IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 22, 2019, accepted July 13, 2019, date of publication July 16, 2019, date of current version August 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2929259

Adaptive Traffic Signal Control Mechanism for Intelligent Transportation Based on a Consortium Blockchain

XIAOHONG ZHANG AND DI WANG
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 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 The development of vehicular ad-hoc networks (VANETs) has facilitated adaptive traffic signal control for intelligent transportation. In this paper, we proposed the traffic signal control mechanism based on a consortium blockchain, which has saved plenty of financial and material resources. It has solved the centralization problems and minimized the high degree of human intervention in the process of traffic signal light management. As a road is congested, the vehicle forwards road condition messages. The traffic department (*TD*) adjusts the signal light duration to allow the synergistic optimization management, and control the traffic vehicle status through a smart contract. In addition, we propose a credibility mechanism to effectively prevent vehicles from broadcasting mendacious messages and malicious requests, thereby enhancing the credibility of vehicles and providing a secure and trustworthy communication environment for the VANETs. It is hazardous for vehicles to send plaintext messages in an open environment because their privacy and security are threatened. Thus, we utilize ElGamal encryption and group signature algorithm to guarantee the confidentiality, privacy, and non-repudiation of any information. The safety analysis and performance evaluation demonstrate that the scheme is feasible and valid, and it can facilitate the adaptive control of traffic signal lights.

INDEX TERMS Consortium blockchain, traffic signal, vehicular ad-hoc networks (VANETs), adaptive control, group signature.

I. INTRODUCTION

Official statistics indicate that the number of registered vehicles will reach 2 billion in the next 10 to 20 years [1]. The increased number of vehicles has led to a poor traffic environment, such as severe road congestion, or the rise of traffic accidents. A key element of traffic jams is the improper signal configuration of the duration at intersections [2]. At present, traffic signal control mainly comprises timing control, induction control, and adaptive control. Timing control for signal lights is only utilized in conditions which the traffic flow is stable. Induction control is not sensitive to time parameters, such as the time period. Adaptive traffic signal control regulates the cycle time of the signal light in real time based on the actual traffic flow. So dynamic real-time traffic signal regulation is essential for addressing traffic congestion issue [3], [4].

Video technology is applied to statistically analyze the number of vehicles [5]–[7], but these schemes are susceptible to severe weather, thereby resulting in large errors in terms of the calculated traffic density. Wu *et al.* [8] employ a two-layer pipe model to gather and process traffic status messages transmitted by vehicles, then dynamically adjusting the durations of the signal lights according to the real-time road conditions. However, above schemes are vulnerable to attacks on the central node, because they all calculate the density of the vehicle flow in a centrally controlled manner, which leads to information asymmetry and information islands. Thus, a distributed collaborative method is developed to obtain traffic flow information, which has good stability [9] and is not

The associate editor coordinating the review of this manuscript and approving it for publication was Lu An.

attacked by central nodes or affected by weather. Moreover, Shaghaghi *et al*. utilize the traffic messages sent by vehicles to generate the traffic signal duration and dynamically control the signal lights [10]. The above schemes can realize the dynamic regulation of traffic lights, but there are still many shortcomings:

1) Security threats: In [9] and [10], the traffic information transmitted in plaintext, which is vulnerable to be tampered with or forged by attackers, thereby undermining the confidentiality and security of message. Assumpting an attacker may tamper with a message that is heavily congested on the road to a smooth road. This malicious tampering reduces road traffic efficiency and even threatens traffic safety.
2) Centralization: The traditional traffic signal control system adapts a central control to calculate the density of the traffic flow. It is easy to be collapsed because of the attack of the central nodes. At the same time, the maintenance and update of the central controller require a lot of manpower, material and financial resources. Central control is liable to cause information asymmetry and form information islands.

Therefore, it has become the focus of academia to obtain real and accurate traffic information by decentralization. Vehicular ad-hoc networks (VANETs) have significant roles in the communication process for intelligent transportation systems [11]. Each vehicle is regarded as a node in a VANET, where a vehicle has the ability to transmit information and provide request services in a vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) manner. The security, confidentiality, and anonymity of communication processes are threatened by the high mobility and volatility of VANETs. Thus, many studies have investigated privacy protection for VANETs. A trust authority can issue a certificate for each vehicle [12] and this certificate can be used to generate a signature for the traffic information, but it cannot address the problem of certificate management and private key escrow. Cui *et al*. [13] propose a cuckoo filter to speed up the signature time, but not the batch verification process, thereby leading to large computational overheads and a failure to address the key escrow problem. Limbasiyae and Das [14] base on a vehicular cloud computing platform to effectively prevent plaintext and man-in-the-middle attacks, the computational cost of this scheme is small but the communication overheads are large. In addition, a distributed and scalable privacy protection algorithm is proposed to effectively avert Sybil and denial-of-service attacks [15].

The above schemes guarantee the security and confidentiality of message to a certain extent, but the centralization problem remains unsolved. Therefore, a blockchain-based privacy protection announcement in the VANET [16] is proposed to ensure the reliability of vehicle information transmission but without exposing a vehicle's private information. This scheme uses a threshold ring signature to verify the message, where the number of attackers who forge the signature is higher when the size of the ring increases. Lu *et al*. [17] proof the existence and absence of blockchain technology to update and revoke public keys, thereby preventing vehicles from sending forged and false messages. However, the frequent updating and revoking of the private key can readily cause network congestion and data redundancy. The attributed-based blockchain first supports the non-interactive access control of traffic data by a fine-grained blockchain structure [18], achieving a balance between privacy protection and information availability. Jiang *et al*. [19] propose a blockchain architecture and network model to ensure distributed secure storage for the characteristics of Internet of Vehicles (IoV). The data is validated by several blocks whose timestamp is within a certain range, effectively avoiding data damage caused by attacks on a single roadside unit (*RSU*) node. For the VANET, new vehicle identity authentication mechanisms by using the blockchain consensus and dissemination [20], [21] have designed, they can effectively improve the quality of authentication and reduce malicious attacks on the network.

Different from the existing literature, we propose an adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain, and break the central control of traffic signals for VANETs. The significant contributions of this paper are as follows.

1) In order to avoid attacks on the center node and to prevent information asymmetry with intelligent traffic signal control, the decentration of the blockchain eliminates the need for the central control of signal lights. The distributed blockchain structure ensures that the entire signal control mechanism is not affected and it is highly robust when some *RSU* are damaged or attacked.
2) Traffic department (*TD*) decrypts the message stored in the consortium blockchain. ACP (Artificial system, Computational experiments, Parallel execution) is applied to realize the coordinated optimization of signal light management, and control via the parallel execution by artificial traffic signal systems.
3) An efficient batch verification algorithm based on BLS (Boneh-Lynn-Shacham) group signature is proposed to guarantee non-repudiation of the message, and solved the potential security risks, meanwhile ElGamal encryption algorithm can ensure the confidentiality and integrity of the message. In the information acquisition process, the vehicle is provided with conditional anonymity to protect the identity and privacy of the vehicle, and the malicious vehicle identity can be traced and revealed when disputes arise.
4) We analyzed the security as well as evaluating the communication overheads and computational cost of the algorithm, thereby demonstrating that the proposed algorithm obtained better real-time performance than other algorithms, and it could satisfy the security and privacy requirements of VANETs.

II. PRELIMINARIES

A. CONSORTIUM BLOCKCHAIN

Nakamoto described the new concept of digital currency in 2008 [22] and proposed the notion of a blockchain for the first time. A blockchain is based on the underlying Bitcoin technology, where it allows open, transparent, and decentralized data interactions by using asymmetric encryption, an incentives mechanism, consensus algorithms, and chained structures in scenarios without mutual trust. All nodes allow the distributed recording, storage, and updating of data, and achieve successful communication by maintaining a common blockchain, which information can be verified, saved and cannot be tampered with permanently.

The types of blockchain are divided into three categories: a public blockchain, private blockchain, and consortium chain [23]. Nodes in the public blockchain can freely enter or leave the network without permission to achieve complete decentralization. However, the number of network nodes is very large, so data verification and the node consensus time are also high, and causes system delay in network. Only some nodes in a private blockchain own read and write permissions, whereas most nodes have limited read permissions. The status of network nodes is not equal and data sharing cannot be achieved. A consortium blockchain preselects a certain number of bookkeeper nodes to verify the validity of data and blocks, and thus a shorter time is required to reach a consensus and for data verification in consortium blockchain, which accelerates the generation of blocks. The traffic signal time allocation is high for data verification and in terms of the consensus time, so consortium blockchain is most suitable for this paper. The incentive mechanism, cryptographic signature, consensus algorithm, and timestamp for the consortium blockchain optimize the traditional traffic signal time allocation mode. The distributed shared ledger solves the transaction data centralization problem. ElGamal encryption protects the privacy of data among the interacting parties, as well as improving the security and message transparency in VANET information interactions.

The *RSUs* in the consortium blockchain are equal. Appropriate *RSUs* are preselected as bookkeeper nodes according to the number of network nodes. The AlgoRand [24] consensus algorithm is applied, which is characterized by low delay, decentralized control, and flexible trust, and only a small number of computations are required.

B. ACP APPROACH

The physical traffic signal control system and its virtual artificial counterparts can be operated and interacted by an ACP parallel system [25], [26]. The ACP comprises an artificial system (A), computational experiments (C), and parallel execution (P), as described in the following.

- Artificial system (A). Making use of data mining technology and bottom-up multi-agent methods to model the traffic signal physical system and simulate its characteristics.
- Computational experiments (C). Utilizing machine learning, and statistical analysis, *TD* decrypts the road condition information stored in the blockchain and integrates factors (i. e. vehicle type and road congestion) into the artificial traffic signal control system.
- Parallel execution (P). Virtual and reality are a pair of parallel control systems. The results calculated by artificial (virtual simulation) traffic signal control system are feedback to the physical (reality) system, then execute in parallel the allocation and control of the green light duration.

C. BILINEAR PAIRING

Supposing g_1 and g_2 be additive cyclic groups and multiplicative cyclic groups of prime order p, respectively. The bilinear mapping [27], [28] $e\,(g_1, g_1) \rightarrow g_2$ satisfies the following properties:

- Bilinear: for all $U, V, S \in g_1, s, t \in Z_p^*$,

$$\begin{cases} e(sU, tV) = e(U, V)^{st} \\ e(U, V + S) = e(U, S)e(U, S) \\ e(U + S, V) = e(U, V)e(S, V) \end{cases} \tag{1}$$

- Non-degeneracy: $e\,(U, V) \neq 1$ for all $U, V \in g_1$.
- Computability: $e(U, V)$ for $U, V \in g_1$ computable in *polynomial time.*
- Symmetry: $e(U, V) = e\,(V, U)$ for $U, V \in g_1$.

D. CHINESE REMAINDER THEOREM

The Chinese remainder theorem [29] sets positive integers $b_1, b_2, \cdots, b_k$ as pairwise prime, where $B = b_1 b_2 \cdots b_k$, $B_i = B/b_i, (i = 1, 2, \cdots, k), b_i > a_i$, and the congruence equations are:

$$\begin{cases} D \equiv a_1 (\mathrm{mod} b_1) \\ D \equiv a_2 (\mathrm{mod} b_2) \\ \cdots \\ D \equiv a_k (\mathrm{mod} b_k) \end{cases} \tag{2}$$

The solution of the congruence equations is $D \equiv a_1 B_1 B_1^{'} + a_2 B_2 B_2^{'} + \cdots + a_k B_k B_k^{'} (\mathrm{mod} B)$, where $B_i^{'} B_i \equiv 1 (\mathrm{mod}\ b_i), i = 1, 2, \cdots, k$

E. ELGAMAL CRYPTOSYSTEM

The ElGamal encryption algorithm [30] is a multiplicative homomorphic encryption algorithm, which comprises key generation, encryption algorithm, and decryption algorithm processes. The ElGamal encryption algorithm is developed based on the difficulty of computing discrete logarithm problems on cyclic groups and the Diffie–Hellman hypothesis, which is a semantic security encryption algorithm.

- Key generation. Randomly select a large prime number q. $O(O < q)$ is the generator of the cyclic group Z_p^*. Randomly select a number x $\in$ Z_p^*. Calculate $\lambda = g^x \bmod q$. The public key is (λ, g, q) and the private key is x.

- Encryption algorithm. Select a random number k, which is relatively prime with $q-1$, to calculate the ciphertext as follows.

$$C = E(M) = (c, d) = (g^k \bmod q, \lambda^k M \bmod (q-1)) \quad (3)$$

- Decryption algorithm. Calculate the plaintext:

$$M = D(C) = d/c^x (\mathrm{mod} q) = d(c^x)^{-1} \bmod q \quad (4)$$

F. GROUP SIGNATURE

A group signature [31], [32] is a special signature method, which involves a group manager (GM), a group discloser (GD), and group members (M).M registers with GM to join the group and when the signature verifier finds a forged message or signature verification fails, GD can trace the true identity of the malicious group member. The group signature used in this paper involves group creation, joining group, signature, signature verification, signature opening, and member revocation.

- Group creation. Set G_1,G_2 as the additive cyclic group and the multiplicative cyclic group with order that is prime p. P is the generator, the bilinear pair is $e(G_1, G_1) \rightarrow G_2$, the Hash function is $H : Z_p^* \rightarrow G_1$, the system parameter is $S = \{G_1, G_2, e, p, P, H\}$, and GM randomly selects $y_{GM_i} \in Z_p^*$ as the private key and calculates $Y_{GM_i} = y_{GM_i} P \in G_1$ as the group public key.
- Joining group. User U_i randomly selects $y_{U_i} \in Z_p^*$ as the private key and calculates $Y_{U_i} = y_{U_i} P$ as the public key. U_i randomly selects $d_i \in Z_p^*$ and the user's real identity is ID_{U_i}. Each user is assigned a pseudonym $FID_{U_i} = ID_{U_i} \oplus H\left(Y_{U_i} + d_i\right)$. The user requests to join the group and sends FID_{U_i} to GM. GM determines the identity legitimacy of U_i and sends $(FID_{U_i}, d_i, Y_{U_i})$ to GD, and then saves $(FID_{U_i}, d_i, Y_{U_i})$ in the storage list. U_i joins the group as a group member and then randomly selects $y_i^U \in Z_p^*$. U_i calculates $Y_i^U = y_i^U P$, $sp_{U_i} = \left(x_i^u + y_{U_i}\right) (\mathrm{mod} p)$ as the private key of the group member. GM randomly selects the prime number q_i,when $i \neq i^{'}$,$q_i \neq q_{i^{'}}$, and applies the public key of the received group members to calculate $D \equiv Y_1 Q_1 Q_1^{'} + Y_2 Q_2 Q_2^{'} + \cdots + Y_s Q_s Q_s^{'} (\mathrm{mod} Q)$ using the Chinese remainder theorem, where $Q_i Q_i^{'} \equiv 1 (\mathrm{mod} q_i)$, $i = 1, 2, \cdots, s$, and then broadcasts D.
- Signature. U_i signs the message M, calculates $\sigma_i^U = sp_{U_i} H(M)$, and sends $(M, \sigma_i^U, FID_{U_i})$ to GM. GM determines whether U_i is a group member according to FID_{U_i}. GM refuses to receive the message if it is not a group member; otherwise, GM calculates $\sigma_i^{GM} = y_{GM_i} H(M)$ and randomly selects $z_i \in Z_p^*$ to calculate $Z_i = z_i P$, $w_i = z_i H(M)$,$\sigma_i = \sigma_i^{GM} + \sigma_i^U + w_i$, and $S_{U_i} = Y_i^U + Y_{U_i} + Z_i$. GM sends $(Y_{U_i}, H(M), z_i)$ to GD. GD saves it in the storage list and the signature of message M is $sign = (\sigma_i, S_i, q_i)$.
- Signature verification. a) Single message verification: GM first verifies whether $Y_{U_i} = D (\mathrm{mod} q_i)$ is true, before verifying whether the equation $e(P, \sigma_i) = e\left(Y_{GM_i} + S_{U_i}, H(M)\right)$ is true. GM receives message M if verification is successful; otherwise, the message M is rejected. b) Batch verification: GM first verifies whether $Y_{U_i} = D (\mathrm{mod} q_i)$ is true. The signature is $(\sigma_1, S_1, q_1), (\sigma_2, S_2, q_2), \cdots, (\sigma_n, S_n, q_n)$, and if the equation $e(P, \sum_{i=1}^{n} \sigma_i) = e\left(Y_{GM_i} + \sum_{i=1}^{n} S_{U_i}, \sum_{i=1}^{n} H(M_i)\right)$ is true, then the verification process is successful and the message M is received; otherwise, the message M is rejected.
- Signature opening. If the signature verification process fails or the message is falsified and forged, GD opens the group signature, calculates $Y_{U_i} = D (\mathrm{mod} q_i)$ based on the signature $sign = (\sigma_i, S_i, q_i)$, queries Y_{U_i} corresponding to FID_{U_i} in the storage list, and exposes the true identity of the signer by calculating $ID_{U_i} = FID_{U_i} \oplus H(Y_{U_i})$.
- Member revocation. If group member $U_i (1 \leq i \leq s)$ leaves the group, U_i sends a leave request Req_{left} to GM, which updates Y_{U_i} to a random prime number $Y_{U_i}^{'}$, recalculates $D^{'}$, and publishes it.

III. PROPOSED INTELLIGENT TRAFFIC SIGNAL CONTROL MECHANISM

A. SYSTEM DESIGN

In case of dense traffic condition at a signal intersection, an onboard unit (OBU) forwards the road condition information to the vicinal RSU. The $RSUs$ record the road condition information to the block. Other RSU nodes verify the validity of the block and then connect the block to the blockchain after successful verification. The smart contract triggers the TD to decrypt the information recorded in the blockchain and the ACP is called to regulate the green light duration according to the real-time road conditions. When the traffic flow is sparse, we employ leaping signal control to improve the green time utilization and achieve intelligent traffic light control. After controlling the signal lights, TD gives a reward to vehicles that send accurate and reliable information to enhance the credibility of the OBU. By contrast, a punishment is sent to the vehicle with fake information. This credit mechanism yields a safe and reliable vehicle ad-hoc network communication environment. $OBUs$ can use the existing credit value to obtain the information for other roads. If the information sent by other $OBUs$ is authentic and credible, then they will receive the corresponding credit value reward. Table 1 shows the symbols and definitions used in the model of the traffic signal control mechanism.

B. SYSTEM MODEL

The overall structure of the system model is shown in Figure 1.

A diagram showing the structure of the intelligent traffic signal control mechanism is presented in Figure 2. The specific parameters are defined as follows.

TABLE 1. Descriptions of symbols used in this paper.

Symbol	Definition
RSU	Roadside unit node
OBU	Onboard unit node
TD	Traffic department
ID_{OBU_i}	OBU_i real identity
FID_{OBU_i}	OBU_i pseudonym
FID_{RSU_i}	RSU_i pseudonym
C_{OBU_i}	OBU_i encryption information
M_{OBU_i}	Traffic message for OBU_i
M'_{OBU_i}	Service request message for OBU_i
M''_{OBU_j}	Reply message for OBU_j
$sign$	Signature of the message
T	Timestamp
Y_{RSU_i}	Group public key for RSU_i
Y_{OBU_i}	Public key for OBU_i
y_{RSU_i}	Private key for RSU_i
sp_{OBU_i}	Group member OBU_i private key

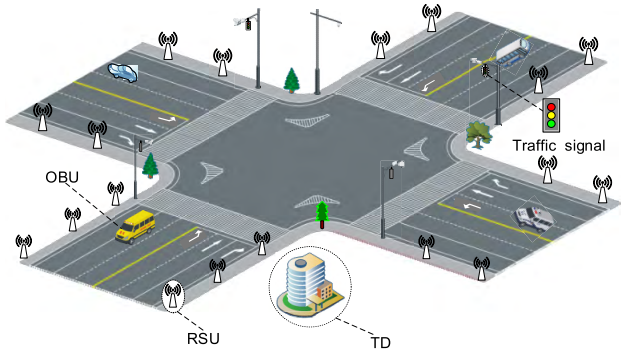

FIGURE 1. Structure of the system model.

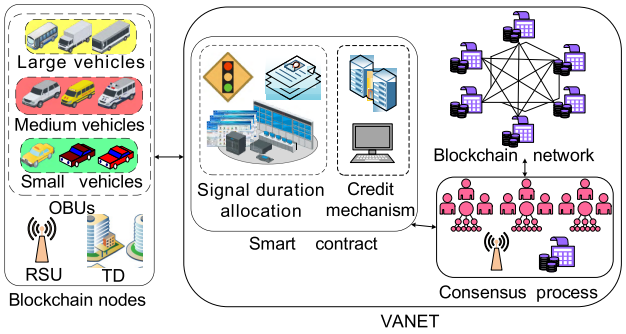

FIGURE 2. Traffic signal control mechanism structure.

- Blockchain node. Blockchain nodes $(f_1, f_2, \cdots, f_j)$ are consists of consortium blockchain F, which include the traffic department (TD), roadside units ($RSUs$), and onboard units ($OBUs$). The purpose of pseudonym is only visible to the nodes in the chain and cannot be tracked by an attacker.
- RSU node. In order to ensure efficient communication when the traffic is congested, the RSU is fixed in place on both sides of the road every kilometer or less. According to the network scale and the number of nodes, a certain RSU is preselected as the distributed accounting node for the consortium blockchain. A series of $RSUs$ can be expressed as:

$$RSU = \{RSU_1, RSU_2, \cdots, RSU_j\},\ RSU_i \in RSU, RSU \subset F$$

An OBU passes through the jurisdiction of a RSU and communicates with the $RSUs$ in short range. The RSU acts as the GM and mainly responsible for group members registering, receiving, or forwarding the ciphertext.

- OBU node. Each vehicle is equipped with an onboard unit, which enables to wireless communicate with other vicinity $OBUs$ and $RSUs$. A series of vehicle units can be expressed as:

$$\mathrm{OBU} = \{\mathrm{OBU}_1, \mathrm{OBU}_2, \cdots, \mathrm{OBU}_j\},\quad \mathrm{OBU}_i \in OBU, OBU \subset F$$

After a vehicle is produced, the OBU sends out a request to join the group, and the RSU that acts as the GM verifies OBU legal identity, then enters the scope of group, and becomes a node of consortium blockchain. Illegal OBU nodes cannot participate in information exchange.

- The traffic department (TD).TD decrypts the road condition information recorded in the blockchain, and mobilize the ACP to preprocess the information via smart contracts, then the duration of the green light allocation is computed. Dynamic signal light regulation is achieved via virtual and real interactions, and by parallel tuning of the physical and artificial traffic signal systems. TD gives honest vehicle a credit reward for providing accurate road condition information, whereas the credit value of a malicious vehicle that provides false information will be reduced. TD also serves as a GD and exposes the real identity of the malicious vehicle and broadcasts it over the whole network.

C. SCHEME FLOW

The OBU transmits a ciphertext (such as the road congestion conditions) to the RSU, the RSU records the ciphertext to the block and verifies it by pre-selected bookkeeping nodes. The block is connected to the consortium blockchain after successful verification. TD decrypts the ciphertext in the blockchain to obtain the plaintext information. ACP is employed to process the data information and adjust the green light duration in real time according to the traffic flow and vehicle type.

Figure 3 shows a flow chart to illustrate the scheme. When the road is severely congested, a longer time is allocated to the green light to reduce the number of vehicle stops and starts. When the traffic flow is small and the road is unimpeded, a green light is assigned a shorter duration to shorten the waiting time for vehicles. If the traffic volume is particularly small or there are even no vehicles, the green light duration allocation for the current road is skipped to effectively reduce

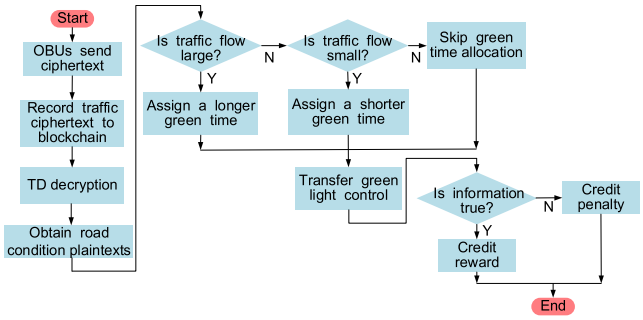

FIGURE 3. Traffic signal control flow.

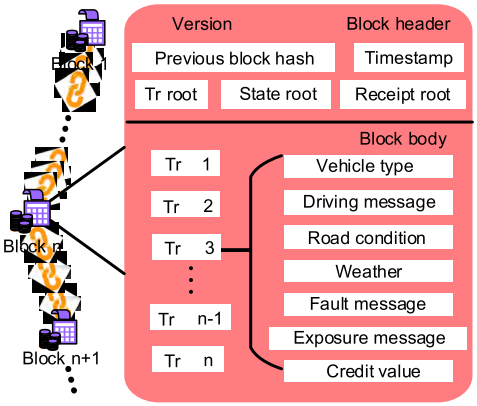

FIGURE 4. Traffic signal control mechanism block.

the number of starts and stops for vehicles, or vehicles waiting time. *TD* rewards *OBUs* that send correct road condition messages but punishes those that send false road condition messages.

D. TRAFFIC SIGNAL CONTROL MECHANISM BLOCK STRUCTURE

A blockchain comprises blocks and chain structures. Each block has a block head and block body. The chain structure mainly uses a cryptographic Hash algorithm to process the block header and form the block header's Hash. The block header stores the Hash value of the previous block and the block body stores relevant information.

In this paper, we employ an Ethereum blockchain which each block header contains a state root, transaction (Tr) root, and receipt root [33]. As shown in Figure 4, the state tree records the overall state after a traffic signal is controlled, including increases or decreases in an *OBU*'s credit value after each information interaction, the state of the traffic signal, and whether the node is a group member. The transaction root represents all of the historical interactive information in the block, which mainly comprises the road condition, vehicle type, and other data sent by the *OBU*. The receipt root represents the receipt for each data interaction, i.e., the result of each interaction, such as the allocation of green light time.

The block body comprises Hash values for the vehicle interaction messages, such as the vehicle type, driving message, road condition, weather, fault message, exposure message, and credit value.

According to the number of passengers and height of the vehicle, the vehicles are divided into three categories: small vehicles such as cars and taxis, medium-sized vehicles such as ambulances and commercial vehicles, and large vehicles such as trucks and buses. Driving message, road condition, weather, fault message, exposure message are described in the importance of information I. According to the authenticity of the information, the *TD* gives a credit reward or punishment to the vehicle sending the information. The credit value is used as a basis for the priority response or no response when the *OBU* sends an information request in the future.

The initial credit value for a vehicle is zero and the credit function is used to calculate the credit value as following formula:

$$C_{v_i}(m+1) = C_{v_i}(m) + R_{v_{i,m}}(I,N,L) + P_{v_{i,m}}(I,N,L) \quad (5)$$

where $C_{Vi}(m)$ represents the credit value of vehicle i after sending or receiving information m times, $R_{V_{i,m}}(I,N,L)$ denotes the credit value obtained by vehicle i after transmitting or receiving information for the m_{th} time, and $P_{V_{i,m}}(I,N,L)$ expresses the credit penalty value obtained by transmitting or receiving the message for the m_{th} time. The importance of information of I is ranked according to its urgency from low to high as follows.

a) $I = 1$, driving message, such as vehicle driving speed, current position.
b) $I = 2$, road conditions, including road congestion, road maintenance, damage.
c) $I = 3$, weather conditions such as heavy rain, heavy snow, and foggy weather with low visibility.
d) $I = 4$, traffic accidents such as car accidents and drunk driving.
e) $I = 5$, failures caused while driving a vehicle such as a steering wheel failure and puncture.
f) $I = 6$, reporting malicious vehicles that send false or forged messages.

The vehicle credit value obtained using equation (5) is closely related to credit reward function $R_{V_{i,m}}(I,N,L)$ in equation (6) and the credit penalty function $P_{V_{i,m}}(I,N,L)$ in equation (7). The credit reward or credit penalty depends on the importance of the information I, the order N in which the messages are sent (set $N = 1$ for the first vehicle that sent the message), and the Euclidean distance between the vehicle transmitting the message and the vehicle receiving the information is L (in meters):

$$R_{V_{i,m}}(I,N,L) = \frac{bI}{N^2 L} \quad (6)$$

$$P_{V_{i,m}}(I,N,L) = -\frac{cI}{N^2 L} \quad (7)$$

where b is the credit reward coefficient, c is the credit penalty coefficient, and c is much larger than b. According to equations (6) and (7). The faster the vehicle responds to requests from other vehicles and the more authentic and important the information it sending, the more credit rewards it receives. When the vehicle issues a request for information about the

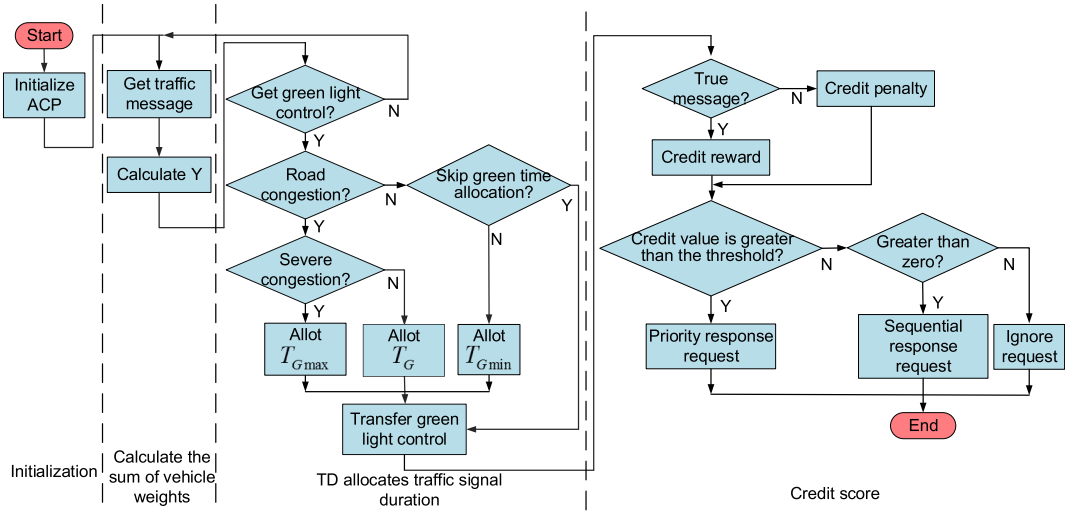

FIGURE 5. Traffic signal control smart contract.

road conditions, the information possessed by the adjacent vehicle meets its needs and responds quickly to the requesting vehicle to effectively reduce the information transmission delay and obtain a greater credit reward. The credit penalty coefficient is set much larger than the credit reward coefficient, so the vehicle is punished severely for sending false or forged information.

If the *TD* decrypts correct road conditions information from the blockchain, then it rewards the honest vehicle according to formula (6), where I is 2, N is selected according to the message sending sequence, and L is set as 1. If the *TD* obtains false road conditions information, then the malicious vehicle is given a credit penalty according to formula (7), where the specific values of I, N, and L are the same as those above.

If the vehicle sends an accurate message and the message is more important, then the vehicle receives more credit rewards, and vice versa. While driving on the road, the vehicle discloses other vehicles that send false information. A credit reward is given for correct exposure to improve the credit value, and a credit punishment is imposed for incorrect exposure to reduce the credit value.

IV. INTELLIGENT TRAFFIC SIGNAL CONTROL VIA SMART CONTRACTS

The blockchain reinterprets smart contracts where the original smart contract refers to a protocol defined in digital form. A smart contract [34] is a programmable code embedded in a blockchain, which can automatically enforce the treaty provisions. The contract contains several preset states, state transition functions, conversion rules, trigger conditions for executing contracts, interaction methods, and other features. A blockchain detects the status of a smart contract in real time. When the trigger condition is met, the smart contract is executed automatically. In our method, a smart contract for intelligent traffic signal control dynamically allocates the green light duration for the traffic signal according to the vehicle's weight. The allocated green light time range is $T_{G\max} \leq T_G \leq T_{G\min}$, where $T_{G\min}$ and $T_{G\max}$ indicate the minimum green time and maximum green time, respectively, to prevent other road sections from becoming congested due to unreasonable green light time allocation. Figure 5 shows the signal control process based on smart contracts.

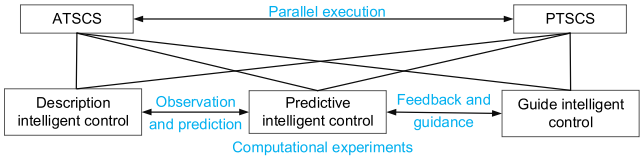

FIGURE 6. ACP architecture diagrams.

- **Initialization**

An artificial traffic signal control system (ATSCS), corresponding to a physical traffic signal control system (PTSCS), was established using ACP. The duration control for the ATSCS is fed back to the PTSCS in order to allocate an appropriate passing time for the green light. The ACP architecture employed by our method is present in Figure 6. The system has completed learning and training by default. A road condition message obtained by *TD* can be preprocessed without learning and training.

- **Vehicle weight calculation**

Different types of vehicles have different body lengths. If only the number of vehicles is considered, large errors will be incurred in terms of the allocation of green time. Thus, we divide the vehicles into small, medium, and large types with weights of $x_1, x_2, x_3 (0 < x_1 < x_2 < x_3 < 1)$, respectively.

Small vehicles have standard weights. The numbers of small, medium, and large vehicles in the same lane at the same intersection are calculated as n_1, n_2, n_3, respectively. The summed weight of all vehicles in the same lane at the same intersection that affect the green time distribution

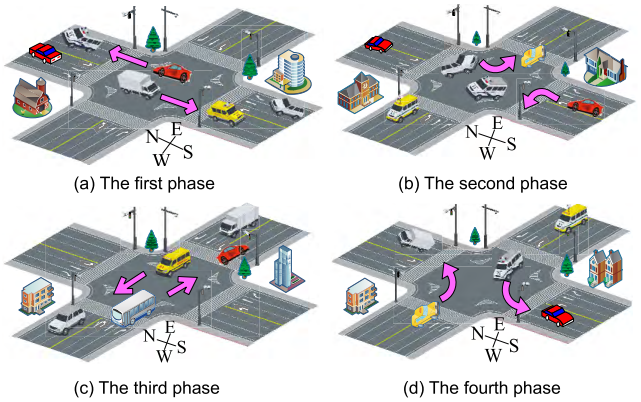

FIGURE 7. Phase distribution.

is computed. Right-turning traffic does not affect the normal driving of cars in other directions, so our proposed signal control mechanism ignores the effect of right-turning traffic on the allocation of the green light duration. The phase distribution is shown in Figure 7. In addition to right-turning traffic, there is only traffic traveling south and north straight ahead in the first phase, and left-turning traffic heading south and north in the second phase. There is only traffic heading straight east and west in the third phase, and left-turn traffic heading east and west in the fourth phase.

We describe the control of the green light duration in one phase distribution and the green light duration allocations in the other phase distributions are similar. We assume that the total number of vehicles in the current phase distribution is $n(n = n_1 + n_2 + n_3, exceptright - turn\ traffic)$. Let each vehicle's weight be X_{OBU_i} (all greater than 0). The cumulative weight of all vehicles that affect the green light time allocation is $Y(0 \le Y \le 1)$. Then, we have:

$$\mathrm{Y}=\sum_{\mathrm{i}=1}^{n} X_{OBU_i}/\mathrm{n} = \frac{n_1x_1 + n_2x_2 + n_3x_3}{n} \tag{8}$$

where the value of X_{OBU_i} is given by equation (9):

$$X_{OBU_i} = \begin{cases} x_1, & small - vehicle \\ x_2, & medium - vehicle \\ x_3, & l\arg e - vehicle \end{cases} \tag{9}$$

- **Adaptive traffic signal control**

The waiting times and the numbers of starts and stops for vehicles at traffic intersections are important factors that affect the vehicle traffic volume. When vehicles pass the traffic lights at an intersection, the green light duration for the traffic signal is allocated dynamically to reduce the waiting time and the number of starts and stops for vehicles. The green light is allocated a short period of time in case of sparse traffic condition, whereas the green light is allocated a long time in case of dense traffic condition. When the traffic is very low, the allocation of the green light duration is skipped and the green light control is transferred to the next phase to effectively reduce the number of starts and stops as well as the waiting time for vehicles. If the green time allocation is skipped, the vehicles moving in some directions remain unable to pass the intersection. We set the green light skipping threshold to α, let continuously skip the green light times be k. when k is greater than α, *TD* assigns the minimum green duration $T_{G\min}$ to the phase where is skipped the green time allocation multiple times.

(1) If the traffic flow is sparse, the minimum green time $T_{G\min}$ is allocated for the intersection. The assigned green light duration can be expressed

$$T_G = T_{G\min}, \quad Y \le \beta \tag{10}$$

where the cumulative weight is Y, the threshold for the total weight of all vehicles in the same lane at the same intersection is β when the traffic flow is sparse.

(2) If the traffic flow is dense, the assigned green light duration can be expressed

$$T_G = T_G + \left\lceil e^Y - \beta \right\rceil, \quad \beta < Y \le \theta \tag{11}$$

where $\lceil \bullet \rceil$ is a ceiling function, the threshold of the total weight of all vehicles in the same lane at the same intersection is θ when the traffic is dense.

(3) If the traffic flow is severe congestion, the maximum green time $T_{G\max}$ is allocated for the intersection. The assigned green light duration can be expressed

$$T_G = T_{G\max}, \quad Y > \theta \tag{12}$$

where the threshold of the total weight of all vehicles in the same lane at the same intersection is θ when the traffic is dense.

So the assigned green light duration can be expressed by equation (13)

$$T_G = \begin{cases} T_{G\min}, & Y \le \beta traffic\ is\ sparse \\ T_G + \left\lceil e^Y - \beta \right\rceil, & \beta < Y \le \theta trafficisdense \\ T_{G\max}, & Y > \theta traffic\ is\ severe\ congestion \end{cases}. \tag{13}$$

- **Credit score**

After the duration of green light was allocated, *TD* rewards the vehicles with a credit value for transmitting true and accurate road condition messages, but deducts the credit value for malicious vehicles that send false and forged messages. A vehicle can pay credit values to enjoy services such as real-time road condition information. Priority response to service requests for vehicles with high credit values. Road condition messages and service requests sent by vehicles are ignored when the credit value is less than 0.

V. IMPLEMENTATION OF INTELLIGENT TRAFFIC SIGNAL CONTROL MECHANISM

As mentioned earlier, the road condition information interactions are divided into two cases. First, the *RSU* records information such as ciphertext for the road condition messages sent by an *OBU* to the blockchain. After *TD* decrypts

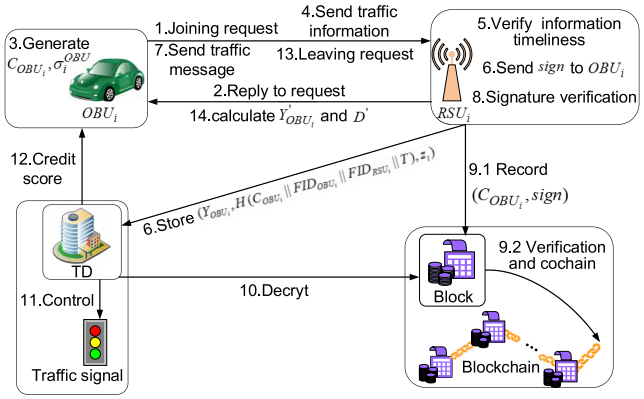

FIGURE 8. Traffic signal control process diagram.

the ciphertext to obtain the plaintext, the smart contract is executed automatically. The allocation of the green light duration is computed according to the plaintext for the road conditions. The vehicle weights are summed and the ACP is applied to dynamically adjust the duration of the green light. An honest *OBU* is given a credit reward and a malicious *OBU* receives a credit penalty. Second, the *OBU* enjoys a service such as real-time road conditions information by paying the credit value. The *OBU* can make a request to obtain the real-time road conditions from another *OBU* in a certain section. If the information sent by the responding vehicle is true and reliable, then the smart contract sends the credit value from the vehicle making the service request to the responding vehicle as a credit reward. If the information sent by the vehicle is forged, the smart contract deducts the credit value from the responding vehicle as a penalty.

A. TRAFFIC SIGNAL CONTROL

RSU_i is a *GM* responsible for group members joining and leaving the group. *TD* is a *GD* that exposes the true identity of a malicious vehicle after it fails to pass signature verification or sends forged message, and then broadcasts malicious vehicles to the whole network. RSU_i approves OBU_i to join the group after OBU_i becomes a group member. When OBU_i leaves the group, RSU_i revokes the group member OBU_i. The signal light regulation process is shown in Figure 8. The detailed process employed for controlling the duration of the traffic signal is as follows.

Step 1: OBU_i requests to join the group by sending a join request $Req_{join}||FID_{OBU_i}||FID_{RSU_i}$ to RSU_i.

Step 2: First, RSU_i verifies the identity of OBU_i. If OBU_i is a legal *OBU*, then OBU_i is allowed to join the group and become a group member. $Reply_{accept}||FID_{RSU_i}||FID_{OBU_i}$ is forwarded to OBU_i. Otherwise, the agreement is terminated. RSU_i uses the public key of group members to calculate $D \equiv Y_{OBU_1}Q_1Q_1^{'} + Y_{OBU_2}Q_2Q_2^{'} + \cdots + Y_{OBU_s}Q_sQ_s^{'} (\mathrm{mod}\, Q)$ according to the Chinese remainder theorem, where $Q_iQ_i^{'} \equiv 1(\mathrm{mod} q_i)$, $i = 1, 2, \cdots, s$, and D is published.

Step 3: OBU_i encrypts the road conditions information M_{OBU_i} using the encryption parameter (g_{TS}, λ_{TS}) for TS, including the vehicle location, whether the road is congested, and the vehicle type. A road conditions ciphertext is obtained

$$C_{OBU_i} = E\left(M_{OBU_i}\right) = (c, d) = (g_{TS}^k \bmod q, \lambda_{TS}^k M_{OBU_i} \bmod (q-1)).$$

OBU_i uses the group members private key sp_{OBU_i} to calculate $\sigma_i^{OBU} = sp_{OBU_i}H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||T)$.

Step 4: OBU_i sends a road conditions message $C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||T||\sigma_i^{OBU}$ to RSU_i, where T is the current timestamp, which can be used to prevent replay attacks.

Step 5: After receiving the message, RSU_i determines whether OBU_i is a group member according to FID_{OBU_i}. If it is not a group member, RSU_i refuses to receive the message. If it is a group member, the real-time nature of the message is verified by determining whether the inequality $|T_{RSU_i} - T| < \Delta t$ is satisfied, where T_{RSU_i} indicates when RSU_i received the message and Δt indicates the allowed delay. If the inequality is satisfied, go to 6; otherwise, the information is discarded and the agreement is terminated.

Step 6: RSU_i computes:

$$\sigma_i^{RSU} = y_{RSU_i}H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||T).$$

RSU_i randomly selects $z_i \in Z_p^*$ to calculate $Z_i = z_iP$, $w_i = z_iH\left(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||T\right)$,$\sigma_i = \sigma_i^{RSU} + \sigma_i^{OBU} + w_i$, and $S_{OBU_i} = Y_i^{OBU} + Y_{OBU_i} + Z_i$.$RSU_i$ sends $(Y_{OBU_i}, H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||T), z_i)$ to *TD*. *TD* saves it in the storage list, generates a signature $sign = (\sigma_i, S_i, q_i)$, and sends it to OBU_i.

Step 7: OBU_i transmits the road conditions message $C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||T||sign||Y_{OBU_i}$ to RSU_i.

Step 8: After receiving the message, RSU_i first verifies whether $Y_{OBU_i} = D(\mathrm{mod} q_i)$ is satisfied. If the equation is satisfied, RSU_i verifies whether the data have been tampered with or forged, that is, verifies whether

$$e(P, \sum_{i=1}^{n}\sigma_i) = e\left(Y_{RSU_i} + \sum_{i=1}^{n}S_{OBU_i}, \sum_{i=1}^{n}H(C_{OBU_i}\|FID_{OBU_i}||FID_{RSU_i}||T)\right)$$

is equal. If they are equal, the verification step is successful; otherwise, the verification fails and the agreement is terminated.

Step 9: If the verification process in step 8 is successful, $(C_{OBU_i}, sign)$ is recorded in a block by RSU_i and the validity of the block is verified using the AlgoRand consensus algorithm. After successful verification, the block is connected to the blockchain.

Step 10: TD decrypts the road ciphertext stored in the blockchain using the decryption parameters x_{TD} and the decryption algorithm to obtain the plaintext $M_{OBU_i} = D(C_{OBU_i}) = d(c^{x_{TD}})^{-1} \bmod q$.

Step 11: After *TD* decrypts the road conditions ciphertext, the smart contract employs the ACP to calculate Y utilizing

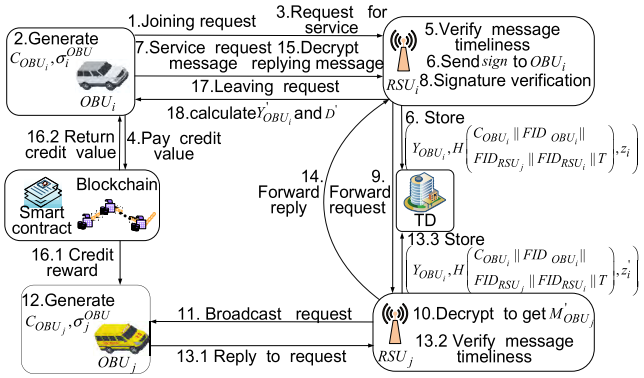

FIGURE 9. Vehicle communication process.

the plaintext. *TD* applies the ACP to perform parallel control for the green light duration of the traffic signal.

Step 12: After the traffic signal is controlled, *TD* uses the smart contract to give a credibility reward to the honest *OBUs* and a credit penalty to the malicious *OBUs* that send false information. $ID_{OBU_i} = FID_{OBU_i} \oplus H(Y_{OBU_i} + d_i)$ is calculate to obtain the real identity of the vehicle and *TD* broadcasts ID_{OBU_i} to the whole network in order to expose the malicious vehicle.

Step 13: OBU_i sends a leave request $Req_{left}||FID_{OBU_i}||FID_{RSU_i}$ to RSU_i when leaving the group.

Step 14: When RSU_i receives the request, Y_{OBU_i} is updated to a random prime number Y'_{OBU_i}. RSU_i recalculates $D' \equiv Y_{OBU_1}Q_1Q'_1 + \cdots + Y'_{OBU_i}Q_iQ'_i + \cdots + Y_{OBU_s}Q_sQ'_s (\mathrm{mod}\, Q)$, and publishes D' to revoke the group member OBU_i.

B. COMMUNICATION BETWEEN VEHICLES

OBU_i can obtain the real-time road conditions for a certain section, the weather conditions for the road ahead, and other services by using the credit value. OBU_i sends a service request to the *GM* in the group. OBU_i forwards the request to the corresponding RSU_j. RSU_j broadcasts the service request to the group. In the group, OBU_j can provide the service and sends a reply message to RSU_j. RSU_j transmits the reply message to RSU_i. RSU_i then sends a reply message to OBU_i and OBU_i obtains valid information based on the content of the reply message. If the information sent by OBU_j is accurate and reliable, then the smart contract deducts a credit value of OBU_i and pays OBU_j a reward for providing the service. By considering an *OBU* with knowledge of the road condition messages for a certain section as an example, the information exchange process between vehicles is shown in Figure 9, and this process is described in detail in the following.

Step 1: Joining a group to become a group member is the same as Steps 1∼2 in the traffic signal control process.

Step 2: OBU_i requires the road condition message for a certain road section and uses the encryption parameter $(g_{RSU_j}, \lambda_{RSU_j})$ from RSU_j to encrypt the service request information, including details of road congestion and traffic accidents. After encryption, a service request ciphertext is obtained $C_{OBU_i} = E\left(M'_{OBU_i}\right) = (c, d) = (g^k_{RSU_j} \bmod q, \lambda^k_{RSU_j} M'_{OBU_i} \bmod q)$. OBU_i uses the group member private key sp_{OBU_i} to calculate $\sigma_i^{OBU} = sp_{OBU_i} H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T)$.

Step 3: OBU_i sends a service request message

$$C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T||\sigma_i^{OBU}$$

to RSU_i, where T is the current timestamp, which can be used to prevent replay attacks.

Step 4: The vehicle unit OBU_i pays the credit value to the smart contract to prevent bogus requests. If OBU_i sends a false request, the smart contract will deduct the credit value from OBU_i. If OBU_i sends a real request, the smart contract will deduct a certain credit value from OBU_i to reward an honest response *OBU* and return the remaining credit value to OBU_i after the interaction ends.

Step 5: After receiving the message, RSU_i determines whether OBU_i is a group member according to FID_{OBU_i}. If it is not, RSU_i refuses to receive the message. If it is a group member, the real-time nature of the message is verified whether the inequality $|T_{RSU_i} - T| < \Delta t$ is satisfied, where T_{RSU_i} indicates when RSU_i received the message and Δt indicates the allowed delay. If the inequality is satisfied, go to Step 6; otherwise, the information is discarded and the agreement is terminated.

Step 6: RSU_i computers

$$\sigma_i^{RSU} = y_{RSU_i} H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T).$$

RSU_i randomly selects $z_i \in Z_p^*$ to calculate $Z_i = z_i P$, $w_i = z_i H\left(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T\right)$, $\sigma_i = \sigma_i^{RSU} + \sigma_i^{OBU} + w_i$, and $S_{OBU_i} = Y_i^{OBU} + Y_{OBU_i} + Z_i.RSU_i$ sends $(Y_{OBU_i}, H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T), z_i)$ to *TD*. *TD* saves it in the storage list, generates a signature $sign = (\sigma_i, S_i, q_i)$, and sends it to OBU_i.

Step 7: OBU_i transmits a service request message $C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T||sign||Y_{OBU_i}$ to RSU_i.

Step 8: After receiving the message, RSU_i first verifies whether $Y_{OBU_i} = D(\mathrm{mod} q_i)$ is satisfied. If the equation is satisfied, it verifies whether the data has been tampered with or forged, and whether

$$e(P, \sum_{i=1}^{n} \sigma_i) = e\left(Y_{RSU_i} + \sum_{i=1}^{n} S_{OBU_i}\ , \right.$$
$$\left. \sum_{i=1}^{n} H(C_{OBU_i}||FID_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T)\right)$$

is equal. If they are equal, the verification step is successful; otherwise, verification fails and the agreement is terminated.

Step 9: If the verification process in Step 8 is successful,RSU_i will transmit $C_{OBU_i}||FID_{RSU_i}||FID_{RSU_j}||T||sign$ to RSU_j.

Step 10: RSU_j uses the decryption parameters x_{RSU_j} and the decryption algorithm to obtain the plaintext $M'_{OBU_i} = D(C_{OBU_i}) = d\left(c^{x_{RSU_j}}\right)^{-1} \bmod q$.

Step 11: RSU_j broadcasts a request message to vehicles in the area.

Step 12: OBU_j responds to the request and encrypts the reply message using the encryption parameters $(g_{OBU_i}, \lambda_{OBU_i})$ for OBU_i, including the degree of road congestion and whether there is a traffic accident. The reply ciphertext $C_{OBU_j} = E\left(M''_{OBU_j}\right) = (c, d) = (g^k_{OBU_i} \bmod p, \lambda^k_{OBU_i} M''_{OBU_j} \bmod p)$ is obtained after encryption. OBU_j uses the group member private key sp_{OBU_j} to calculate $\sigma_j^{OBU} = sp_{OBU_j} H(C_{OBU_j}||FID_{RSU_j}||FID_{RSU_i}||FID_{OBU_i}||T)$.

Step 13: OBU_j sends $C_{OBU_j}||FID_{OBU_j}||FID_{RSU_j}||FID_{RSU_i}||T||\sigma_j^{OBU}$ to RSU_j. After the RSU receives the message, it verifies the timeliness, message signature, and signature verification of the message, which are similar processes to Steps 5∼8 so their descriptions are omitted.

Step 14: If the normal verification in Step 13 is successful, RSU_j sends a reply ciphertext $C_{OBU_i}||FID_{RSU_j}||FID_{RSU_i}||FID_{OBU_i}||T||sign$ to RSU_i.

Step 15: RSU_i forwards the reply ciphertext to OBU_i. OBU_i uses the decryption parameters x_{OBU_i} and the decryption algorithm to obtain the reply message $M''_{OBU_j} = D(C_{OBU_j}) = d\left(c^{x_{OBU_i}}\right)^{-1} \bmod q$.

Step 16: After the information interaction is complete, OBU_i evaluates and judges the authenticity and accuracy of the reply information received, and sends the assessment result and the FID_{OBU_j} to TD. A smart contract is triggered to deduct the credit value from OBU_i and a certain credit value is given to reward the honest response by OBU_j. The remaining credit value is returned to OBU_i. If a forged reply is sent by OBU_j, the smart contract deducts the corresponding credit value from OBU_j as a penalty. The TD calculates $ID_{OBU_j} = FID_{OBU_j} \oplus H(Y_{OBU_j})$ to obtain the real identity of the OBU_j that sends the false information, and broadcasts ID_{OBU_j} to the entire network to expose the malicious vehicle.

Step 17: OBU_i sends a leave request $Req_{left}||FID_{OBU_i}||FID_{RSU_i}$ to RSU_i when it wants to leave the group.

Step 18: When RSU_i receives the request, Y_{OBU_i} is updated to a random prime number Y'_{OBU_i}. RSU_i recalculates

$$D' \equiv Y_{OBU_1} Q_1 Q'_1 + \cdots + Y_{OBU_{i-1}} Q_{i-1} Q'_{i-1} + Y'_{OBU_i} Q_i Q'_i + Y_{OBU_{i+1}} Q_{i+1} Q'_{i+1} + \cdots + Y_{OBU_s} Q_s Q'_s (\bmod Q),$$

and publishes D' to revoke group membership OBU_i.

VI. SAFETY ANALYSIS AND PERFORMANCE EVALUATION

A. VALIDITY OF THE TRAFFIC SIGNAL CONTROL MECHANISM

The OBU transmits a road condition message, which the blockchain network processes in a distributed structure, to the RSU using a pseudonym identity. The RSU nodes preselected for bookkeeping record the data in a block and other RSU nodes verify the data. After other RSU nodes verify the validity of the message and the block, the block is connected to the current blockchain. TD triggers a smart contract according to the road conditions information and controls the duration of the signal light in real time via the ACP. TD gives the vehicle a reward for exposing the true identity of the malicious vehicle. In addition, the road condition information in this scheme is not affected by the weather and it has good stability. Table 2 compares the signal control mechanism based on the consortium blockchain with other signal regulation mechanisms, thereby demonstrating that our proposed traffic signal control mechanism is better than the other mechanisms and more suitable for regulating the traffic signal duration.

TABLE 2. Comparison of signal regulation mechanisms.

	Ref. [7]	Ref. [8]	Ref. [9]	Our scheme
Identity management	✓	✓		✓
Distributed structure			✓	✓
Credit mechanism				✓
Stability		✓	✓	✓
Blockchain based				✓
Non-repudiation	✓		✓	✓

B. SAFETY ANALYSIS

We analyzed the security of our proposed intelligent traffic signal control mechanism in terms of the encryption signature algorithm and consortium blockchain network.

1) TRAFFIC MESSAGE INTERACTION SAFETY

a: ELGAMAL ENCRYPTION

The security of the encryption algorithm used in our method is determined by the ElGamal discrete logarithm problem. Every time the ElGamal encryption algorithm encrypts a plaintext, it has to choose a random number. Therefore, the ciphertext depends on the plaintext and the chosen random number. For the same plaintext, the ciphertext generated at different times is different, and the randomness of encryption operation greatly improves the securith of message. Even if the interaction information between the RSU and OBU is intercepted by the attacker, the ElGamal encryption algorithm satisfies the semantic security and does not reveal any private message, thereby ensuring the confidentiality of the message interaction.

b: GROUP SIGNATURE

The OBU uses the private key to sign related information such as road conditions. After receiving the message, the RSU uses the group public key for verification. The security of the group signature used in our method is determined by the computational Diffie–Hellman problem, which guarantees that the attacker cannot forge a new signature by eavesdropping, thereby eliminating the possibility of data forgery attacks. The attacker cannot distinguish the signature without opening the signature, which ensures the irrelevance and anonymity of the signature. The TD can expose the true identity of the malicious OBU and this traceability ensures the security of VANETs. Chinese Remainder theorem guarantees that the

TABLE 3. Safety comparison.

	Ref. [35]	Ref. [36]	Ref. [37]	Our Scheme
Anonymity	✓	✓	✓	✓
Unforgeable		✓	✓	✓
Revocability		✓		✓
Collusion-resistance			✓	✓
Anti-man-in-the-middle attack				✓
Forward security				✓
Backward security				✓

newly joined group members cannot use the old group public key to verify the signature, and the signature of the group members leaving the group cannot be verified by the new group public key, thereby ensuring the forward and backward security.

The paper proposes BLS signature-based batch verification algorithm, which introduces the Chinese remainder theorem, to facilitate the rapid joining and revocation of group members. The batch verification algorithm based on BLS group signature, which improves the verification efficiency, as well as is a simple and effective signature method. The security of our scheme is compared with that of existing schemes [35]–[37], and the results are shown in Table 3.

Through analysis, it can be manifested that our scheme ensures anonymity, unforgeable, revocability, and at the same time solves the potential security risks of collusion attack, forward security, backward security and man-in-the-middle attack in the existing schemes. Our scheme has far-reaching significance for the highly dynamic VANETs in the field of traffic signal regulation.

2) CONSORTIUM BLOCKCHAIN NETWORK SAFETY

a: NODE COMMUNICATION AUTHORITY

The *OBU* and *RSU* use pseudonyms to register as legal nodes in the consortium blockchain. The legal nodes cannot perform data interactions even if they enter the blockchain network and they must be registered as group members in the *GM*. Messages sent by group members will be received and the signatures will be verified. Messages sent by malicious or non-member nodes will be rejected and signature verification will also fail. The communication authority of nodes ensures the security of the blockchain network and reduces the communication overheads.

b: NODE IDENTITY PRIVACY PROTECTION

During the information interaction process, a pseudonym *FID* that is unique to the *OBU* is used as an identity identifier to effectively avoid tracking by attackers. Regardless of the communication between *OBUs*, or the communication between the *OBU* and the *RSU*, they do not know each other's real identity *ID*. If a *OBU* sends a forged message or the signature verification process fails, *TD* opens the signature to reveal the real identity *ID* of the *OBU*. Even if the attacker knows the true identity of the node, he still cannot obtain the location, vehicle type, credit value, and other information for the node.

c: AVOIDANCE OF BOGUS REQUESTS AND MALICIOUS RESPONSES

During the interactions between vehicles, in order to avoid bogus requests and ensure that the *OBU* has the ability to pay credit values, it is necessary to pay a certain credit value as collateral to the smart contract address when sending the service request. If a *OBU* sends a bogus request, the smart contract automatically deducts all the credit value for the payment. In order to avoid the *OBU* maliciously responding to a service request and increasing the network overheads by causing congestion, when the *OBU* sends the fake message, the smart contract will deduct its credit value as a penalty. After the vehicle information interaction is complete, the smart contract automatically deducts the credit value for the service from the requesting node and pays it to the responding node. The remaining credit value is returned to the service requesting node. This credit mechanism is employed to provide a credible communication environment for *OBUs* and to enhance the credibility of vehicles.

d: MESSAGE TAMPERING PREVENTION

The consortium blockchain uses a Hash algorithm to protect the integrity of the information recorded in a block that is connected by a chain structure. If a block is changed, each subsequent block will be changed as well as the data in the blockchain. It is more difficult to tamper with the data when there are more blocks. Thus, it is almost impossible to change the data in a certain block or blockchain.

C. PERFORMANCE EVALUTION

In the performance evaluation, we mainly analyzed the communication overheads and computational overheads for the traffic signal control mechanism.

1) COMMUNICATION OVERHEADS

The communication overheads for the proposed traffic signal control mechanism include the communication overheads of the *OBU* and *RSU*, and the overheads between *OBUs*.

During the regulation of the traffic signal, OBU_i sends a request to join the group to RSU_i. The road conditions information signed by OBU_i is sent to RSU_i. OBU_i transmits the road conditions information with a multi-signature to RSU_i. OBU_i unicasts the request to leave the group to RSU_i. Therefore, the communication overheads for OBU_i comprises four unicasts and zero broadcasts. RSU_i unicasts the traffic information with its own signature to OBU_i. When OBU_i joins the group, RSU_i calculates D and broadcasts it to the entire network. When OBU_i leaves the group, RSU_i calculates D' and broadcasts it to the entire network. Thus, the communication overheads for RSU_i are one unicast and two broadcasts. *TD* uses a smart contract to update the credit value in real time for the credit score. When OBU_i transmits false road conditions information, the real identity *ID* of

TABLE 4. Communication overheads for the information interaction process.

Process	Node	Unicast	Broadcast
Traffic signal control	OBU_i	4	0
	RSU_i	1	2
	TD	1	1/0
Communication between vehicles	OBU_i	5	0
	RSU_i	3	2
	RSU_j	1	1
	OBU_j	1	0
	TD	2	2/1/0

TABLE 5. Computational costs of different operations.

Symbol	Definition	Computation cost (ms)
T_e	Time cost of exponential operation	1
T_h	Time cost of Hash operation	0.09
T_m	Time cost of multiplication operation	0.39
T_p	Time cost of bilinear pairing operation	3.21
T_{ECC_m}	Time cost of multiplication in elliptic curve operation $\left(1T_{ECC\_m} = 29T_m\right)$	11.31

OBU_i is broadcast to the whole network; otherwise, no broadcast is required. Thus, the communication overheads for TD are one unicast and 1/0 (send false information/send accurate information) broadcast. The communication overheads between vehicles follows similarly, so no repeated explanation. Table 4 summarizes the communication overheads for the information interaction process.

2) COMPUTATIONAL OVERHEADS

The computational cost of the proposed scheme comprises the computational overheads of the encryption algorithm, signature algorithm, single signature verification, and batch verification in the traffic signal control process. The computational cost of communication between vehicles is the same as that for traffic signal control so the calculation is omitted.

The computational overheads of the traffic signal control process mainly comprises the exponential operation T_e, Hash operation T_h, multiplication operation T_m, and bilinear pairing operation T_p. The computational cost of addition is relatively smaller than these operations, so it is omitted. Experiments were performed with the Intel i5 processor, clocked at 3.0 GHz. Table 5 lists the specific values for the different computational overheads.

Table 6 compares the computational overheads of different encryption algorithms with our method. Figure 10 compares the computational costs of different encryption algorithms, which demonstrates that our encryption algorithm is efficient.

1) He *et al.* (Ref. [38]) used Paillier additive homomorphic encryption to satisfy the semantic security and the computational cost was small. In our method, we employ ElGamal multiplicative homomorphic encryption to satisfy the semantic security, but also to directly operate the ciphertext, reduce the number of encryption and decryption operations, and to reduce the computational costs.
2) Ferray *et al.* (Ref. [39]) used proxy re-encryption to re-encrypt the signed ciphertext by bilinear pairing, thereby increasing the computational overheads.
3) He *et al.* (Ref. [40]) applied an attribute-based encryption algorithm and the computational cost increased in a linear manner with the number of attributes, where the minimum computational cost was 6 ms.

TABLE 6. Comparison of the computational overheads of encryption algorithms.

Scheme	Year	Computation overheads	Cost (ms)
Ref [38]	2018	$4T_e + 3T_m$	5.17
Ref [39]	2017	$2T_p + 5T_m$	8.37
Ref [40]	2017	$(3+3k)T_e$, where $k \geq 1$ and an integer is taken	6 ($k=1$,minimum overheads)
Our scheme		$4T_e + 2T_m$	4.78

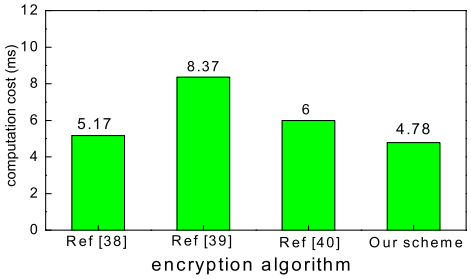

FIGURE 10. Comparison of the computational costs of various encryption algorithm.

TABLE 7. Comparison of the computational overheads for the signature and verification processes.

Scheme	Year	Signature overheads	Cost (ms)	Verification cost	Cost (ms)
VSS [41]	2018	$4T_e + 3T_m$	4.39	$3T_p + T_m + T_e$	11.02
MI [42]	2018	$4T_{ECC\_m} + 2T_h$	46.59	$2T_{ECC\_m} + T_h$	22.71
EECB [43]	2017	$6T_m + 2T_h$	2.52	$2T_p + 2T_m + T_h$	7.29
Our scheme		$6T_m + 3T_h$	2.61	$2T_p + T_h$	6.51

Table 7 compares the computation overheads of our signature algorithm and verification with the VSS [41], MI [42], and EECB [43] methods. Comparison of the computational overheads for batch verification is shown in Table 8.

a) VSS [41] employs a third-party arbitration center to verify signatures, which increases the number of bilinear pairing operations and the computational overheads.
b) MI [42] uses a group signature based on elliptic curves and the multiplication operation for the elliptic curves requires a long time, thereby greatly increasing the

TABLE 8. Comparison of the computational overheads for batch verification.

Scheme	Year	Batch verification overheads	Cost (ms)
VSS [41]	2018	$3T_p + nT_m + T_e$	$0.39n + 10.63$
MI [42]	2018	$2T_{ECC\_m} + nT_h$	$0.09n + 22.62$
EECB [43]	2017	$2T_p + (n+1)T_m + nT_h$	$0.48n + 6.81$
Our scheme		$2T_p + nT_h$	$0.09n + 6.42$

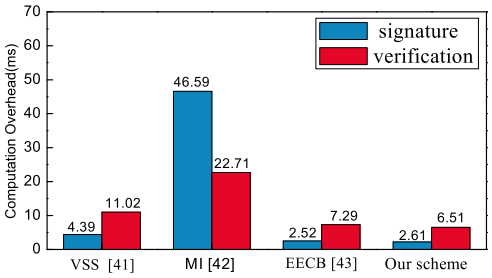

FIGURE 11. Comparison of the computational overheads for signature and verification.

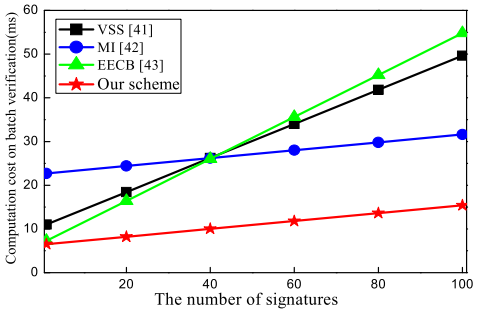

FIGURE 12. Comparison of the computational overheads for batch verification.

computational costs of the signature and verification processes.

c) EECB [43] uses pseudonym signature and verification operations where tokens are presented to PKG (Private Key Generator) in order to obtain pseudonyms. Thus, the process employed for obtaining pseudonyms is complicated so the computational overheads are excessive.

Figure 11 compares the computational overheads for the signature and verification processes. Figure 12 compares the computational overheads for batch verification. These figures show that the signature algorithm used in our method is more effective than other schemes in terms of the computational overheads.

VII. CONCLUSION

An adaptive traffic signal control mechanism is proposed based on a consortium blockchain, which can intelligently switch the traffic lights, quickly allocate the green lights duration time, and ensure the safety of the road traffic. ElGamal encryption and group signature algorithms have guaranteed the communication security and the privacy of the *OBU*'s identity. The proposed method can revoke the membership in the group and track the true identity of malicious *OBUs*. Performance evaluations demonstrate that the encryption, signature, verification, and batch verification algorithms are better than other algorithms, and their computational costs are lower, thereby demonstrating the effectiveness of our scheme. Smart contracts are used to allow *TD* to control the signal duration to coordinate the optimization of signal management and decision making via the ACP. The credit mechanism effectively prevents bogus requests and malicious responses from vehicles, as well as improving the credibility of vehicles and providing a trusted communication environment for VANETs. The feasibility and safety performance of traffic signal control via smart contracts are verified, this design can be widely used in intelligent traffic optimization control.

REFERENCES

[1] D. Y. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, Mar. 2016.

[2] Y. Ren, Y. Wang, G. Yu, H. Liu, and L. Xiao, "An adaptive signal control scheme to prevent intersection traffic blockage," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1519–1528, Jun. 2017.

[3] C.-H. Wan and M.-C. Hwang, "Value-based deep reinforcement learning for adaptive isolated intersection signal control," *IET Intell. Transp. Syst.*, vol. 12, no. 9, pp. 1005–1010, 2018.

[4] S. Chen and D. J. Sun, "An improved adaptive signal control method for isolated signalized intersection based on dynamic programming," *IEEE Intell. Transp. Syst. Mag.*, vol. 8, no. 4, pp. 4–14, Oct. 2016.

[5] H. J. Jeon, J. Lee, and K. Sohn, "Artificial intelligence for traffic signal control based solely on video images," *J. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 433–445, 2018.

[6] D. F. Ma, X. Luo, S. Jin, W. Guo, and D. Wang, "Estimating maximum queue length for traffic lane groups using travel times from video-imaging data," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 3, pp. 123–124, Jun. 2018.

[7] M. L. Yang, Y. M. Bie, and Y. L. Pei. (2018). *A Traffic Signal Control Algorithm for an Oversaturated Isolanted Intersection Based on Video Detection Data*. [Online]. Available: https://ascelibrary.org/doi/10.1061/9780784479292.188

[8] L. Wu, L. Nie, B.-Y. Liu, N. Wu, Y.-F. Zou, and L.-Y. Ye, "An intelligent traffic signal control method in VANET," *Chin. J. Comput.*, vol. 39, no. 6, pp. 1105–1119, Jun. 2016.

[9] W. R. Liu, G. Qin, Y. He, and F. Jiang, "Distributed cooperative reinforcement learning-based traffic signal control that integrates V2X networks' dynamic clustering," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 8667–8681, Oct. 2017.

[10] E. Shaghaghi, M. Reza, R. M. Noor, H. Yeo, and J. J. Jung, "Adaptive green traffic signal controlling using vehicular communication," *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 3, pp. 373–393, Feb. 2017.

[11] Y. Xie, W. H. Ho, and E. R. Magsino, "The modeling and cross-layer optimization of 802.11p VANET unicast," *IEEE Access*, vol. 6, pp. 171–186, 2018.

[12] V. Sucasas, G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems," *Comput. Secur.*, vol. 60, pp. 193–205, Jul. 2016.

[13] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.

[14] T. Limbasiya and D. Das, "Secure message confirmation scheme based on batch verification in vehicular cloud computing," *Phys. Commun.*, vol. 34, pp. 310–320, Jun. 2019.

[15] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8647–8655, Sep. 2018.

[16] L. Li, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[17] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 2169–3536, 2018.
[18] L. C. Cheng, "SCTSC: A Semicentralized Traffic Signal Control Mode with Attribute-Based Blockchain in IoVs," *IEEE Trans. Comput. Social Syst.*, to be published. doi: 10.1109/TCSS.2019.2904633.
[19] T. G. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.
[20] X. L. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for Internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45061–45072, 2019.
[21] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in VANET," in *Proc. IEEE 3rd Int. Conf. Comput., Commun. Secur. (ICCCS)*, Oct. 2018, pp. 161–166.
[22] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[23] 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.
[24] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. Symp. Operating Syst. Princ.*, Oct. 2017, pp. 51–68.
[25] X. Liu, S. Tang, Y. Lin, Z. Li, and Z. Chen, "ACP-based management and control for urban passenger transportation hubs," *IEEE Intell. Syst.*, vol. 32, no. 6, pp. 58–66, Dec. 2017.
[26] F. Zhu, Z. Li, S. Chen, and G. Xiong, "Parallel transportation management and control system and its applications in building smart cities," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 6, pp. 1576–1585, Jun. 2016.
[27] F. C. Guo, Y. Mu, W. Susilo, H. Hsing, D. S. Wong, and V. Varadharajan, "Optimized identity-based encryption from bilinear pairing for lightweight devices," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 2, pp. 211–220, Mar. 2017.
[28] H.-T. Wu and C.-W. Tsai, "Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 65–71, Jul. 2018. doi: 10.1109/mce.2018.2816306.
[29] J. Wang, Y. Han, and X. Yang, "An efficient location privacy protection scheme based on the chinese remainder theorem," *Tsinghua Sci. Technol.*, vol. 21, no. 3, pp. 260–269, Jun. 2016.
[30] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12601–12617, 2017.
[31] C. Esposito, A. Castiglione, F. Palmieri, and A. D. Santis, "Integrity for an event notification within the industrial Internet of Things by using group signatures," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3669–3678, Jan. 2018.
[32] C. Hefeng, M. Wenping, Z. Chengli, and S. Changxia, "Short group signatures with efficient concurrent join," *China Commun.*, vol. 11, no. 11, pp. 90–99, Nov. 2014.
[33] X. Zhang and M. Fan, "Blockchain-based secure equipment diagnosis mechanism of smart grid," *IEEE Access*, vol. 6, pp. 66165–66177, 2018.
[34] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[35] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.
[36] 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.
[37] Y. Liu, Z. He, S. Zhao, and L. Wang, "An efficient anonymous authentication protocol using batch operations for VANETs," *Multimedia Tools Appl.*, vol. 75, no. 24, pp. 17689–17709, Dec. 2016.
[38] Y. He, J. Ni, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving partner selection for ride-sharing services," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5994–6005, Jul. 2018.
[39] M. A. Ferrag and A. Ahmim, "ESSPR: An efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," *Telecommun. Syst.*, vol. 66, no. 3, pp. 481–503, 2017.
[40] Q. He, P. Liu, and Y. Wang, "Attribute based encryption method with revocable dynamic and static attributes for VANETs," *J. Comput. Res. Develop.*, vol. 54, no. 11, pp. 2456–2466, Jul. 2017.
[41] J. Shen, D. Liu, X. Sun, F. Wei, and Y. Xiang, "Efficient cloud-aided verifiable secret sharing scheme with batch verification for smart cities," *Future Gener. Comput. Syst.*, 2018. doi: 10.1016/j.future.2018.10.049.
[42] L. L. Chen, "A threshold group signature scheme for mobile Internet application," *Chin. J. Comput.*, vol. 41, no. 5, pp. 1052–1067, May 2018.
[43] Y. M. Wang, "Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs," *Secur. Commun. Netw.*, vol. 18, no. 2, pp. 374–382, May 2017.

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, and the Ph.D. degree in control theory and information safety from the University of Science and Technology Beijing (USTB) and Beijing University of Posts and Telecommunications (BUPT), in 2002 and 2006, respectively. She was a Visiting Scholar with the University of California at Berkeley, Berkeley, USA, from 2014 to 2015. She is currently a Full Professor with the Department of College of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. Her current research interests include blockchain technology, information security, nonlinear dynamics, and wireless sensor networks.

DI WANG received the B.S. degree in electronic and information engineering from the Jiangxi University of Science and Technology, Jiangxi, China, where she is currently pursuing the M.S. degree in communication and information systems. Her current research interests include blockchain technology and information security.