Received January 30, 2020, accepted February 11, 2020, date of publication February 24, 2020, date of current version March 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2974964

Electronic Payment Schemes Based on Blockchain in VANETs

XINYANG DENG [1] **AND TIANHAN GAO** [1,2]
[1] Software College, Northeastern University, Shenyang 110169, China
[2] Engineering Research Center of Security Technology of Complex Network System, Ministry of Education, Northeastern University, Shenyang 110169, China

Corresponding author: Xinyang Deng (xinyang1121@sina.com)

This work was supported by the National Natural Science Foundation of China under Grant N180716019 and Grant N182808003.

ABSTRACT Vehicular ad-hoc networks (VANETs) is considered as an important part of intelligent transportation system (ITS). Depending on the interconnection between vehicles and roadside units (RSUs), VANETs can provide a variety of application services for drivers and passengers. Due to the necessary service cost, many applications have to face the problem of how to charge vehicle for the services. This paper, which relies on blockchain technology, takes park toll management system and electronic toll collection system (ETC) as scenarios. Two payment schemes, V-R transaction and V-Rs transaction, are then proposed. The security and performance analysis show that the proposed schemes are efficient and robust.

INDEX TERMS VANETs, blockchain, electronic payment, ETC.

I. INTRODUCTION

With the development of transportation industry and wireless network, vehicular ad-hoc networks (VANETs) are proposed and show great potential in intelligent transportation system (ITS) for providing network and communication services [1]. In VANETs, vehicles can communicate with each other (V2V) relaying on opportunistic wireless links. In V2V communication, safety and entertainment messages are usually exchanged to guarantee each vehicle to obtain diverse application services like traffic safety and infotainment [2]. Besides, vehicle to roadside (V2R) communication between vehicle and roadside unit (RSU) is also an important component of VANETs, which can provide network service and more accurate application service for vehicles, such as traffic probe (TP). Generally, the applications depending on VANETs can be divided into safety-related applications, efficiency-related applications, and entertainment-related applications [3].

1) Safety-related applications. In security application scenarios, the vehicle equipped with DSRC equipment regularly broadcasts its status through beacon message, including speed and direction. Depending on the beacons and own trajectory, other vehicles are able to judge whether there is the possibility of collision [4]. Meanwhile, RSU also broadcasts security message about the surrounding road conditions, such as lane-changing assistance and traffic sign violation warning. Such safety-related applications may effectively avoid traffic accidents caused by vehicle occlusion and poor road conditions [5].
2) Efficiency-related applications. Due to V2V and V2R communications,vehicles can learn the traffic congestion status and traffic light information of the nearby area and adjust the speed and driving path [6]. Such applications, like Congested Road Notification, improve traffic efficiency and reduce energy consumption.
3) Entertainment-related applications. There are several traditional applications to enhance drivers or passengers' experience in vehicle, like the AM/FM radio receiver with optional CD/DVD player. However, these applications usually fail to provide dynamic entertainment services according to users'needs. Users are usually passive consumers rather than active participants [7]. In order to improve the situation, Cadillac CUE [8], OnStar's RemoteLink [9], Chevrolet MyLink [2] propose a series of entertainment-related applications, which provide rich services as news, music, match, as well as the connections to friends or family.

Since great business opportunities are offered by a wide range of VANETs applications, it is expected that the research in this area continues to attract attention of researchers.

The associate editor coordinating the review of this manuscript and approving it for publication was Antonio Skarmeta Gómez.

However, when users enjoy the services brought by these applications, the necessary costs (such as human cost, infrastructure construction cost) will be generated, which is important to built a healthy ecology. Consequently, it is essential to build an efficient and secure payment scheme that satisfies the requirements under VANETs.

The electronic payment system offered by RSU is thought it thought to be an ideal solution. Taking ETC (electronic toll collection) based on DSRC as an example, RSU broadcasts the service within its communication range. When vehicles response with the service, the payment protocol will be triggered. However, each transaction between RSU and vehicle has to be transferred to the payment platform, and all accounts have to be maintained by platform, which may cause enormous efficiency and security issues.

Recently, blockchain is considered as competitive approach to participate and record transactions. In blockchain, members can interact with each other without a trusted intermediary where the public ledgers are maintained by all the participants, central managers are thus removed [10]. In addition, the introductions of cryptography primitives and consensus mechanisms guarantee the stability and security of the system.

In this paper, two electronic payment schemes based on blockchain are proposed respectively. Specifically, the payment platform serves for converting real currency into virtual currency. Besides, the entities involved in a transaction include a vehicle and a RSU (V-R transaction) like the park toll management system, or a vehicle and multiple RSUs (V-Rs transaction) as electronic toll collection. We will introduce the whole transaction processes based on these two scenarios.

The remainder of this paper is organized as follows. In section II, the preliminaries such as VANETs, DSRC, WAVE and blockchain are sketched. Section III elaborates the proposed schemes about V-R transaction and V-Rs transaction. In Section IV, the security analysis of the schemes are given. The performance analysis is presented in Section V. Finally, the paper is concluded in Section VI.

II. PRELIMINARIES

A. VANETs

Vehicular Ad-hoc Network (VANET), as a particular type of Mobile Ad-hoc Network(MANET), is considered as a new application of wireless communication technology in the field of vehicle control [11]. As shown in Figure 1, VANETs, also called V2X (vehicle to everything), mainly includes V2V (vehicle to vehicle) communication and V2I (vehicle to infrastructure) communication [12]. In V2V communication, vehicles must work together to guarantee the dissemination of V2V service notification in time, such as congested road, post crash, road hazard, and road forecast [13], [14]. In V2I communication, RSU is deemed to an important infrastructure to provide network service for vehicles and help vehicles obtain safety, traffic management, and infotainment application [15]. Generally, V2X communication is launched on the basis of DSRC [16] and the IEEE WAVE standard [17] in North American or ETSI ITS-G5 [18] in Europe. In the proposed scheme, DSRC and IEEE WAVE standard are adopted.

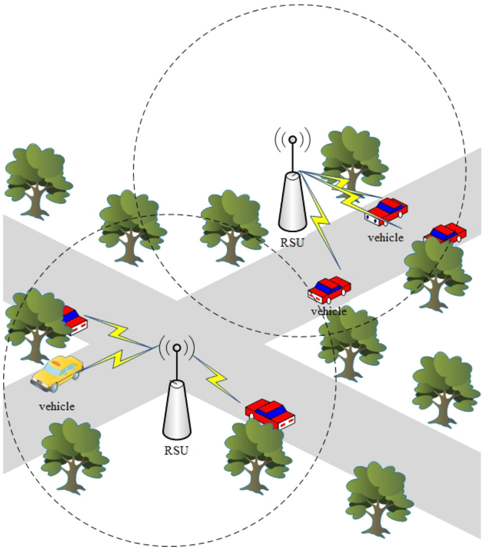

FIGURE 1. VANETs architecture.

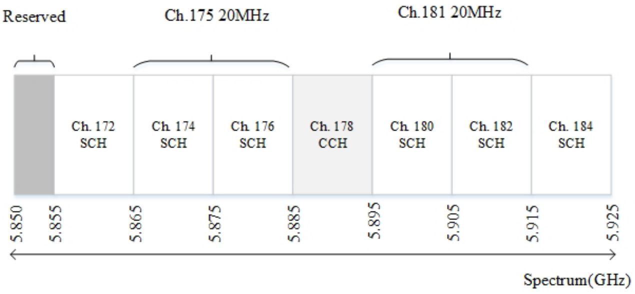

FIGURE 2. DSRC channels.

B. DSRC AND WAVE

DSRC [16] is proposed as an efficient and dedicated vehicle wireless communication technology to meet the requirements of V2I and V2V communication in VANETs, which is based on IEEE 802.11p standard and allocated from 5.85 to 5.925 GHz of spectrum for dedicated short-range communication radio services in ITS. As shown in Figure 2, the band is segmented into 7 channels. Each channel is allocated 10 MHz, forming one CCH (control channel) and 6 SCHs (service channel), where two 10MHz channels can also be combined into 20 MHz channels, such as channel 175 and channel 181. DSRC radio can only communicate on one channel at a time. To use multiple channels, it is necessary to switch radio dynamically.

Figure 3 shows layered architecture for DSRC/WAVE stack. In the physical layer and MAC layer, IEEE 802.11p is adopted. In the middle layer of the stack, WAVE

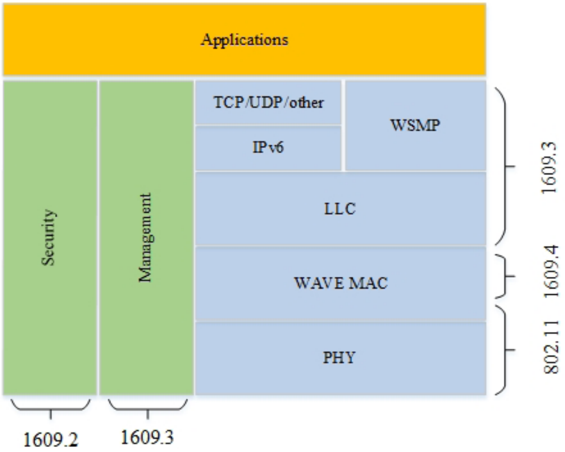

FIGURE 3. DSRC/WAVE stack.

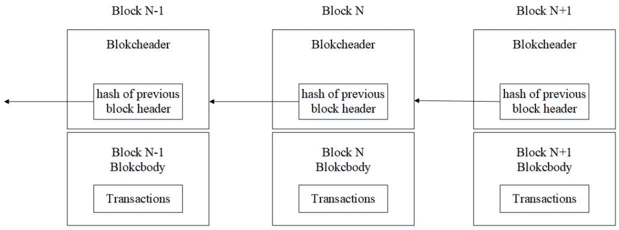

FIGURE 4. Logical representation of a blockchain.

(Wireless Access for Vehicle Environment), defined by the working group of IEEE 1609, is employed which is mainly composed of four components (1609.2, 1609.3, 1609.4) [19]: 1609.2 for security services [20], 1609.3 for networking services [21], 1609.4 for multi-channel operations [22].

C. BLOCKCHAIN

As depicted in Figure 4, blockchain is a synchronized and distributed ledger, which maintains a growing list of interconnected blocks. Since Bitcoin designed by Nakamoto *et al.* [23] appeared, blockchain has attracted lots of attentions from academia due to its advantages of decentralization, openness, and tamper-resistant. Blockchain consists of a set of nodes connected via the network like mesh and P2P topologies [24]. The nodes in blockchain can interact directly without any third trusted party. Such a trust-less infrastructure guarantees faster and cheaper transactions [25]. Ethereum is thought to be another important encrypted currency system based on blockchain. Compared with Bitcoin, Ethereum shortens block time, takes proof-of-stake to replace the proof-of-work, and supports smart contract [26]. The content of the contract is stored on the bolckchain in the form of codes. Relying on the tamper-resistant feature of the blockchain, the validity of the contract is maintained and all participants can not breach the contract from the beginning. These functions and features are very suitable for tthe ransactions between nodes in Internet of Things (IoT), where VANETs is a representative scenario [27].

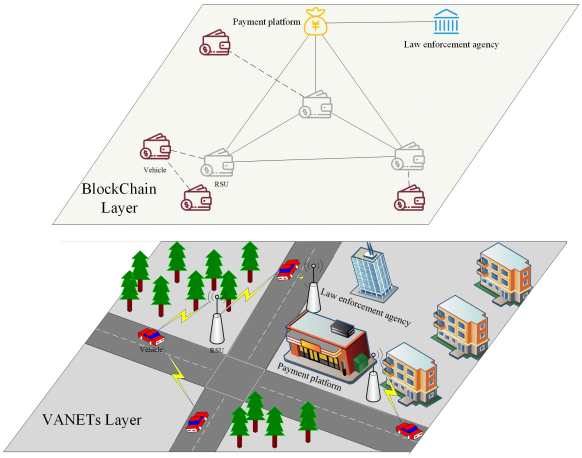

FIGURE 5. System model.

III. THE PROPOSED SCHEMES

A. SYSTEM MODEL

As shown in Figure 5, an electronic payment system model based on VANETs [28] and blockchain [29] is designed, which includes VANETs layer and blockchain layer.

1) VANETs LAYER

In the VANETs layer, all entities involved in communications and transactions are divided into: RSU, vehicle, and payment platform.

RSU broadcasts its application service on the CCH firstly. Then, RSU authenticates and communicates with vehicles interested in the service on the SCH. During authentication, RSU ensures the legality of the identity claimed by the vehicle. Meanwhile, RSU and vehicle build a secure bi-channel for the subsequent secure communication. Each vehicle can discover the service broadcasted by RSU on the CCH and switch to the corresponding SCH to communicate with the RSU for transaction. At the end of the transaction, the vehicle is also allowed to obtain a successful receipt from RSU. Payment platform is considered as a trusted third-party, like bank. In this platform, vehicles and RSUs are requested to register and open corresponding accounts to involve in the transaction. Besides, law enforcement agency is requried to connect to the network. If there are illegal vehicles in VANETs, law enforcement agency can obtain the illegal information through payment platform.

2) BLOCKCHAIN LAYER

Different to the traditional structure, the blockchain layer in the proposed scheme cuts out certificate authority (CA), and the security of all transactions is maintained by the entities within blockchain. Specifically, Genesis block is generated by payment platform. All accounts of RSUs and vehicles should be sent to the blockchain through payment platform. When added to the blockchain, each vehicle is required to deposit a certain amount of currency to guarantee that transactions are correctly executed. In addition, RSUs and

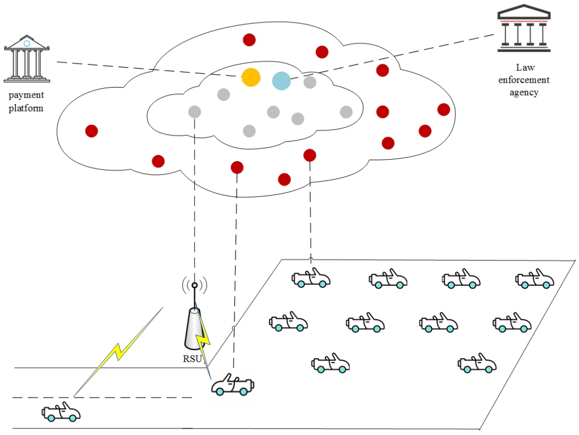

FIGURE 6. Park toll management system.

vehicles have different permissions in the blockchain. RSUs are responsible for maintaining all accounts in the blockchain through a unified consensus mechanism. Meanwhile, RSU is also allowed to trade with vehicles. Vehicles do not have the right to participate in the maintenance of blockchain due to its discontinuity and instability of network connections. However, all vehicles have the right to acquire data in the blockchain from RSU. After finishing the transaction with RSU, vehicles are able to request receipt from the RSU and verify its legality.

B. V-R TRANSACTION

V-R transaction refers that the transaction is executed between one vehicle and one RSU, where the vehicle carrying on board unit (OBU) is a payer unit and RSU acts as a payee unit. We take a park toll management system as the scenario of V-R transaction. As shown in Figure 6, when getting ready to enter a carpark, the vehicle first receives WSA (WAVE service advertisement) about the parking application service which includes the SCH to be used from RSU on the CCH. Then, the vehicle changes to the indicated SCH and communicates with RSU to send parking request and obtains the correspinding service. When leaving the carpark, the vehicle sends departure request to RSU. Once the service is completed, the vehicle pays to RSU and obtains the receipt. The details are depicted as following.

1) TRANSACTION INITIATION PROTOCOL

Before transaction initiation, RSU needs to create a smart contract (*Contract*) in the blockchain, which mainly includes necessary policies, like regulation of tolls, payee identity, etc. When a vehicle enters a carpark, transaction initiation protocol is performed as shown in Figure 7.

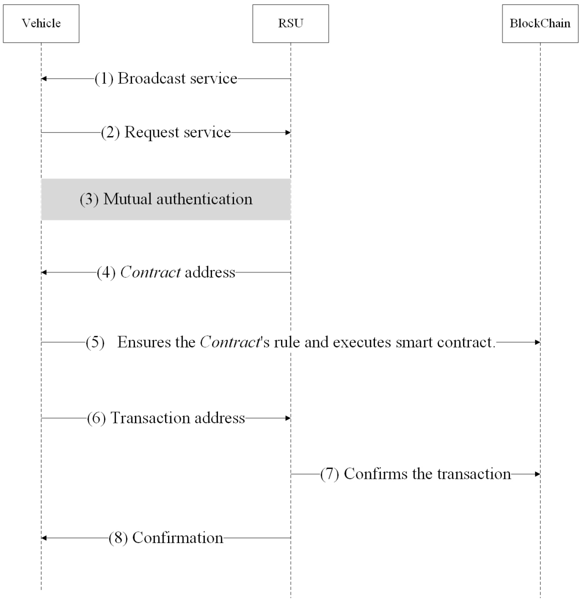

FIGURE 7. Transaction initiation protocol.

1) RSU broadcasts parking service regularly and reports the SCH and it's identity on the CCH.
2) Vehicle turns to the appropriate channel and requests the parking service.
3) During mutual authentication, vehicle needs to verify the validity of RSU, while RSU only determines whether the balance of the vehicle's claimed account in the blockchain meets the parking fee policy. If the balance is enough, the protocol continues to execute, otherwise RSU rejects the vehicle's parking request.
4) After successful authentication, vehicle joins the blockchain. RSU sends the address of *Contract* to vehicle.
5) Vehicle ensures the content of *Contract*'s rules and invokes the functions written in *Contract* to execute the smart contract. The blockchain system sets the nounce, start time, the address of payer, the address of payee and sends transaction address stored on the blockchain back to vehicle. Meanwhile, vehicle's signature is also added to the transaction.
6) Vehicle sends the transaction address to RSU.
7) When receiving the message from vehicle, RSU gets the transaction and confirms the contents.
8) RSU sends confirmation to vehicle.

2) TRANSACTION CONFIRMATION PROTOCOL

When vehicle gets ready to leave the parking lot and enters RSU communication range, transaction confirmation protocol is triggered as shown in Figure 8.

1) RSU broadcasts parking service regularly and reports the SCH and it's identity on the CCH.
2) Vehicle turns to the SCH and requests the settle account service.
3) When receiving the request from vehicle, RSU updates the transaction in blockchain to set the value of end time, and signs the transaction.
4) RSU sends response to vehicle to indicate that the transaction has been updated.
5) Vehicle confirms the transaction and signs it.

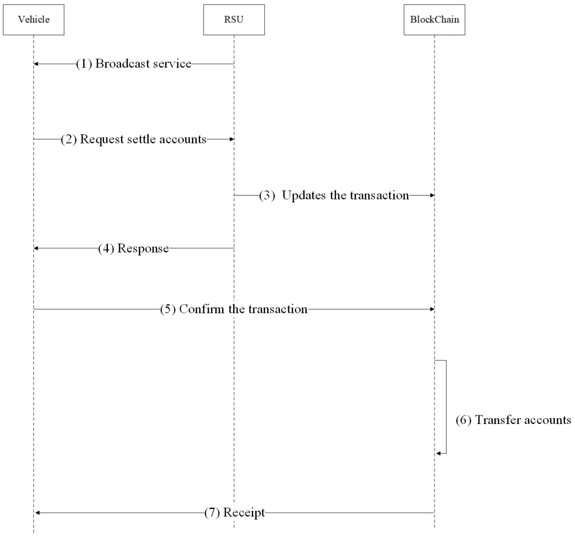

FIGURE 8. **Transaction confirmation protocol.**

6) The blockchain system confirms the legality of the transaction and transfers parking fees from vehicle account to RSU account.
7) Finally, vehicle obtains the receipt of the transaction.

C. V-Rs TRANSACTION

V-Rs transaction refers that the transaction is executed between one vehicle and multiple RSUs. We chooses electronic toll collection (ETC) as the scenario of V-Rs transaction. When getting ready to enter the highway, the vehicle receives the ETC service from the RSU$_1$ on the CCH. Then, the vehicle changes to SCH and communicate with RSU$_1$ to send erntering requests. When the vehicle leaves the highway, the vehicle communicates with the RSU$_1$ in the same way and sends a departure request. Meanwhile, the vehicle pays with its ETC account and obtains the receipt. The details are depicted as below.

1) TRANSACTION INITIATION PROTOCOL

Before transaction initiation, ETC system creates the smart contract which includes charging policy on blockchain. All RSUs are informed of the smart contract address by ETC system.

1) Vehicle receives RSU$_1$'s broadcast service on CCH when getting ready for entering the highway.
2) Vehicle sends ETC service request on SCH.
3) During mutual authentication, vehicle verifies the legality of RSU$_1$. RSU$_1$ ensures that the account of the vehicle is legal and that the balance of the account on the blockchain meets the policy.
4) If the mutual authentication is successful, RSU$_1$ sends the contract address to vehicle.
5) After receiving the contract address,vehicle executes the smart contract, the blockchain system sets the nounce, start time,the address of payer, the address of RSU$_1$ and sends transaction address back to vehicle.Meanwhile, vehicle signs the transaction.
6) The transaction address is sent to RSU$_1$ by vehicle.
7) RSU confirms the transaction and signs it.
8) RSU sends transaction confirmation message to vehicle.
9) Vehicle verifies RSU$_1$'s signature.

2) TRANSACTION CONFIRMATION PROTOCOL

When the vehicle gets ready to leave the highway and enters RSU$_2$'s communication range, the vehicle is request to complete the transaction. The details are described below.

1) RSU boardcasts the ETC payment service, which is different from the service when vehicle enters highway.
2) Vehicle switches its radio to the indicated SCH and requestes to leave highway.
3) Vehicle and RSU$_2$ execute mutual authentication and build secure channel.
4) Vehicle sends the address of the transaction to RSU$_2$.
5) When receiving the message from vehicle, RSU$_2$ finds and updates the transaction by setting end time, and signs the transaction.
6) RSU$_2$ sends response to imply that the transaction has been confirmed.
7) Vehicle confirms the transaction and signs the contract.
8) Vehicle sends confirmation to RSU$_2$.
9) RSU$_2$ confirms the transaction. If the transaction is legal, RSU$_2$ and vehicle confirm the content of transaction and sign it. The blochchain system will transfer the fee from vehicle's account to ETC's account.
10) Vehicle leaves the highway, and obtains the recepit through blockchain system.

IV. SECURITY ANALYSIS

In the process of communication among entities in VANETs, it is very vital to protect the privacy of all parties and guarantee the security of the communication content. In addition, during the transactions, it is also necessary to ensure the non-tamperability of the payment result and the non-repudiation of the payment behavior. According to the security and privacy requirements of VANETs service in [20], [30], we analyze the security of the proposed scheme in the following aspects.

1) Authentication. Authentication is the process of verifying the legitimacy of the identity claimed by the prover. In the proposed scheme, all payment-related operations must be done after authentication. Depending on the trust relationship establishied by the communicating entities, the scheme not only ensures that the vehicle can obtain legal services, but also guarantees the accounts security of the entities.
2) Accountability. A perfect payment system must ensure that the whole transaction process are recorded in the system. If a vehicle or RSU is successfully attacked by an adversary, the legal accounts may be affected and

even the whole payement system is destroyed. In this situation, the payment system should support to supply all the records of actions and ascertain the identity of the adversary. In the proposed scheme, all transactions are recorded in the blockchain. Through the distributed consensus mechanism of blockchain, RSUs store all transaction records in the payment system. Even if some RSUs are breached by the adversary, law enforcement agencies can still obtain information about the transaction in terms of the records stored in other RSUs.

3) Non-repudiation. Once law enforcement agency has published records of attacks by illegal entities, illegal behaviors should not be denied. In the proposed payment scheme, the content of transaction is required to be signed by RSU and vehicle. The signature provided by the law enforcement agency and the payment platform makes it impossible for the adversary to deny the malicious behavior.
4) Account revocation. In the proposed electronic payment system, all vehicles' public keys and private keys are generated by themselves. Since all transactions are bound with the accounts, the blockchain system can locate the corresponding account according to the public key of the vehicle. Therefore, if a misbehavior appears, it can be confirmed that the illegal entities cannot make legal transactions by freezing the accounts.
5) Conditional anonymity and confidentiality. The law enforcement agency has the right to reveal the true identity of the illegal entities and the content of the corresponding transactions. However, according to [19], the identity of vehicle should be protected in the whole process of authentication and communication between vehicle and RSU, that is, the anonymity of vehicle should be achieved. Meanwhile, vehicles and RSUs should not know the content of transactions that do not belong to them,even if they store the data of all transactions as nodes of the blockchain. In the blockchain system, cryptographic mechanisms such as ring signatures [31] or zero-knowledge proofs [32] are usually used to achieve the security goal.
6) Perfect forward privacy. During authentication, communication, and payment, the vehicle only needs to make RSU believe that its identity is legal and the account balance in the blockchain is sufficient, while RSU only needs to make sure that the vehicle believes its identity and the services it provides are legal.Entities are not required to obtain additional information to meet the forward privacy goal.
7) Replay protection. In digital cash system, the most common replay attack is double spend attack. All blockchain systems have to address this issue and come up with a variety of solutions. For example, in bitcoin system [23], UTXO (Unspent Transaction Output) mechanism and blockchain consensus mechanism can effectively resist double spend attack. In the proposed system, Ethereum is adopted, where timestamps are added to the transactions to ensure the uniqueness of each transaction.

Therefore, the proposed scheme can guarantee the security of the payment in VANETs well. Even if there is illegal transaction, the scheme can determine the illegal vehicle through the recorded payment information and inform law enforcement agency.

V. PERFORMANCE ANALYSIS

In this section, the performace analysis of the proposed electronic payment system is given in detail with respect to communication overhead, computation overhead, as well as signaling cost in the V-R transaction.

A. COMMUNICATION OVERHEAD

In this paper, communication overhead refers to the total size of message transmitted in a transaction.

In our scheme, after mutual authentication bwetween RSU and vehicle, RSU sends the address of contract (20 bytes) to vehicle. When vehicle ensures and executes the smart contract, it is required to send the address and the signature, where the signature is 72 bytes long [33]. After confirming the transaction, RSU sends the signature confirm the transaction. Thus, the communication overhead of transaction initiation is:

$$\begin{aligned} CO_{initiation} &= 20 \times 2 + 72 \times 2 \\ &= 184(bytes) \end{aligned} \tag{1}$$

During transaction confirmation, RSU sends its signature as the respose to vehicle. Vehicle confirms the transcation and provides signature as the proof that the transaction has been confirmed. Then blockchain executes accounts transfer service, and sends the receipt to vehicle through RSU, where receipt is the transaction address recorded on the block. Therefore, the communication overhead of transaction confirmation is:

$$\begin{aligned} CO_{confirmation} &= 20 + 72 \times 2 \\ &= 164(bytes) \end{aligned} \tag{2}$$

As transaction policy and smart contract are stored in the blockchain, vehicle and RSU can find the transaction content through the transfered address, and confirm the transaction through the signature, thus the communication overhead is relatively low.

B. TRANSACTION LATENCY

Transaction delay refers to the total time from the vehicle sending the transaction request to the transaction being confirmed. We conduct our performace evaluation on a laptop running ubuntu16.04 LTS and equipped with an 2.6 GHz Intel i7 CPU and 2GB RAM. In the experiment, Ethereum is adopted. Due to the limitation of solidity language, there is no effective method to calculate the execution time of smart contract accurately, we use web3j tool to call the smart contract, and time statistics is executed through java's method.

TABLE 1. The data elements of smart contract.

Element	Type
$payeeAddress$	address
$payerAddress$	address
$price$	uint
$startTime$	uint
$endTime$	uint
$amount$	uint

The singnature algrithm is ECDSA256 [35]. The execution time of executing smart contract in transaction initiation and transaction confirmation is 460ms and 444.5ms respectively. The data elements defined in the smart contract are shown in Table 1.

In transaction initiation, after mutual authentication, contract and transaction address need to be sent through wireless network. Meanwhile, vehicle is requested to ensure the policy of contract through RSU. According to [34], we assume that the transmission delay is 20ms, the transaction delay during transaction initiation is:

$$\begin{aligned} TI_{initiation} &= 20 \times 4 + 460 \\ &= 540(ms) \end{aligned} \tag{3}$$

In transaction confirmation, RSU updates the content of the consponding transcation in blockchain, and sends respond to vehicle. Vehlcle confirms the final content of the contract, and signs it. Then, blockchain transfers the fees from vehicle account to RSU account. Finally, vehicle obtain receipt from blockchain through RSU. Consequently, the transaction delay during transaction confirmation is:

$$\begin{aligned} TI_{confirmation} &= 20 \times 3 + 444.5 \\ &= 504.5(ms) \end{aligned} \tag{4}$$

As for transaction latency, the most time-consuming is the signature generation. Therefore, which signature scheme is adopted in the blockchain system can greatly affect the transaction latency of the proposed scheme.

C. SIGNALING COST

The signaling cost refers to the entire amount of transaction signaling cost both in initiation and confirmation phases. We adopt the fluid-flow model [36] to evaluate the cost. We assume that vehicle's movement direction is in the range of (0,2π). The crossing rate(R) and signaling cost (SC) are respectively defined as:

$$R = \frac{\rho v L}{\pi} \tag{5}$$

$$SC = TL \times R \tag{6}$$

where ρ, v, l are defined as vehicle density, vehicle average velocity, and permeters of a subnet. In the proposed scheme, "TL" includes transmission delay for transaction initialization and transaction confirmation. We sets $L = 100m$, $\rho = 0.1 \sim 0.01(1/m^2)$, $v = 0 \sim 40(m/s)$, according to [34]. The result is shown in Figure 9.

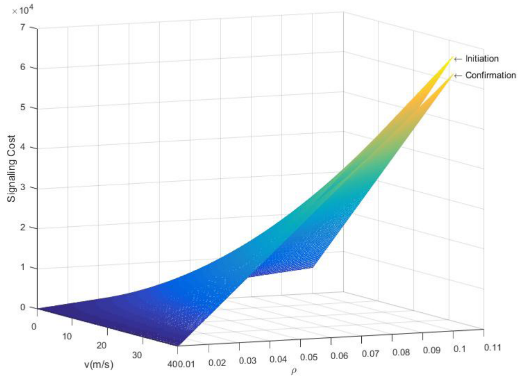

FIGURE 9. Signaling cost.

According to Figure 9, we can see that, with the increase of vehicle density and speed, the signaling cost is rising. However, due to low density and slow speed of vehicle in parking toll management system and electronic toll collection system, the signaling cost of the proposed schemes is ideal.

VI. CONCLUSION

In this paper, taking park toll management system and electronic toll collection system as application scenarios, we proposes two electronic payment schemes in VANETs. Based on blockchain technology, all transactions are automatically executed through smart contracts. Only RSUs participate in the consensus mechanism, and vehicles can obtain data through RSU, which ensures the fast synchronization of data stored by all entities in the blockchain. The introduction of cryptography building blocks protects the security and privacy of vehicle accounts.

In the future, we will refine the communication architecture and authentication protocol, and propose a feasible solution for protecting the privacy of the vehicle. Furthermore, we will look for similar payment approaches in VANETs and make a comparative analysis with the proposed scheme.

REFERENCES

[1] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–17, Mar. 2018.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, p. 584–616, 4th Quart., 2011.

[3] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.

[4] A. P. P. Aguiar, J. Almeida, M. Bayat, B. Cardeira, R. Cunha, A. Häusler, P. Maurya, A. Oliveira, A. Pascoal, A. Pereira, and M. Rufino, "Cooperative control of multiple marine vehicles theoretical challenges and practical issues," in *Proc. Manoeuvering Control Mar. Craft*, Guarujá, Brazil, Sep. 2009, p. 1–6.

[5] J. T. Isaac, J. S. Camara, S. Zeadally, and J. T. Marquez, "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 10, pp. 2478–2484, Jun. 2008.

[6] R. P. Singh and A. Gupta, "Traffic congestion estimation in VANETs and its application to information dissemination," in *Distributed Computing and Networking*, vol. 6522. Berlin, Germany: Springer, 2011, pp. 376–381.

[7] O. K. Tonguz and M. Boban, "Multiplayer games over vehicular ad hoc networks: A new application," *Ad Hoc Netw.*, vol. 8, no. 5, pp. 531–543, Jul. 2010.

[8] W. Sha, D. Kwak, B. Nath, and L. Iftode, "Social vehicle navigation: Integrating shared driving experience into vehicle navigation," in *Proc. 14th HotMobile Workshop*, New York, NY, USA, 2013, p. 161–166.

[9] S. Stephen, L. Han, P. Shankar, and L. Iftode, "Roadspeak: Enabling voice chat on roadways using vehicular social networks," in *Proc. 1st Workshop SocialNets*, Scotland, U.K., 2008, p. 43–48.

[10] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[11] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*. Hoboken, NJ, USA: Wiley, 2010.

[12] *Wireless Access in Vehicular Environments*, IEEE Standard 802.11p-2010, 2010.

[13] L. Nassar and F. Karray, "Fuzzy logic in VANET context aware congested road and automatic crash notification," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Vancouver, BC, Canada, Jul. 2016, pp. 1031–1037.

[14] B. Haider, S. Henna, A. Gul, and F. Aadil, "A survey on mobility management techniques in VANETs," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Nadi, Fiji, Dec. 2016, pp. 125–133.

[15] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.

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

[17] R. A. Uzcategui, A. Jose De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 126–133, May 2009.

[18] *Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems Operating in the 5 GHz range; Access Layer Part*, document ETSI TS 102 687 V1.1.1, ETSI, Jul. 2011.

[19] *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*, IEEE Standard 1609.0–2019 (Revision of IEEE Std 1609.0–2013), Apr. 2019, pp. 1–106.

[20] *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, IEEE Standard 1609.2–2016 (Revision of IEEE Std 1609.2–2013), Mar. 2016, pp. 1–240.

[21] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services Corrigendum 1: Miscellaneous Corrections*, IEEE Standard 1609.3-2010/Cor 1-2012 (Corrigendum to IEEE Standard 1609.3–2010), Jul. 2012, pp. 1–19.

[22] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation*, IEEE Standard 1609.4-2016 (Revision of IEEE Std 1609.4–2010), Mar. 2016, pp. 1–94.

[23] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[24] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[25] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," in *Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Beijing, China, Nov. 2017, pp. 70–74.

[26] (2016). *Smart Contract: 12 Use Cases for Business & Beyond, Prepared by: Smart Contracts Alliance in Collaboration With Deloitte an Industry Initiative of the Chamber of Digital Commerce*. [Online]. Available: https://www.cryptocoinsnews.com/smart-contracts-12-use-cases-for-business-and-beyond/

[27] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[28] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)*, IEEE Standard 1609.11-2010, Jan. 2011, pp. 1–62.

[29] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[30] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *Proc. Int. Conf. Comput. Sci. Eng.*, Vancouver, BC, Canada, 2009, pp. 139–145.

[31] S. SF, M. H. Au, J. K. Liu, and T. H. Yuen, "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *Computer Security—ESORICS* (Lecture Notes in Computer Scienc), vol. 10493, S. Foley, D. Gollmann, and E. Snekkenes, Eds. Cham, Switzerland: Springer, 2017.

[32] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, San Jose, CA, USA, May 2014, pp. 459–474.

[33] D. R. L. Brown, *Standards for Efficient Cryptography 2 (SEC 2): Recommended Elliptic Curve Domain Parameters*, vol. 2. Standards for Efficient Cryptography, 2010, p. 37.

[34] J.-H. Lee and J.-M. Bonnin, "HOTA: Handover optimized ticket-based authentication in network-based mobility management," *Inf. Sci.*, vol. 230, p. 64–77, May 2013.

[35] *Information Technology—Security Techniques—Digital Signatures With Appendix—Part 3: Discrete Logarithm Based Mechanisms*, Standard ISO/IEC 14888-3, 2014, p. 130.

[36] S. Pack and Y. Choi, "A study on performance of hierarchical mobile IPv6 in IP-based cellular networks," *IEICE Trans. Commun.*, vol. E87-B, no. 3, pp. 462–469, 2004.

XINYANG DENG received the B.E. degree from the Software College, Dalian University of Foreign Languages, in 2014. He is currently pursuing the degree with the Software College, Northeastern University. His primary research interests are next generation network security, PMIPv6 security, and identity-based cryptography.

TIANHAN GAO received the B.E. degree in computer science and technology, the M.E. and Ph.D. degrees in computer application technology from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University, in April 2006, as a Lecture of the Software College. He received an early promotion to an Associate Professor, in January 2010. He was a Visiting Scholar with the Department of Computer Science, Purdue, from February 2011 to February 2012. He received the Doctoral Tutor Qualification, in 2016. He is the author or coauthor of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, and virtual reality.