TChain: A Privacy-Preserving Consortium Blockchain for Parking Charge Management

ZHE FENG

Department of Automation, Shanghai Jiao Tong University and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

LIJUN WEI

Department of Automation, Shanghai Jiao Tong University and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

YUHAN YANG

Department of Automation, Shanghai Jiao Tong University and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

JING WU

Department of Automation, Shanghai Jiao Tong University and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

CHENGNIAN LONG*

Department of Automation, Shanghai Jiao Tong University and the Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

With the rapid development of intelligent transportation system, parking charge management shows a trend of digitization and intelligence, which improves the efficiency and brings great convenience in parking charge service. Nevertheless, exposure of vehicle-track and traffic transaction information become potential threats that have been ignored by most parking management system. In building intelligent transportation systems, privacy and security issues should be addressed first. In this paper, we propose a hierarchical consortium blockchain TChain and build our practical solutions with parking charges as a typical scenario, which contains on-chain and off-chain ledger interaction model. Specifically, to prevent malicious collection and use of on-chain information, we introduce Pedersen commitment and Token mechanism to anonymize the content of blockchain data and conceal the relationships of transactions. Besides, we analyze and perform a series of vital experiments to verify the effectiveness and security of our proposed solution.

CCS CONCEPTS • Security and privacy • Systems security • Distributed systems security

* Corresponding Author: C. Long (Email: longcn@sjtu.edu.cn)

Additional Keywords and Phrases: Consortium blockchain, On-chain and off-chain interaction, Privacy preserving

1 INTRODUCTION

With the maturity of sensor, communication, edge computing and other emerging technologies, intelligent transportation systems (ITS) are rapidly developing, and provide convenience for people's lives and travel patterns [1, 2]. In ITS, various types of mobile sensor devices, vehicles, and roadside units can autonomously exchange and transmit messages in real time, which improves and promotes the efficiency of traffic information sharing, thus supporting the requirements of diversified transportation scenarios such as parking charging, vehicle tracking, and traffic dispatching [3].

However, with the increasing of the number of participating nodes and the intelligence of the devices, ITS may suffer some additional security risks. Specifically, some malicious vehicle nodes may steal the private information of other nodes in the process of interaction. In addition, some malicious attackers may disrupt the decision-making results of vehicle nodes through message tampering, identity forgery, etc. The above security risks may influence and reduce the trust and cooperation among nodes. Therefore, it is important and imminent to construct a secure and reliable interaction mechanism for data and identity protection.

Blockchain technology, as a distributed ledger technology, has excellent properties such as tamper-resistance and traceable, which can help the data security for intelligent transportation system. First of all, the unique chain data storage form of blockchain can ensure the strict chronology of transportation big data, thus ensuring the standardization of data. In addition, the blockchain can promote multiparty cooperation and motivate users to participate in the synchronization and maintenance of the network; Moreover, the combination of hash functions and distributed ledgers [4] allows for fast discovery and access to information on the blockchain, improving the efficiency of interactive services. Specifically, Lun's CreditCoin [5] adopt anonymous vehicular protocol, Lei propose a framework for providing secure key management based on blockchain [6], and Islam propose to use blockchain to implement attribute-based access control for IoT [7]. However, due to the openness of the blockchain system itself, the security of the on-chain data is still not well solved. All transactions in the blockchain, including the flow of assets and transaction amounts between pseudonymous users, are exposed in plaintext on the blockchain. A malicious attacker can analyze the patterns of the on-chain data to infer the real identity information and behavioral characteristics of the nodes. To solve the problem above, we propose TChain to protect data privacy, integrity and confidentiality. TChain is developing a pluggable streaming consensus protocol with system engineering optimization underlying the framework of FISCO-BCOS [8]. In order to improve the secure access and cross-domain authentication of large-scale IoT devices, TChain proposes a distributed CA-PKI architecture based on blockchain and a trusted device technology based on hardware security. In this paper, we mainly study on-chain data privacy preserving and verifiable issues in TChain. We choose parking charges as a typical scenario, where the users' identity and the parking charge data are packed and uploaded to the blockchain in plaintext. To solve the problem of information exposure of parking managers, we upload data to the blockchain using Pedersen commitment and Token to hide the number of transactions and transaction flow, and the organizations can use Token to perform asset verification.

Our work makes the following contributions:

•We propose a hierarchical architecture for transportation consortium blockchain, including fast consensus algorithms, trusted identities, distributed PKI systems, on-chain and off-chain collaboration.

•We propose a new ledger structure and data flow for the entire parking charge process, which ensures the security of on-chain and off-chain data for the parking charge scenario.

•We construct a theoretical validation model based on Pedersen commitment [9], and design a mechanism to issue Token to organizations. It guarantees the privacy preserving of on-chain ledger and achieves the verifiability.

The remainder of this paper is organized as follows. Section 2 reviews system overview. The ledger structure and transaction flow are introduced in Section 3. Discussion about the proposed system is given in Sections 4, respectively. Finally, Section 5 concludes this paper.

2 SYSTEM OVERVIEWS

2.1 TChain Architecture

TChain is a three-layer transportation consortium chain architecture: *base layer*, *middle layer*, and *interface layer*, as shown in Fig. 1.

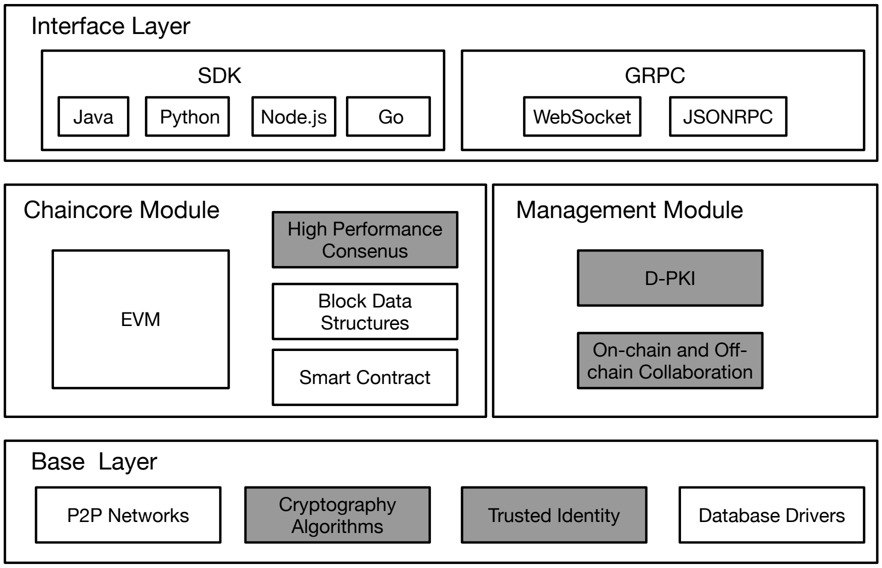


Figure 1: TChain-transportation consortium blockchain component architecture.

Base layer provides the foundation for network communication, encryption algorithms, underlying data management, and trusted identities. Trusted identity is an important component to ensure device access security and the authenticity and integrity of off-chain data. It is a combination of software and hardware security technologies, such as PUF-based device identity [10] and multi-factor authentication [11].

Middle layer is composed of chaincore module and management module. Chaincore module provides smart contract execution environment, on-chain storage data structures, and consensus algorithm. In terms of consensus algorithm, TChain is developing a full-stack optimized streaming consensus protocol to reduce the communication complexity to *O(n)* by using multiple signatures to achieve a linear communication complexity [12]. The management module includes distributed key management and on-chain and off-chain data interaction. We provide support for distributed CA-PKI systems to evolve on the centralized and hierarchical architecture of CA-PKI, solving the complexity of single point of failure and multiple cross-certificate management. For on-chain and off-chain data interaction, we propose a private and public ledger model. Private data is stored in the off-chain private ledger and the hash value of private data is stored in the on-chain public ledger. On-chain transaction data is encrypted using Pedersen commitment and Token, protecting the amount of transaction while protecting the relationship between participants.

The interface layer provides external access to the blockchain, with two types of invocations: SDK and GRPC. SDK supports multiple programming languages to interact with the blockchain, including Java, Python, Node.js, and Go. GRPC supports the websocket protocol and connection in accordance with the JSONRPC specification.

2.2 Parking Charge

Parking charge is a vital part in the intelligent transportation system, which requires related parking data (e.g., parking time and the individual information of users) to help to perform parking data storage and parking payment. However, the parking charge process may disclose personal individual information due to the lack of privacy preserving mechanism. We use the parking charge scenario to fully illustrate the on-chain and off-chain integration process, as shown in Figure 2.

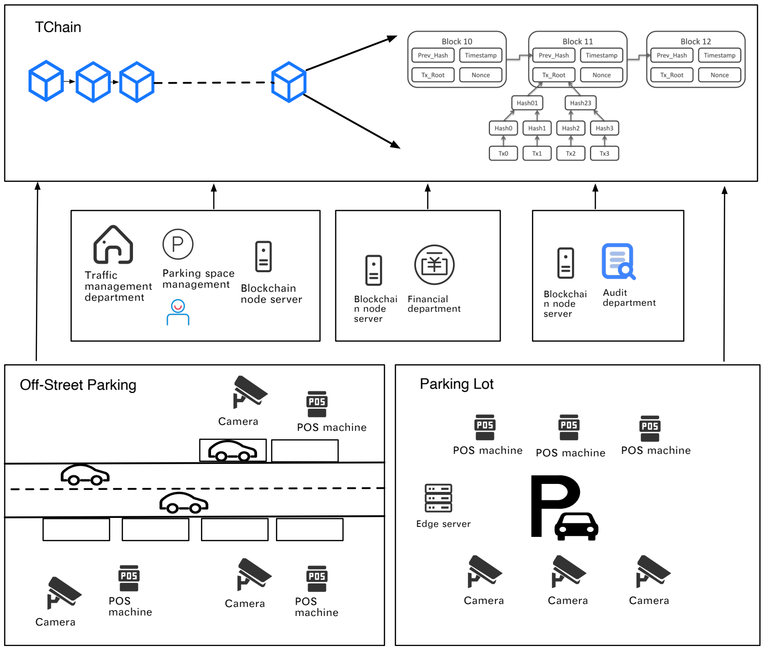


Figure 2: Parking charge scenario.

Nodes at the edge consists of camera nodes and POS machine nodes, both on-street distributed and in parking lots. The camera collects information such as car number plate and parking time, the POS machine provide transaction information such as parking fee.

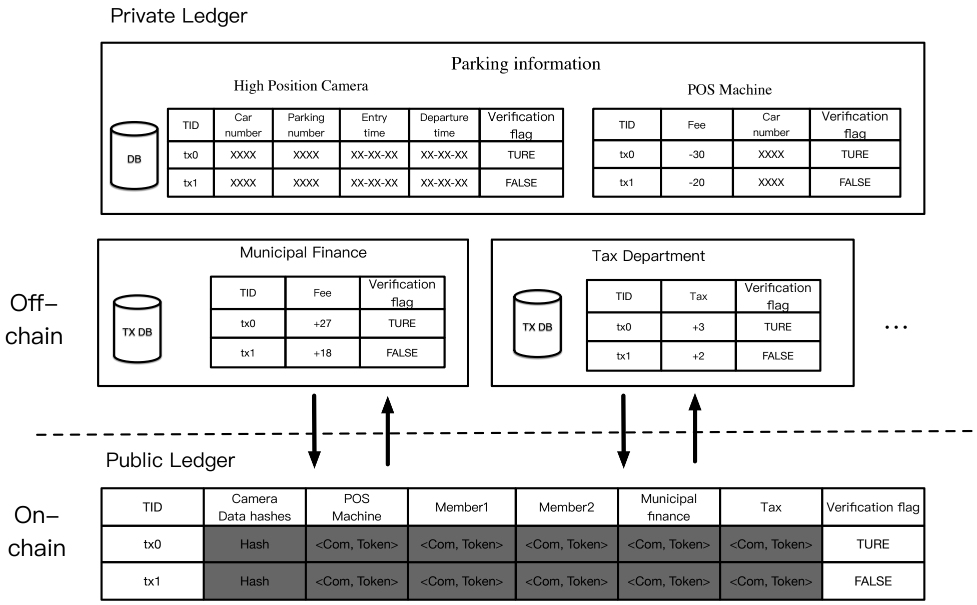
Organizations involved in the parking charge process includes transportation management department, finance department, and audit department. The transportation management department dispatches fee collectors and manages the transportation flow, and the finance department collects parking fees. Considering the data security and privacy preserving requirement in the parking charge scenario, the confidentiality of the transaction flow and the parking fee should be guaranteed.

Tchain uses public ledger and private ledger to store on-chain and off-chain data respectively. TIDs are created after a camera node finds a car parked in a parking space, and after the car leaves the parking space. Edge server calculates parking fees from parking time. After that, the POS machine gets the fee to be charged. The car number plate and parking time are recorded in the off-chain private ledger, and the fingerprint hash of the data is stored in the on-chain ledger. The parking fees provided by the POS are encrypted and stored in the on-chain ledger, and the verification flag is set to TURE in the public ledger after each institution verifies that the amount is correct.

3 ON-CHAIN AND OFF-CHAIN COLLABORATION

3.1 Ledger Structure

The data in the consortium blockchain is divided into private data stored locally and public data stored on the chain. There are two types of data ledgers in TChain: private ledger and public ledger. Private ledger is kept autonomously by each organization and stores private information in plaintext. The public ledger records the hash of the credential data and the encrypted transactions that occurred between organizations, and stores verification information. The structure between public ledger and private ledger is shown in the Fig. 3.



TID	Car number	Parking number	Entry time	Departure time	Verification flag
tx0	XXXX	XXXX	XX-XX-XX	XX-XX-XX	TURE
tx1	XXXX	XXXX	XX-XX-XX	XX-XX-XX	FALSE

TID	Fee	Car number	Verification flag
tx0	-30	XXXX	TURE
tx1	-20	XXXX	FALSE

TID	Fee	Verification flag
tx0	+27	TURE
tx1	+18	FALSE

TID	Tax	Verification flag
tx0	+3	TURE
tx1	+2	FALSE

TID	Camera Data hashes	POS Machine	Member1	Member2	Municipal finance	Tax	Verification flag
tx0	Hash	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	TURE
tx1	Hash	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	FALSE

Figure 3: Private ledger and public ledger.

3.1.1 Private Ledger

In order to protect the private information of users within the parking charge scenario, such as transaction amount and parking entry and exit times, the private information is recorded in a private ledger of the off-chain organization, and the private information plaintext is stored locally at the node. Each local parking management agency, such as roadside parking or factory garage parking operation company, manages parking data and transaction data generated by high position cameras and POS machines under its jurisdiction. Moreover, the municipal finance department stores the amount received from this transaction, and the tax department stores the amount of taxes and fees collected. This information is linked by a TID, which is synchronized by the interaction between the off-chain private ledger and on-chain public ledger. In addition, each private ledger has a validation flag.

3.1.2 Commitment Encryption

In order to protect transaction information (e.g., sender, recipient, transaction amount and relationship of senders and recipients) between organizations, TChain uses Pedersen commitment [9]. Pedersen commitment satisfies computational binding and homomorphic addition functions, enabling verification of transaction data while protecting privacy.

Let g and h be two random generators of a cyclic group G with $\mathrm{s} = |\mathrm{G}|$ elements. Select the value to be kept confidential $\mathrm{m} \in \mathrm{Z}_p$, then pick a random number $\mathrm{r} \in Z_p$,

$$\mathrm{Com} = \mathrm{com}(\mathrm{m}, \mathrm{r}) = \mathrm{g}^{\mathrm{m}}\mathrm{h}^{\mathrm{r}}. \tag{1}$$

After generating a Pedersen commitment, the recipient reveals nothing from the commitment about the amount of the transaction m. If the sender can find different m and m' both of which open the commitment, $\mathrm{g}^m h^r = \mathrm{g}^{m'} h^{r'}$ is equivalent to solving $\log_g(h) = \frac{m'-m}{r-r'}$. We assume discrete logarithm is hard, the recipient cannot open the commitment using m'.

Pedersen commitment is satisfying homomorphic addition, which can use encrypted data for computing in validating transactions and organization's revenue and expenditure. Rule for homomorphic addition is as follows:

$$\mathrm{com}(\mathrm{m}_1, \mathrm{r}_1) \cdot \mathrm{com}(\mathrm{m}_2, \mathrm{r}_2) = \mathrm{com}(\mathrm{m}_1 + \mathrm{m}_2, \mathrm{r}_1 + \mathrm{r}_2). \tag{2}$$

Com acts as a proof to ensure that the values of expenses and income within the transaction are conserved and that no one fudges the amount or steals the funds. Formally, the transaction amount should satisfy $\sum_{k=1}^{N} m_k = 0$. Using homomorphism and setting $\sum_{k=1}^{N} r_k = 0$ in advance, the verifier can ensure that the Com of a row satisfies

$$\prod_{\mathrm{k}=1}^{\mathrm{N}} \mathrm{Com}_{\mathrm{k}} = 0. \tag{3}$$

3.1.3 Token Verification

Organizations get nothing from Commitment about the number of transactions. The organization as a participant in the transaction needs to ensure that the amount recorded in the Com on the public ledger is consistent with the actual revenue and expenses. As a non-transactional sender, other organizations only know the Com, g and h about the transaction. The recipient of the transaction has already obtained the amount of revenue off-chain, and the ledger on-chain serves as a record and audit. To keep the data consistent across Com in the ledger, each organization issues Token when a transaction is generated,

$$\mathrm{Token}_i = pk^{r_i}. \tag{4}$$

In the equation, pk is the public key of the organization and sk is the private key, Pk is generated as $\mathrm{pk} = \mathrm{h}^{sk}$, r and h are the same as in the Pedersen commitment. From an organization's point of view, each transaction receives a corresponding Token. Organizations can perform individual validation for each transaction or use batch validation to improve efficiency. The following shows the process of batch validation, of which individual transaction validation is a simplified version. M is the actual amount received by the organization and m is the amount recorded in Com,

$$\mathrm{s} = \prod \frac{Com_i}{g^{M^i}}, \tag{5}$$

$$\prod Token_i = pk^{\sum r_i} = h^{sk \sum r_i} = (\prod \frac{Com_i}{g^{m_i}})^{sk} = s^{sk}. \tag{6}$$

If $M^i = m^i$ holds, we can get $\prod Token_i = (\prod \frac{Com_i}{g^{m_i}})^{sk} = (\prod \frac{Com_i}{g^{M^i}})^{sk} = s^{sk}$. We only need to verify $\prod Token_i = s^{sk}$ to guarantee $M^i = m^i$.

3.1.4 Public Ledger

In order to consensus and validate the transaction, encrypted transaction information need to be upload in the public ledger. The car number and parking time information is stored in off-chain database, while they need to be hashed and recorded on the blockchain to ensure that the off-chain data has not been tampered with. Each organization involved in a parking transaction stores $< \mathrm{Com}, \mathrm{Token} >$ in the public ledger, which is the encrypted information needed to validate each transaction and each organization's transaction amount, respectively. Therefore, the public ledger has a transaction validation flag of TURE after transaction balance validation (Equation (1)) and amount validation of each organization (Equation (2)).

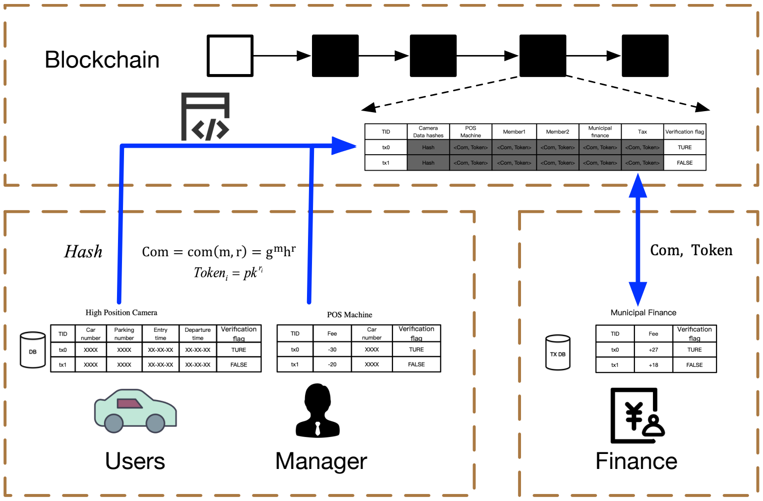
As shown in the Fig. 3, the shaded part of the public ledger is the encrypted content, and the amount of fees in each transaction is positioned negative and the amount of income is positive. Assuming the tax rate is ten percent, the POS node in $\mathrm{tx0}$ contributes 30 in place of the user, paying 3 in taxes fiscal revenue of 27. The number of transactions is -30, $+3$ and $+27$. All the Com in the transaction are used to verify that the amount of the transaction in $\mathrm{tx0}$ is correct.

For organizations that do not participate in the transaction, the amount of the transaction is set to 0 and the corresponding commitment is also generated. This ensures that the sender and recipient of the transaction cannot be known from the public ledger. The preserving of the transaction relationships further improves privacy.

TChain creates transactions based on transactional smart contracts deployed on the blockchain, and the process of generating Com and Token is generated by additional contracts, thus ensuring that non-interactive zero-knowledge proof [13] are given without the need to make changes to the original system. The smart contracts cannot be modified after deployment, which ensures that the encryption process cannot be modified by malicious nodes.

3.2 Privacy-preserving Transaction

In TChain, privacy-preserving transactions take place between the parking manager and the finance department. Users' privacy information is stored in the parking manager's private ledger and stored on the blockchain after generating data fingerprint using hash. The interaction of organization is shown in Figure 4.



TID	Camera Data hashes	POS Machine	Member1	Member2	Municipal finance	Tax	Verification flag
tx0	Hash	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	TURE
tx1	Hash	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	<Com, Token>	FALSE

High Position Camera

TID	Car number	Parking number	Entry time	Departure time	Verification flag
tx0	XXXX	XXXX	XX-XX-XX	XX-XX-XX	TURE
tx1	XXXX	XXXX	XX-XX-XX	XX-XX-XX	FALSE

POS Machine

TID	Fee	Car number	Verification flag
tx0	-30	XXXX	TURE
tx1	-20	XXXX	FALSE

Municipal Finance

TID	Fee	Verification flag
tx0	+27	TURE
tx1	+18	FALSE

Figure 4: Interaction in privacy preserving transactions.

The payment parking transaction information use a cryptographic smart contract to calculate Com and Token, and then the transaction information is stored on the blockchain public ledger using hash, $<\mathrm{Com},\ \mathrm{Token}>$ (see Figure 5).

Preparation: First, the amount of each organization in this transaction are determined based on parking fee and tax rate, with 0 for organizations not involved in the transaction, and N (the number of Organizations in Blockchain network) random numbers is generated for encryption.

Execution and validation: During cryptographic operations, calculations are performed on all organizations on TChain, thus hiding the sender and the recipient of the transaction. After performing the encryption operation, the calculated $<\mathrm{Com},\ \mathrm{Token}>$ is placed in the public ledger. After that, we use commitment to verify the balance of the transaction amount.

Consensus: Transactions for consensus in the public ledger are sent to each organization and after that each organization uses Token to verify the organization amount. After verifying that the amount in the commitment matches the actual amount received, the validation flag is set to TRUE.

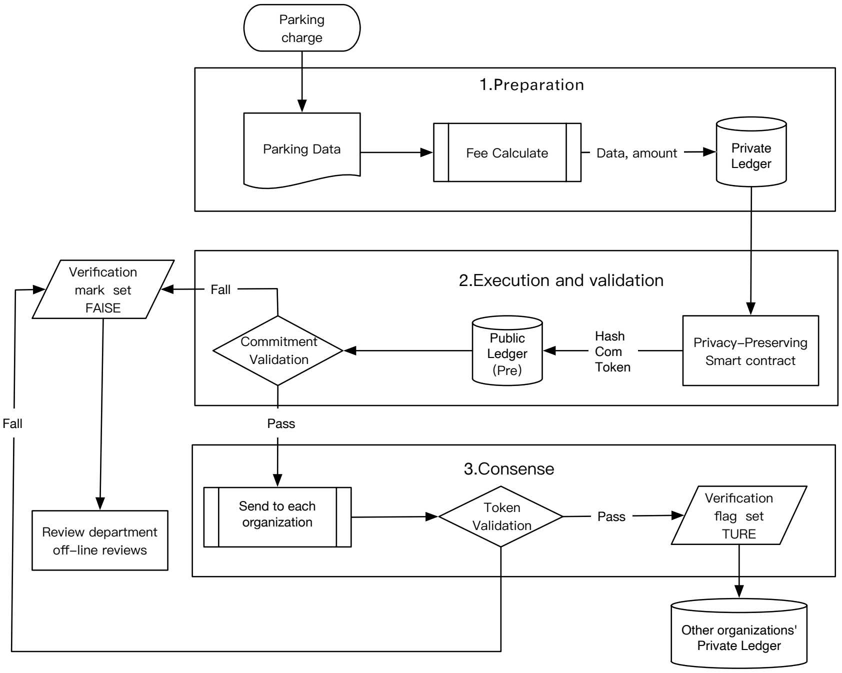

Parking charge
1.Preparation
Parking Data
Fee Calculate
Data, amount
Private Ledger
2.Execution and validation
Verification mark set FAISE
Fall
Commitment Validation
Public Ledger (Pre)
Hash Com Token
Privacy–Preserving Smart contract
Fall
Pass
3.Consense
Review department off–line reviews
Send to each organization
Token Validation
Pass
Verification flag set TURE
Other organizations' Private Ledger

Figure 5: The flow of privacy preserving transactions.

4 PERFORMANCE EVALUATION

In this section, we evaluated the performance of the TChain system. We demonstrate this in two aspects:(1) Time cost of using privacy preserving and auditing transactions, and (2) the guarantee of a certain throughput to support parking charge transactions.

We develop and configure smart contracts in TChain. In order to analyze the impact of privacy preserving, this experiment uses a stand-alone deployment so that network time delay is not considered. Nodes on the blockchain network are distributed in docker containers on a single host. We use Golang to build privacy-preserving smart contracts, which are deployed on the blockchain network. And we wrote the client application using Node.js to invoke the contract implementation. We used Caliper-benchmark on a VM (virtual machine) running ubuntu 16.04 with 1.9GB of RAM and a quad-core Intel i5 1.4GHZ CPU.

4.1 Time Cost and Throughput

We conducted 10 rounds of experiments, sending 10000 transactions per round, at a sending rate of 1000 TPS (transaction per second). TChain maintains a throughput of 338 TPS at a network size of 8 nodes. Table 1 shows the time taken comparison between plaintext record and our privacy-preserving transaction for each step in a non-privacy preserving asset transfer transaction.

Privacy-preserving transactions add the process of generating Com and Token. In addition, the transaction balance verification based on commitment and the organization amount verification based on Token are added to the verification transaction process.

Table 1: The time of transactions.

Notation	Definition	Time1(ms): plaintext	Time2(ms): encrypted
$T_{commitment}$	The time of generation of the Pedersen commitment	-	2.3
T_{token}	The time of generation of the Token	-	2.6
T_{cont_tx}	The time for execute parking charge transactions	43.2	42.2
T_{cont_ver}	The time of validating transactions	28.3	35.3
T_{block}	The time of sorting and packing into blocks	81.0	85.0

The encrypted computing and additional authentication process with an added latency is less than 8%, and the main latency is due to the block transaction order verification and changes to the state of the ledger. There is also network time delay in the production environment, so that the proportion of delay caused by Com and Token encryption is smaller in the overall transaction flow. In addition, TChain guarantees a certain throughput while ensuring data security and privacy through homomorphic encryption. TChain can reach 298 TPS in the 8-node network. For a parking system, a throughput of around *200* is sufficient for proper operation.

4.2 Security Analysis

Privacy Preserving: In order to protect the details of transactions on the blockchain from being accessed by malicious nodes. Pedersen commitment is generated for all members of the consortium blockchain, whether they are transaction participants or non-participants, and the transaction relationships and transaction amount are not accessible from the information in the public ledger.

Auditable: For the auditing of encrypted transaction data, we use Pedersen commitment that satisfies homomorphic addition. Information on the amount of the transaction can be verified for balancing. From an individual organization’s perspective, Token are used to ensure that the amount encrypted on the public ledger is the same as the amount encrypted on the private ledger. In this way, the encrypted information on the TChain can be audited.

5 CONCLUSION

In this paper, a hierarchical consortium blockchain TChain is proposed for parking charge scenario, wherein we design the on-chain and off-chain ledger interaction model to facilitate the charge services. We introduce Pedersen commitment to anonymize the content of blockchain data and conceal the relationships of transactions, which avoids the exposure of vehicle-track and traffic transaction information. To evaluate the performance of our proposed scheme, we deploy experiments using Caliper, and the result shows that the latency caused by the additional privacy preserving mechanism is marginal. Moreover, the throughput of the system is sufficient to support the normal operation of parking charge service, hence the feasibility is guaranteed.

ACKNOWLEDGMENTS

This work was supported in part by the Science and Technology Commission, Shanghai Municipality under Grant 19511102102; in part by the Shanghai Automotive Industry Technology Development Foundation under Grant 2008; and in part by the NSFC under Grants 62073215, 61873166, and 61673275.

REFERENCES

[1] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. 2016. Edge computing: Vision and challenges. IEEE Internet of Things Journal. 3, 5 (October 2016), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

[2] Zhang, J., Wang, F. Y., Wang, K., Lin, W. H., Xu, X., & Chen, C. 2011. Data-driven intelligent transportation systems: A survey. IEEE Transactions on Intelligent Transportation Systems. 12, 4 (December 2011), 1624-1639. https://doi.org/10.1109/MCOM.2009.5307471

[3] Hartenstein, H., & Laberteaux, L. P. 2008. A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine. 46, 6 (June 2008), 164-171. https://doi.org/10.1109/MCOM.2008.4539481

[4] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. 2018. Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering. 30, 7 (July 2018), 1366-1385. https://doi.org/10.1109/TKDE.2017.2781227

[5] Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., & Zhang, Z. 2018. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems. 19, 7 (July 2018), 2204-2220. https://doi.org/10.1109/TITS.2017.2777990

[6] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. 2017. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal. 4, 6 (December 2017), 1832-1843. https://doi.org/10.1109/JIOT.2017.2740569

[7] Islam, M. A., & Madria, S. 2019. A permissioned blockchain based Access Control System for IOT. In 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, Atlanta, GA, USA, 469-476. https://doi.org/10.1109/Blockchain.2019.00071

[8] FISCO Core Group. FISCO-BCOS. FISCO open source working group. https://github.com/FISCO-BCOS

[9] Pedersen, T. P. 1991. Non-interactive and information-theoretic secure verifiable secret sharing. In Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 129-140. https://doi.org/10.1007/3-540-46766-1_9

[10] Su, Y., Wu, J., Long, C., & Wei, L. 2020. Secure Decentralized Machine Identifiers for Internet of Things. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT). ACM, Hawaii, USA, 57-62. https://doi.org/10.1145/3390566.3391670

[11] Huang, X., Xiang, Y., Bertino, E., Zhou, J., & Xu, L. 2014. Robust multi-factor authentication for fragile communications. IEEE Transactions on Dependable and Secure Computing. 11, 6 (November 2014), 568-581. https://doi.org/10.1109/TDSC.2013.2297110

[12] Yin, M., Malkhi, D., Reiter, M. K., Gueta, G. G., & Abraham, I. 2019. Hotstuff: Bft consensus with linearity and responsiveness. In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing (PODC '19). ACM, Toronto, Canada, 347-356. https://doi.org/10.1145/3293611.3331591

[13] Rackoff, C., & Simon, D. R. 1991. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Annual International Cryptology Conference (CRYPTO '91). Springer, Berlin, Heidelberg, 433-444. https://doi.org/10.1007/0-387-34805-0_19

Authors' background

Your Name	Title*	Research Field	Personal website
Zhe Feng	**Master student**	**Blockchain technology, digital Identity and network security.**	
Lijun Wei	**PhD candidate**	**Blockchain technology, trust management and IoT architecture and application.**	
YuHan Yang	**PhD candidate**	**IOT security, mobile edge computing and blockchain technology.**	
Jing Wu	**Associate professor**	**Robust model predictive control, security control, and stability analysis and estimations for cyber-physical systems.**	

Chengnian Long	**Full professor**	**Internet of Things and blockchain technology, cyber-physical systems security, and smart wireless systems.**	http://automation.sjtu.edu.cn/ShowPeople.aspx?info_id=1634&info_lb=590&flag=98