certain amount of data coins to the address given by V_s . V_a can provide sufficient data coins to ensure the contribution of related data to finish the payment. During data interactions, data coins are defined as the proof of the amount of data contributed by the vehicle.

For example, the RSU obtains the recording rights and the system gives R data coins as a reward. It is assumed that the amount of data contributed by V_s in the RSU coverage range is s, and the total collected data recording pool is T. The smart contract in the RSU firsts check to determine whether the vehicle is within the control range and the vehicle's data proportion contributed to the record pool. The data coins are allocated according to the corresponding percentage data contribution:

$$r = R\frac{S}{T} \tag{16}$$

where r is the reward that V_s obtains for this data block record. If V_a wants to obtain the required data from the RSU or V_s, they will pay the corresponding amount of data coins to them. In order to balance the data needs and supply in the DSSCB, incentives are provided to motivate vehicle nodes to satisfy the local data needs for their own benefit. If V_s contributes collaborative intelligence more frequently to the VANET, it will be assigned a higher priority to access the resource pool.

V. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

Next, we present the security analysis and performance evaluation for our proposed DSSCB solution. The comparison shows that our scheme has many advantages.

A. SECURITY ANALYSIS FOR DSSCB

Security is critical for the VANET system during the data sharing and storage process. Our proposed DSSCB meets the security requirements required for data transactions and data storage. The relevant security features are as follows.

1) DECENTRALIZATION

In contrast to the traditional VANET data storage method, our method employs a distributed storage scheme based on the consortium blockchain. The scheme does not rely on a database of trusted third-party entities and reduces the cost required for maintaining a centralized database. It also avoids the vulnerability of traditional centralized data storage to centralized malicious attacks. Decentralized storage replicates the data content and distributes it across the nodes throughout the entire network. The overall system efficiency is improved by utilizing the idle resources available to all of the RSUs.

2) PRIVACY PROTECTION

Attackers cannot access encrypted data by brute force in a short time by using asymmetric encryption and signature verification techniques. We consider that an attacker cannot easily determine the true identity of the vehicle when a vehicle node is transmitting data. The digital signature authentication scheme based on the bilinear pairing property of the elliptic curve converts the real identity RID_i of the vehicle V_i into an anonymous identity $AID_i = RID_i t_2$, where $RID_i = D^T d_i$. Even if the attacker knows that the TA is the only d_i generated by the vehicle V_i, then it is necessary to know the m dimensional column vector D that is randomly selected by the TA. Therefore, we consider that it is very difficult to determine the true identity of the vehicle V_i, thereby ensuring identity privacy protection.

3) NON-REPUDIATION AND INTEGRITY

During the data sharing phase, all transaction data need to be signed by the current vehicle node before they are sent. The identity is then verified by the legal vehicle registered with the TA and the authorized RSU. Only legitimate and authenticated vehicles can share and receive data. Knowing the source of the data sender based on a digital signature technique ensures the non-repudiation of the data. All of the encrypted sensor data are publicly audited by using the PoW mechanism and verified by the PSNs. If the data are changed or incomplete, the consensus phase will not be passed, which ensures the integrity of the data sent.

4) UNFORGEABLE AND TAMPER-PROOF

In our proposed scheme, the distributed nature of the consortium blockchain combined with the digital signature technique ensures that no attacker can act as a vehicle node to threaten the network because no entity can falsify the digital signature of another entity without the private key of the signer. An opponent that controls one or more RSUs in the DSSCB is also unable to change any of the information in the current real data. The PBFT consensus mechanism is employed, so the system can still work normally if 33% of the nodes are damaged [36]. If we suppose that there are f abnormal RSU nodes in the whole network and the total number of RSUs satisfies $n \geq 3f + 1$, then the system can defend against malicious tampering data attacks initiated by abnormal RSUs to ensure that the final consensus results are not changed.

An example is provided as follows. Let the total number of RSUs in the area be n and the probability that one RSU wants to be an abnormal RSU is 1/2. The attacker wants to tamper with the consensus result and needs to control the malicious node with $f = (n-1)/3$ at least. In this case, the probability of successful tampering is only $1/2^{(n-1)/3}$. Thus, as the number of RSUs in the whole network increases, the possibility of malicious tampering will decrease and the system will be more stable. Therefore, our proposed method is unforgeable and tamper-proof. Table 2 compares the performance of our DSSCB scheme and other schemes [13]–[15], [17]. In general, the proposed DSSCB is more advantageous than the other four solutions in terms of data sharing and storage for vehicles in VANETs.

TABLE 2. Performance comparison between DSSCB and other solutions.

Characteristic	[13]	[14]	[15]	[17]	DSSCB
Decentralization	×	×	√	√	√
Privacy protection	√	√	√	√	√
Anonymity	√	√	×	×	√
Tamper-proof and unforgeable	√	√	√	√	√
Traceable	√	×	√	√	√
Scalable	×	×	×	√	√
Lightweight	×	×	×	√	√
Low overhead and high efficiency	×	√	×	×	√

B. PERFORMANCE EVALUATION FOR DSSCB

We evaluated the performance of the proposed DSSCB scheme in terms of the computational delay and communication overheads, as follows.

1) CALCULATION DELAY

During data sharing by vehicles, the main computational delay is the verification delay for the message. We compared the signature verification method used by DSSCB with the verification schemes employed in other scenarios. T_{mul} represents a point multiplication operation on an elliptic curve T_{par} represents a bilinear pairwise operation, and T_{mtp} represents the time of a MaptoPoint hash operation. These three operations mainly affect the verification speed so other operations can be ignored. We implemented a previously described method [38] for an MNT curve [25] with an embedding degree of 6 and the order was represented by 160 bits. The experiment was executed using an Intel Pentium IV 3.0-GHz system and the following results were obtained: $T_{par} = 4.5$ MS, $T_{mtp} = 0.6$ MS, and $T_{mul} = 0.6$ MS.

The verification delays with our scheme were compared with some representative scenarios, i.e., Zhang *et al.*'s

TABLE 3. Comparison of the verification delay.

Scheme	Verifying a signature	Verifying n signatures
IBV [11]	$3T_{par}+T_{mtp}+T_{mul}$	$3T_{par}+nT_{mtp}+nT_{mul}$
SPRING [12]	$3T_{par}+11T_{mul}$	$3nT_{par}+11nT_{mul}$
IBCPPA [13]	$3T_{par}+4T_{mtp}$	$(2+n)T_{par}+4nT_{mtp}$
EAAP [14]	$2T_{par}+5T_{mtp}$	$(n+1)T_{par}+(n+4)T_{mtp}$
Our scheme	$3T_{par}$	$3T_{par}$

IBV [11], Lu *et al.*'s SPRING [12], Shao *et al.*'s IBCPPA [13], and Azees *et al.*'s EAAP [14]. Table 3 shows the verification delay time for all of the scenarios when verifying a single request and n requests, where the results demonstrate that our proposed scheme required relatively little time to verify the delay when verifying a single message. In addition, the verification delay did not increase as the number of verification messages increased.

Figure 10(a) compares the delay times required by different schemes when verifying a signature. We calculated the delay time for each scheme for comparison, i.e., IBV $= 3\ T_{par} + T_{mnp} + T_{mul} = 3 \times 4.5 + 0.6 + 0.6 = 14.7$ ms, SPRING $= 3\ T_{par} + 11\ T_{mul} = 3 \times 4.5 + 11 \times 0.6 = 20.1$ ms, IBCPPA $= 3\ T_{par} + 4\ T_{mtp} = 3 \times 4.5 + 4 \times 0.6 = 15.9$ ms, EAAP $= 2\ T_{par} + 5\ T_{mtp} = 2 \times 4.5 + 5 \times 0.6 = 12$ ms, and our scheme $= 3\ T_{par} = 3 \times 4.5 = 13.5$ ms. According to this comparison, the verification delay time required for our scheme was only 91.83% of that when using IBV, which was 67.16% of that with SPRING and 84.91% of that with IBCPPA. Figure 10(b) shows that our method performed significantly better than the other solutions as the number of verification signatures increased.

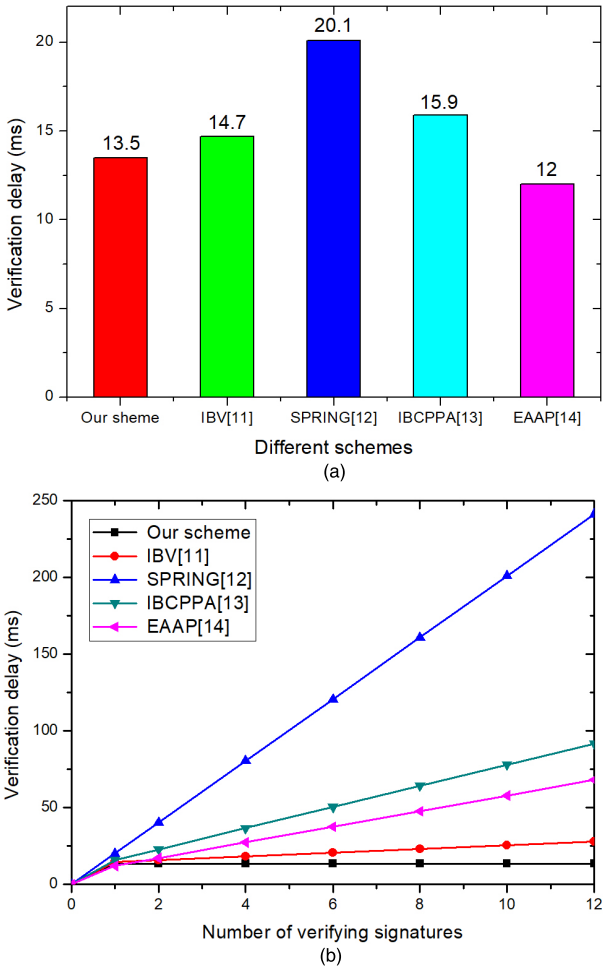

FIGURE 10. Verification delay and number of signatures verified. (a) Verifying the delay of a signature. (b) Verifying the delay of multiple signatures.

2) TRANSMISSION PERFORMANCE

The transaction confirmation time for a data block in our proposed DSSCB scheme was set to 10 min, whereas the transaction block confirmation time for the traditional blockchain (e.g., the bitcoin system) is 60 min. In terms of obtaining a consensus regarding data blocks, the PBFT requires peer-to-peer communication between nodes, so the number of consensus nodes required for this communication mechanism does not need to be excessively large and the consensus process is only performed on the PSNs instead of all network nodes. In this mode, the speed at which the nodes agree is faster and the latency is lower.

Compared with the traditional blockchain, our DSSCB method shortens the time required to confirm a data block by nearly six times and it improves the transmission efficiency by 83.33%, as shown in Figure 11. Due to the control of the number of nodes, our method does not consume as much computational power as the blockchain system and the throughput for the whole network is greatly improved. In terms of the data block consensus, we only implement the consensus processes for RSUs instead of all the connected nodes.

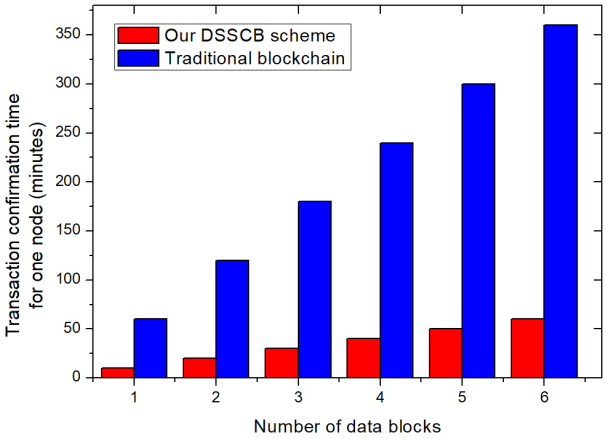

FIGURE 11. Comparison of transmission performance.

We analyze the transmission overhead of our scheme, compared to those of IBV [11], SPRING [12], IBCPPA [13] and EAAP [14] schemes. The transmission overhead consists of sending the information from a vehicle to an RSU in V2R communication or the two vehicles in V2V communication. Table 4 lists the total transmission overhead of all schemes in terms of sending out a single message and n messages.

TABLE 4. Comparison of the transmission overhead.

Scheme	Sending a signature	Sending n signatures
IBV [11]	63 bytes	63 n bytes
SPRING [12]	189 bytes	189 n bytes
IBCPPA [13]	833 bytes	833 n bytes
EAAP [14]	220 bytes	220 n bytes
Our scheme	60 bytes	60 n bytes

Generally, the transmission overhead brought by the identity information, certificate, pseudo identity and timestamp etc. The packet of IBV consists of a 21-byte signature and a 42-byte pseudo identity. The total transmission overhead of the IBV scheme is 63 bytes. The packet size of SPRING scheme costs 189 bytes, which contains a 40-byte signature, a 121-byte certificate, a 26-byte anonymous key and a 2-byte ID. The transmission overhead of IBCPPA scheme includes an 826-byte signature, a 4-byte timestamp and a 3-byte ID. The total packet sizes of IBCPPA are 833 bytes. The packet of EAAP scheme costs 220 bytes, which makes up of a 20-byte signature, a 20-byte public key and a 180-byte certificate. However, opposed to the traditional digital signature system based on large number decomposition and discrete logarithm, the signature length of our scheme is relatively short, requiring only 60 bytes. From Table 4, we can see that our scheme has advantages over other schemes in terms of transmission overhead.

VI. CONCLUSION

Due to the rapid development of VANETs, the centralized databases will collect increasing amounts of data. Therefore, we proposed a DSSCB solution for distributed storage. The integrity and security of the data can be ensured by a digital signature technique when a vehicle node uploads sensor data. The PBFT consensus mechanism is them applied to increase the speed of data transactions. The blockchain replica comprising sensor data is finally distributed and stored in the RSU, which addresses the potential security risks associated with centralized data storage. The RSU internally sets the constraints for data sharing by using smart contracts, including the shared time, region scope, and objects. Data coins represent the contribution of data sharing and they are used to motivate the vehicles to share data so the entire network can operate safely and efficiently. Safety analysis and performance evaluations showed that our solution is safer and more efficient than previously proposed solutions. In future research, we will improve the security and real-time authentication and message verification processes during data sharing, and further improve the efficiency of our proposed solution.

REFERENCES

[1] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[2] R. Brendha and V. Prakash, "A survey on routing protocols for vehicular ad hoc networks," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–7.

[3] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart., 2008.

[4] I. A. Sumra, H. B. Hasbullah, A. Manan, and J. L. Bin, "Comparative study of security hardware modules (EDR, TPD and TPM) in VANET," in *Proc. 3rd Nat. Inf. Technol. Symp. (NITS)*, Riyadh, Saudi Arabia, Mar. 2011, pp. 6–9.

[5] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Sys.*, vol. 50, no. 4, pp. 217–241, 2012.

[6] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Mar. 2013.

[7] C. D. Wang and J. P. Thompson, "Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network," U.S. Patent 5 613 039, Mar. 18, 1997.

[8] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, Mar. 2017.

[9] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, vol. 16, 2016, pp. 254–269.

[10] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, 2016. doi: 10.1371/journal.pone.0163477

[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Phoenix, AZ, USA, Apr. 2008, pp. 246–250.

[12] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant network," in *Proc. 29th IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1229–1237.

[13] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[14] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[15] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.

[16] M. Verma and D. Huang, "SeGCom: Secure group communication in VANETs," in *Proc. IEEE CCNC*, Jan. 2009, pp. 1–5.

[17] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[18] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[19] D. Johnson, A. Menezes, and S. Vanstone, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. Springer-Verlag, 2001.

[20] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.

[21] S. J. Koh, M. J. Chang, and M. Lee, "MSCTP for soft handover in transport layer," *IEEE Commun. Lett.*, vol. 8, no. 3, pp. 189–191, Mar. 2004.

[22] V. S. Miller, "Use of elliptic curves in crytography," in *Proc. Adv. Cryptol.*, Aug. 1985, pp. 417–426.

[23] N. Torri and K. Yokoyama, "Elliptic curve cryptosystem," *FUJITSU Sci. Tech. J.*, vol. 36, no. 2, pp. 140–146, 2000.

[24] D. Boneh, M. Franklin, *Identity-Based Encryption from the Weil Pairing*. Berlin, Germany: Springer, 2001, pp. 213–229.

[25] A. Miyaji, M. Nakabayashi, S. Takano, "Characterization of elliptic curve traces under FR-reduction," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Springer, 2000, pp. 90–108.
[26] J. Camenisch, S. Hohenberger, and M. Pedersen, "Batch verification of short signatures," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 2007, pp. 246–263.
[27] X. Tang, K. Li, Z. Zeng, and B. Veeravalli, "A novel security-driven scheduling algorithm for precedence-constrained tasks in heterogeneous distributed systems," *IEEE Trans. Comput.*, vol. 60, no. 7, pp. 1017–1029, Jul. 2011.
[28] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A survey of inter-vehicle communication protocols and their applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 3–20, 2nd Quart., 2009.
[29] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multi-vehicle cooperative control," *IEEE Control Syst. Mag.*, vol. 27, no. 2, pp. 71–82, Feb. 2007.
[30] T. Crain, V. Gramoli, M. Larrea, M. Raynal. (2017). "(Leader/Randomization/Signature)-free byzantine consensus for consortium blockchains." [Online]. Available: https://arxiv.org/abs/1702.03068
[31] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[32] D. R. Morrison, "PATRICIA—Practical algorithm to retrieve information coded in alphanumeric," *J. ACM*, vol. 15, no. 4, pp. 514–534, 1968.
[33] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[34] E. B. Hamida and M. A. Javed, "Channel-aware ECDSA signature verification of basic safety messages with k-means clustering in VANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2016, pp. 1–8.
[35] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[36] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.
[37] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[38] M. Scott. (2009). *Efficient Implementation of Cryptographic Pairings*. [Online]. Available: http://ecryptss07.rhul.ac.uk/Slides/Thursday/ms cottsamos07.pdf

XIAOHONG ZHANG received the B.S. degree in physics from Jiangxi Normal University, Jiangxi, China, in 1984, the M.S. degree in optical information processing from the Chinese Academy of Sciences, Changchun, China, in 1990, the Ph.D. degree in control theory from the University of Science and Technology Beijing (USTB), in 2002, and the Ph.D. degree in information safety from the Beijing University of Posts and Telecommunications (BUPT), in 2006. She was a Visiting Scholar with the University of California at Berkeley, Berkeley, CA, USA, from 2014 to 2015. She is currently a Full Professor with the College of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. Her main research interests include blockchain technology, information security, nonlinear dynamics, and wireless sensor networks.

XIAOFENG CHEN received the B.S. degree in communication engineering from the Jiangxi University of Science and Technology, Jiangxi, China, where he is currently pursuing the M.S. degree in electronics and communication engineering. His current research interests include blockchain technology and information security.