Research Article

A Decentralized ETC Architecture Based on Blockchain Technology

Shize Huang,1 Lingyu Yang,1,2 Xiaolu Yang,3,4 Xinghua Li,2 and Fei Gao4

1Shanghai Key Laboratory of Rail Infrastructure Durability and System Safety, Tongji University, Shanghai 201804, China
2Key Laboratory of Road and Traffic Engineering of Ministry of Education, Tongji University, Shanghai 201804, China
3China Railway Shanghai Group Co., Ltd., Shanghai 200071, China
4School of Information Science and Technology, Tibet University, Lhasa 850012, China

Correspondence should be addressed to Xiaolu Yang; yangxiaolu@tongji.edu.cn

Received 26 April 2020; Revised 2 April 2021; Accepted 4 May 2021; Published 20 May 2021

Academic Editor: Giuseppe Guido

Copyright © 2021 Shize Huang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Electronic toll collection (ETC) has been widely spread in China, providing efficient, comfortable, and convenient toll services. However, the nature of centralization of those ETC systems has incurred serious security threats. Given blockchain’s features of self-trust, decentralized architecture, and traceability, we propose a decentralized ETC architecture based on blockchain technology. After implementing our architecture in a test network, we verify its feasibility. A thorough discussion indicates that our architecture can effectively operate normal ETC services while avoiding most attacks that threaten traditional ETC systems.

1. Introduction

Electronic toll collection (ETC) has been widely used for its competitive advantages, including reducing operating costs of highway companies, saving drivers’ time, and improving traffic efficiency [1]. However, current ETC systems inherit a critical vulnerability from centralized networks: overburdened servers. A typical ETC system includes a settlement center and numbers of front ends for collecting fees. Tremendous transactions are processed in the single center. If the central server is attacked, the consequences will be calamitous: billions of data will be tampered or even lost, and the whole system will be paralyzed. A couple of existing centralized systems have claimed that they have suffered from the “centralization” issue, like Momo APP and Vivo APP. Many studies have been devoted to the protection of servers. Ma et al. designed a location-aware scheme for transaction verification that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack from malicious readers [2]. Ma et al. proposed a context-aware unlocking approach which selects some toll cards according to certain rules to respond to reader interrogations and thus minimizes the possibility of unauthorized reading and relay attacks [3]. Randriamasy et al. used the principle of differential-GPS mixed with Kalman filtering and extended Kalman filtering applied to the GPS and CAN bus measurements received by the RSU from the connected vehicles [4]. Pietro et al. devised a technique that makes RFID identification server dependent, providing a different unique secret key shared by each pair of tag and server [5]. Zhao et al. proposed SCsec which achieves computationally secure communication between the transmitter and receiver, preventing the eavesdroppers beyond a certain range from learning anything about the content of the communication [6]. Although the above studies are elegant, they fail to target the fundamental issue: high-centralized framework.

Fortunately, blockchain has emerged as a new technology of self-trust, decentralized architecture, and with traceability [7, 8], providing a potential impetus to changing ETC’s framework. In addition, blockchain technology is widely used in traffic signal control mechanisms [9], traffic flow forecasts [10], and traffic information systems [11] in the transportation field.

Therefore, we present a decentralized architecture for the ETC system using blockchain technology. We test the
architecture in a network and verify its feasibility. We also discuss our architecture’s ability of defending against attacks that threaten traditional centralized systems.

2. Conventional ETC and Blockchain Technology

2.1. Fundamental Working Process. ETC requires two key devices: on-board unit (OBU) installed on vehicles and road side unit (RSU) installed on tollgates. The two parts communicate through wireless signals when ETC collects fees.

The working process of an ETC system is described as follows:

1. A driver purchases an electronic label (OBU) and a prepaid IC card from a card issuing company.
2. The driver inserts the IC card into the electronic label (OBU) that has been installed in the vehicle.
3. When the vehicle passes through a tollgate, RSU reads its OBU information through wireless communication.
4. The computer in the toll station generates transaction data.
5. The computer uploads the transaction data to a settlement center.
6. The settlement center conducts calculation, and the clearing bank transfers the profit to the highway company which the toll gate belongs to.

2.2. Framework. ETC adopts the layered-cascade architecture to deploy toll booths, toll stations, and a settlement center [12]. As shown in Figure 1, toll data are transmitted from toll booths to the settlement center. The settlement center processes the toll data, liquidates account points, and asks the card issuing company to pay the tolls which their IC cards recorded. Thus, the clearing bank can transfer money to each highway company. It is obvious that major calculation and storage of the whole system are imposed on the settlement center.

2.3. Concept of Blockchain. Blockchain was proposed by Satoshi Nakamoto in his very first paper as the underlying technology and infrastructure of Bitcoin [13]. It links data blocks in chronological order using cryptography to guarantee a non-tamperable and unforgeable distributed ledger.

Each block in a blockchain initially contains three elements: ID of the block, certain transaction information, and ID of the previous block. Each ID is uniquely identified by a hash value.

Each block includes a set of Merck tree in which each hash value is calculated from transaction information. This scheme ensures that both the transaction data in each block and blocks linked in the blockchain cannot be tampered.

When a block is generated, its timestamp is created and stored in the block. The timestamp is the unique identification of the block and guarantees the authenticity of the block [14]. The structure of a blockchain is shown in Figure 2.

A blockchain is maintained by all nodes in the network, and each node executes and records same transactions information. Any node in the network can read transactions contained in any other node.

2.4. Smart Contracts. The blockchain architecture proposed by Satoshi Nakamoto focuses on supporting the implementation of virtual currency. Although it is flexible, it can barely apply to scenarios other than virtual currency. In order to better apply blockchain technology to other industries, some researchers noticed its superiority in decentralization and expanded it to blockchain 2.0. Its essence is to treat a blockchain as a credit infrastructure that is programmable and distributed so that smart contacts can function based on it [15]. Thus, blockchain is extended to support a decentralized market where transaction contents can be varied.

Blockchain 2.0 employs a combination of technologies for exchanging, processing, and storing data between multiple participants based on modern cryptography, distributing coherence protocols, communicating in peer-to-peer network, and so on.

A smart contract is a piece of code that exists in a blockchain and is identified by a unique address. It contains a set of executable functions and state variables. Once the contract is uploaded, it will exist in the blockchain forever. Any user in the blockchain network can trigger a function in the contract by sending a transaction to the contract. The contract code is executed by each node in the network, which contributes to the verification of a new block. After a function is executed, the state variables in the contract will change accordingly.

2.5. Typical Applications. Blockchains have recently attracted interest of stakeholders across a wide span of industries. Some studies of transportation also have devoted to it. Christidis and Devetsikiotis concluded that the combination of blockchains and IoT can be pretty powerful [16]. Zhang and Wen “realized the transaction of smart property and paid data on the IoT with the help of P2P trade based on the blockchain and smart contract” [17]. Kang et al. proposed a localized P2P Electricity Trading system with CONsortium blockchain (PETCON) to illustrate detailed operations of localized P2P electricity trading [18]. Jaffe et al. presented a financial incentive system to increase the prevalence of urban cycling based on the blockchain system [19]. Lei et al. utilized blockchain concept to simplify the distributed key management in heterogeneous VCS domains [20]. Li et al. resolved critical issues of vehicular announcement network through proposing an effective announcement network called CreditCoin, a novel privacy-preserving incentive announcement network based on blockchain via an efficient anonymous vehicular announcement aggregation protocol [21]. In order to solve the design flaws of the blockchain, security and privacy issues, and incomplete specifications bring risks to its users, Norta et al. detailed the modeling
3. An ETC System Based on Blockchain

Targeting security issues of ETC systems, we propose a new ETC architecture based on smart contract and blockchain. The architecture simplifies toll payment and settlement while retaining all the functions and most of the infrastructure and equipment of original ETC systems. Toll data do not need to pass through the settlement center and the clearing bank any more. Instead, the system can directly transfer drivers’ payment to the corresponding highway company, while ensuring data’s safety and reliability.

3.1. Framework. Figure 3 depicts the framework of our blockchain-based ETC system [18]. The function of each part is explained as follows:

(i) Blockchain Underlying Platform. The platform records transaction information of RSU, users, and card issuing companies through smart contracts and forms a blockchain.
(ii) Users. This unit includes OBU and IC card. OBU stores vehicle information, and the IC card records account points. Each user holds his own private key and public key.
(iii) RSU. An RSU is divided into an RSU entrance and an RSU exit. The entrance only interacts with users and does not perform point transactions. The exit has its own private and public keys and conducts point transactions with users and card issuing companies.
(iv) Card Issuing Company. This organization issues OBUs and IC cards. It can also redeem cash points for users.
(v) Highway Company. It manages RSUs of its own. First, it collects earning points of all its RSU exits through the blockchain underlying platform, and then asks the card issuing company to transfer the corresponding payment. Notably, highway companies do not participate in point transaction but check transaction information on the blockchain and store private key addresses of their own RSUs.

As shown in Figure 3, RSU, users, and card issuing company conduct information exchanges and point transactions through smart contracts on the blockchain underlying platform. The transaction information between the three will be recorded and be used to form a blockchain in the blockchain underlying platform.

3.2. Typical Scenario. Figure 4 explains a typical scenario of the proposed architecture. Action 1 means the user registers...
an account in the card issuing company and buys a prepaid IC card. Action 2 indicates the RSU entrance records the user’s information. Action 3 means the RSU exit charges the user. Action 4 means the card issuing company transfers the money to the highway company that the RSU belongs to according to the RSU exit’s income. Transaction A represents that the card issuing company assigns certain points to the user’s account. Transaction B means that the user’s account transfers certain points to the RSU exit account. Transaction C means that the RSU exit account transfers certain points to the card issuing company account.

Once a transaction is completed, a new block will be created in the blockchain and the transaction information will be recorded in the block. As illustrated in Figure 4, the information of Transaction A is written in block N and that of Transaction B in block N + 1. In this way, the blockchain can store the information of all transactions.

Smart contract is required each time a transaction is ready to start. Only when certain conditions are met, the smart contract will be operated, and then the transaction can be conducted. For example, if the balance of a user’s account is insufficient, the transaction will not succeed, which means when someone illegally changes user’s account balance, transactions will not be processed. This guarantees the security of the ETC system.

3.3. Transaction Flow. Transactions in the proposed architecture flow between three parts: users, RSU exit, and card issuing company. The processes given as follows only describe transactions related to the blockchain, and other workflows, including the calculation of charge amounts and the road segmentation algorithm, remain the same as those in traditional ETC systems.
3.3.1. **Point Transaction between User and Card Issuing Company.** Figure 5 depicts point transaction between user and card issuing company, which is operated as follows:

1. A user registers an account and obtains its own public and private keys
2. The user buys an IC card from the card issuing company while the card issuing company receives the corresponding money
3. The card issuing company reads the IC card
4. The card issuing company obtains the public key address of the IC card
5. The card issuing company transfers the corresponding points to the IC card through the smart contract
6. The blockchain records the transaction occurred in step 5.

3.3.2. **Point Transaction between User and RSU.** Figure 6 exhibits the point transaction between user and RSU, and the steps are explained as follows:

1. A user drives to an RSU entrance, and the entrance records the user’s information
2. The user drives to the RSU exit, and the exit records the user’s information
3. Based on the information collected by the entrance and the exit, the exit sends the information about payable amount and its own public key address to the user
4. The user transfers the corresponding points to the RSU exit through the smart contract
5. The blockchain records the transaction operated in step 5

3.3.3. **Point Transaction between Card Issuing Company and RSU.** Figure 7 illustrates point transaction between the card issuing company and RSU, and the steps are listed as follows:

1. The highway company checks its own revenue points and cash amounts through the blockchain, given that it keeps all the public and private keys of its RSUs
2. The highway company submits an application for exchanging points with money to the card issuing company
3. According to information managed by the highway company, the card issuing company uses the RSU exit’s public key, which is kept by the highway company, to verify the highway company’s revenue points and corresponding amounts through the blockchain
4. If the application is authentic, the card issuing company approves the application
5. All the RSU exits managed by this highway operation company obtain the same public key address assigned by the card issuing company
6. All the RSU exits of this highway operation company transfer the corresponding points to the card issuing company through the smart contract
7. The blockchain records the transaction described in step 6
8. The card issuing company sends the corresponding money to the highway company

4. **Implementation**

We established an Ethereum network to verify the proposed architecture and investigated its advantages.

4.1. **Development Platform.** We used MetaMask to simulate an Ethereum network. MetaMask is a bridge that links the distributed web of tomorrow with browsers of today. It allows Ethereum Apps working on existing browsers without running a full Ethereum node. MetaMask holds a secure identity vault, which allows users to manage their identities on different sites and to sign blockchain transactions.

We employed Remix IDE to develop blockchain applications. Remix is an open source tool written in Javascript. It can be used either in the browser or locally. Users of Remix can write Solidity contracts straight from the browser and test, debug, and deploy smart contracts and so on.

We also involved Go Ethereum (Geth) as the Ethereum debugging tool. Geth, a totally open source and licensed under the GNU LGPL v3, is designed to target Ethereum protocol.

4.2. **Implementation Example.** Figure 8 illustrates an implementation example of the proposed architecture. The most important example of the system implementation is the formulation of related smart contracts. Remix IDE is an online smart contract compilation, testing, and deployment tool. Therefore, the implementation logic and process of the blockchain-based ETC system in this paper are as follows.

In this implementation example, the value of each account is shown as follows:

1. **Account address:**
   - The RSU account value is “0xbfd4FaB042bF-B5a99EBf02DF0d877eBd2cA3a7a.” The user account value is “0x6b05bA24739E87093399e1A9c7E0382-0F0dC15AC.” The card company account value is “0xe08e93a12A3b2987a6aD8797bEE668b57d20b7c7.”
2. **User payment:**
   - When the user exits through the RSU, the exit will tell the user how much to pay, and then the blockchain base platform will execute the following code.

   ```
   Code 1: "Approved ("0xbfd4FaB042bF-B5a99EBf02DF0d877eBd2cA3a7a,” 50)."
   ```
   This means that the underlying platform of the blockchain approves the transfer of the corresponding points (price = 50) to the RSU account.
(3) User recharge:

When the user recharges the IC card, the basic blockchain platform will execute the following code.

Code 2: 

```
transferFrom("0x6b05bA24739E87093399e1A9c7E03820E0dC15AC," "0xbf4FDaB042bFB5a99EBf02fDF0d877eBd2cA3a7a," 50).
```

This means that the user account transfers the corresponding points (price = 50) to the RSU account. Then, the user leaves.

(4) Highway profit:

This part is paid by the card company, and the blockchain basic platform executes the following code.

Code 3: 

```
transfer ("0x6b05bA24739E87093399e1A9c7E03820E0dC15AC," 1000).
```

This means transferring the corresponding points (amount = 1000) to the user account. In this way, charging is completed.
Get the public key address of the card issuing company
Smart contract (point transaction)
Check the company's toll points
Apply for transferring points
Approve the application
Get the public key address of the card issuing company
Transfer money
Verification (receive points) writing (receipt record)

**Figure 7:** Point transaction between the card issuing company and RSU.

**Figure 8:** An implementation example of the proposed architecture.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>User account</td>
<td>0x60b5b2a2378e7093599e1a9c7e3b2a9a83c151c</td>
</tr>
<tr>
<td>RSU account</td>
<td>0x36f3d8042a859e9e6b2a22f0dd77c8d2ca37a</td>
</tr>
<tr>
<td>CIC account</td>
<td>0xe08e93a12a3b29876a6d38795b3e660b572d2b37c</td>
</tr>
<tr>
<td>Price</td>
<td>50</td>
</tr>
<tr>
<td>Amount</td>
<td>1000</td>
</tr>
<tr>
<td>Profit</td>
<td>50</td>
</tr>
</tbody>
</table>

Attention: All blockchain actions are recorded in blockchain
5. Discussion

5.1. Improved Efficiency. The operating mechanism of the blockchain creates trust. With this trust, there is no need for a centralized organization to endorse credit. The dual transaction of transactions can directly conduct peer-to-peer transactions on the basis of the credit created by the blockchain, eliminating the link of centralized organization.

In our decentralized architecture, firstly, since user and RSU are equivalent nodes in our architecture, a user can transfer points directly to an RSU, which means the user pays directly to the highway company. The payment process is simplified by removing the centralized settlement center. Second, since all the point transactions are recorded in the blockchain and secured by private-public keys and hash identities, it is extremely difficult to tamper or lose historical data. Third, point-to-point transactions greatly shorten settlement time between regions and avoid incompatibility between different ETC systems. Last but not least, all transactions are traceable and convenient for review, pushing corruption nowhere to hide. Therefore, our decentralized architecture improves ETC’s efficiency.

5.2. Improved Security

5.2.1. RSU Transaction Data Loss. RSU equipment works in a complex environment and is vulnerable to external influences, like car accident, natural disaster, and system failure. Once an RSU unit is damaged, data stored in it cannot be retrieved.

However, when a blockchain is employed in our architecture, all transactions are written into the blockchain in real time and gradually spread to each node of the entire network. In other words, each node holds a complete copy of all the toll information which means any damage of certain RSU equipment cannot lead to any real loss.

5.2.2. DDoS Attack. Distributed Denial of Service (DDoS) attack is launched by a network of malicious computers. They keep sending enormous garbage information to a target server, thus causing the target to be engaged with that garbage while fail to provide services for normal users. Once the ETC’s central server cannot defend DDOS, the whole system will be paralyzed.

Since the proposed blockchain-based architecture does not contain a central server, DDOS can only target a certain node, and the outcome is obviously small enough to lose the attackers interest.

5.2.3. Settlement Center Intrusion. The ETC systems are composed of several levels of local area networks and wide area networks. If a hacker successfully invaded an ETC central server and gained control, he could arbitrarily tamper the revenue data and perform various transfer and withdrawal operations, leaving no trace at all. Network attacks on a highly “centralized” settlement center will cause billions of transaction data to be lost or tampered with, and the consequences will be immeasurable.

In our architecture, each node is self-trust. If a hacker tampered data of several certain nodes, the entire system would not accept those data. Since most nodes are trustable, the main chain will extend much faster than the hacker’s fake chain. Only if the hacker controlled more than 50% of the nodes in the entire network, could he activate the tampered data. And the process of taking over control is too exhausted and could scare most hackers away.

Further, even if a hacker successfully falsifies the data, he cannot withdraw his accounts because it must be done at a recharge institution.

5.2.4. Swiping Forged Cards. In a traditional ETC system, the attack of swiping forged cards is more difficult to defend. For example, a fraud can use a POS machine to collect money without contact. When he is close to an ETC card that has activated “Quick Pass” function, at most 300 RMB will transfer from the ETC card to the fraud’s account without requiring a password or a consumer signature. The whole process is difficult to track.

Fortunately, our architecture can avoid this problem. Each transaction is confirmed and recorded in the blockchain. Only after the blockchain records an approval of transfer, the payment can be debited. In this way, not only the user needs to confirm the payment but also the payee information is also clearly recorded in the blockchain. The blockchain-based ETC system provides a user transaction query system, and the data are integrated with the non-tamperable feature of the blockchain, which can provide supporting services for audits, disputes, violations of laws, and regulations. Therefore, no one can secretly steal money from ETC cards.

5.3. Feasibility and Scalability. When we apply the proposed ETC architecture to the real network, we will use the private blockchain technology. Figure 9 illustrates the differences between private blockchain and public blockchain. In the private blockchain, there are two kinds of nodes, which are light nodes and full nodes. The light nodes only synchronize the block header information while the full nodes synchronize the block header information and block body information. And the full nodes can calculate the reliability of the transaction in the network. In other words, as long as more than 50% full nodes accept the transaction results, the entire system will accept those transaction data. Since the number of full nodes are controllable and do not expand indefinitely, the proposed ETC architecture will not require too much computing resources in a real network with large number of components. It proves the feasibility and scalability of the proposed ETC architecture.
6. Conclusion

Because of the high-centralized framework of the conventional ETC system, there are many potential security risks. In this paper, we propose a decentralized ETC architecture based on blockchain technology. We further verify its feasibility in a test network. Our architecture can effectively operate normal ETC services while avoiding most attacks that threaten traditional ETC systems. Moreover, our architecture does not significantly increase the amount of calculation, so it can also be applied in real networks. The proposed architecture provides a brand new way of conventional ETC system optimization.

In the future, we will further optimize the point transaction rules and standards and simulate attacks to verify the architecture’s ability of defending. And we also intend to replace proof-of-work with proof-of-stake for more efficient computing and storage costs.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Research Program of Shanghai Municipal Transportation Commission (JT2021-KY-005), National Key R&D Program of China (2016YFB1200402), National Natural Science Foundation of China (61703308), and Sichuan Province Science and Technology Program (2019YFG0040).

References


