A Blockchain-based Data Sharing Platform for Smart Cities

Wenqi Zheng

Department of Computer, Institute of Logistics and Big Data, Zhejiang
Zhejiang Gongshang University Hangzhou College of Commerce, Hangzhou, China

Email: 17326062770@163.com

Abstract. With the development of technology, big data applications have gradually penetrated the scope of smart cities. Therefore, building a new type of Smart City is essential to optimize the national governance system and its capacity. That requires the cooperation of all government sectors to form a positive incentive mechanism for information sharing. However, the massive amount of social operations data raises several issues, such as data islands, inconsistent data standards, data privacy, and security to smart city data governance. Hence, this paper proposes a data collaborative governance method based on blockchain and secure multi-party computing in a trusted execution environment, and incorporates it in designing a data-sharing platform for Smart Cities. The results of pressure tests showed that the functions of each module could operate normally, which were aligned with expectations. This design enables innovative urban governance and alleviates the security and privacy issues in traditional Smart Cities. Therefore, the proposed platform stands highly promising for optimizing data governance in Smart Cities.

Keywords: Blockchain; Smart Cities; Data Governance; Data Sharing

1 Introduction

Smart city is the embodiment of data-driven urban decision-making mechanism in urban management. In the construction process, various resources in the city need to be mobilized based on real-time dynamic data to realize the information of city operation. With the gradual improvement of the city structure, the traditional big data platform cannot classify and integrate the city information. At this stage, the construction of smart cities is based on the original Internet facilities and the emerging Internet of Things (IoT) facilities, which is far from the ecological structure of smart cities. Therefore, the integration and maturity of IoT is insufficient. Data inaccuracy is often a result of uneven data structure, duplicate entries, outdated information, human error, and data islands in data collection and usage. This problem makes it difficult to dig out valuable conclusions. At the same time, various platform systems face challenges

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 75–85, 2022.
https://doi.org/10.2991/978-94-6463-108-1_10

in working together, inefficient data exchange, and insufficient data encryption protection. Therefore, all these problems are yet to be solved in the development of smart cities.

Blockchain is a distributed ledger of transactions or events, recorded and stored in blocks linked using encryption technology. These records are shared and monitored by all network nodes and updated only by miners, which are nodes with powerful computing resources that validate new transactions and record them in the ledger. As shown in Figure 1, the blockchain is composed of blocks holding timestamps of transactions, where each block is connected to the previous one. In a blockchain, a single point of failure does not interrupt normal functions due to its information distribution across the network. It is decentralized, traceable and tamper-proof. It can eliminate the drawbacks of centralized data market, provide system security, user behavior traceability and audit procedures, and provide strong guarantees for smart cities.

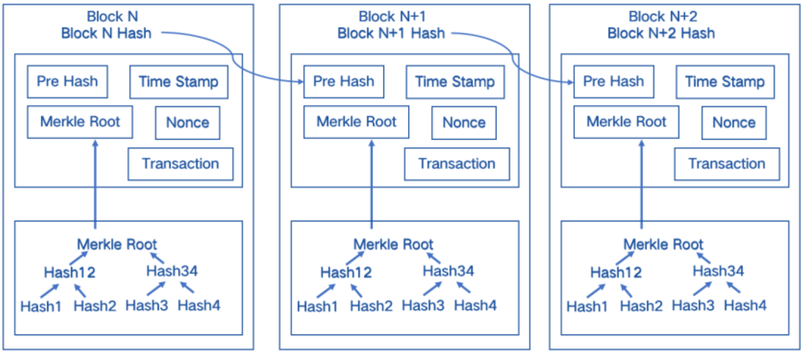

Fig. 1. The structure of blockchain

2 Related work

To solve the above-mentioned problems in smart cities, many solutions for various industries in towns and cities have been proposed [1]. Zhang et al. proposed a cross-chain vehicle networking model based on Ethernet blockchain, Internet of Things, and reputation computing algorithms [3].Zeng et al. proposed a food safety traceability system based on IoT and blockchain [5].Wu et al. proposed an IoT and blockchain-based agricultural product tracking application [6].Shen et al. proposed a blockchain-based food traceability storage system [7].Bocek et al. proposed a medical supply chain tracking system [8].Ferrag et al. proposed a blockchain-based deep learning framework, DeepCoin, for smart grid development [9].Hardjono et al. proposed an autonomous blockchain-based interoperable architecture system [10].Geneiatakis et al. deployed a blockchain-based cross-border e-government commodity transaction service [11].Meng et al. proposed a blockchain-based healthcare trust management system to reduce insider attacks on healthcare IoT and improve malicious behavior detection [12].Zhao et al. proposed a blockchain-resident on the blockchain as a framework transformation scheme for a new food distribution traceability platform [4].

Scholars have also done some explorations to improve the performance of blockchain systems. Xu et al. proposed a data-driven credit evaluation scheme running on blockchain with cross-chain architecture to make the supply chain system more secure and intelligent [2]. Mcghin et al. studied the omissions in blockchain systems such as mining incentives, mining attacks and key management and explored the application in healthcare [14]. Lao et al. analyzed the architecture of popular IoT blockchain systems and provided a suitable traffic model for IoT blockchain [13].

Current studies prefer to use blockchain systems to improve the traceability and security of product information. Less research has been conducted on the overall design of smart cities. Therefore, this paper seek to integrate existing studies to design a more comprehensive management system for the management and operation of smart cities to meet the requirements of different participants in towns and cities and promote sustainable urban governance.

3 System design

Table 1 shows that the smart education system has three main roles: system administrator, government, and business.

Table 1. System Roles

System User Role	**Responsibilities Description**
System administrator	Responsible for managing users, system users, configuring permissions, etc.
Government	Administrative jurisdiction, query data information, etc.
Enterprise	Upload data information, etc.

3.1 System Requirements Design

Requirements analysis is an important part of system development, which ensures the integrity and stability of system functions. The smart education system mainly includes system administrators, government, and enterprises. The smart city system mainly assists in controlling the operation of various industry sectors in the city before, during and after the implementation of different policies. When designing the system structure, its needs can be analyzed from the perspectives of the government, enterprises and system administrators.

From the government's point of view, their primary needs are as follows.

(1) To understand the operation of education, medical care, transportation, and government services in the subdivisions or smaller units in the jurisdiction they manage, so as to provide reference for the subsequent release of decisions.

(2) To be able to issue decisions, suggestions and messages on the operation of enterprises and streets within the jurisdiction.

(3) Uploads the operation status and decision making in the jurisdiction to the system for inspection by higher-level leaders.

(4) It is possible to trace the source of various operation conditions in the jurisdiction to avoid malicious tampering of data and shirking of responsibility.

From the business perspective, the main requirements are as follows.

(1) To receive timely decisions and suggestions from the government and related agencies.

(2) The company's tax and operation data can be uploaded to the system for inspection by higher management.

(3) To be able to communicate with other companies and call relevant data through third-party platforms without acquiring each other's data resources and return the results they need.

From the system administrator's point of view, the main requirements are as follows.

(1) Management and audit of each user's role and division of different permissions.

(2) Maintenance of the management system.

3.2 System structure

The smart city system designed in this paper incorporates blockchain technology. Figure 2 shows the architecture of the system. In this system, all entities of the smart city, such as transportation department, education department, and justice department, have their own industry databases. The servers loading data information in the departments can be set up as Smart City Alliance nodes, and each node decides whether to pass. over authorization to join the federation chain and have the unique bookkeeping rights. These nodes package the relevant information of the local industry database, such as data description, data exchange and data operation, into blocks according to a unified standard, and then participate in the blockchain consensus through the blockchain client. Finally, smart contracts are used to reach agreements for inter-departmental business exchanges.

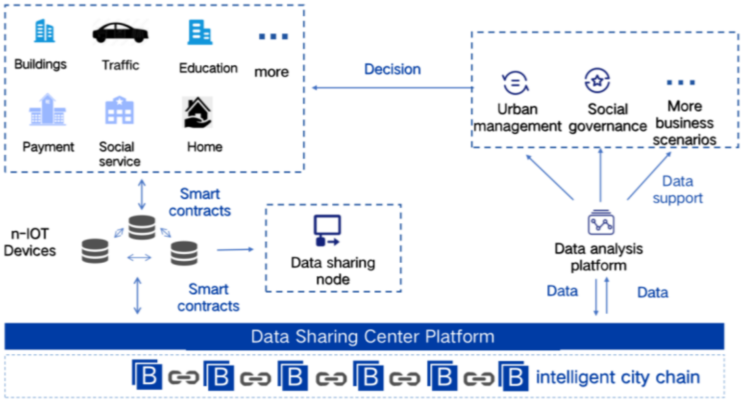

Fig. 2. Structure of Smart City Chain.

When departments need to use data from other departments, they only need to view the descriptive information of relevant data resources through the data sharing platform, write calculation and analysis algorithms, and then apply for database interface calls. After obtaining permission, they can obtain the results of other departments. The analysis results can be used as a reference to assist in urban governance decisions. As decisions are released, they will continue to influence city management. Through continuous updates from each consortium node, the system will generate new data reports to give government departments appropriate feedback to optimize management decisions, forming a positive closed loop. It promotes the development of intelligent services such as innovative medical care, competent transportation, innovative education, competent public security, and intelligent taxation, ultimately realizing the sustainable development of smart cities.

4 Implementation Details

4.1 System modular design

The proposed system can be divided into five main layers: the physical layer, the protocol layer, the cross-chain protocol layer, the off-chain extension layer, and the application layer. Figure 3 shows how they are organized.

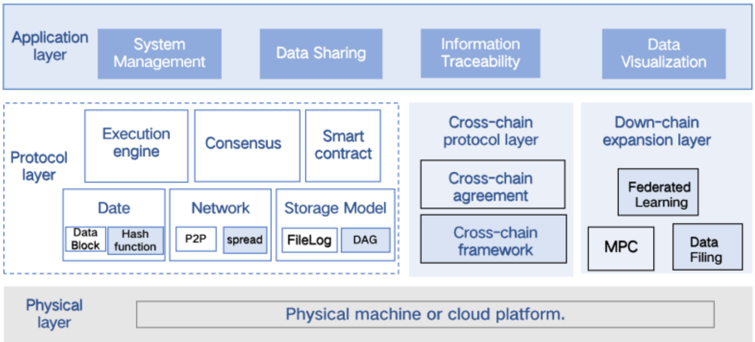

Fig. 3. The design of system modular

4.2 Physical layer

The physical layer mainly includes physical machines, cloud platforms, etc. to ensure standard transmission of data information on various physical media.

4.3 Protocol layer

The protocol layer includes execution engine, consensus algorithm, block data information, network, storage, etc. Among them, the data module is mainly responsible for storing blockchain and relational database. At the same time, it realizes the complete encryption of "massive data - block data chain". The network module identifies the "point-to-point" type of information dissemination and verification, and the consensus module "chains" various types of "consensus" and algorithms in one node type. The incentive module centralizes the economic mechanisms of issuance and distribution into the dissemination ecology. The contract module utilizes the RPC interface provided by web3.js to bridge the service layer and blockchain facilities for intelligent tamper-proofing, and finally into the secure and trusted application layer. In this context, consensus refers to the process protocol for reaching consensus. In a traditional organization, the leader makes a decision and then sends it to the rest of the team. Meanwhile, a blockchain system does not need a leader only when all stakeholders reach an amicable agreement. Executing a decision or a transaction requires an amicable conclusion or an acceptable solution from all stakeholders. Here, nodes with different roles can participate in consensus and they are free to enter, exit and query the services provided by the entire infrastructure. Each entity is responsible for managing their nodes in the framework. Upon entering the system, they need to make an offline application and then receive the necessary registration information from the management body.

4.4 Cross-chain layer

The cross-chain protocol layer provides interfaces and tools for implementing cross-chain transactions.

4.5 Offline expansion layer

The offline extension layer includes secure multi-party computing and data archiving to assist in data co-computation, while archiving redundant data to reduce the storage burden of blockchain nodes and improve the operation speed of the smart city chain.

4.6 Application layer

The application layer provides high-level services for users and mainly uses Node.js technology to implement the main service logic. It includes five modules: system management, intelligent supervision, auxiliary decision-making, information tracing, and data visualization.

(1) System Management Module

The system management module protects the system boundaries and ensures that information flows only between authenticated partners. This module is responsible for system administrator identity verification, supply chain participants' independent registration, permission management, information editing, participation and withdrawal, information broadcasting, etc. After logging into the system administration module, the administrator can assign and authorize roles to different participants in the supply chain and complete the authentication process so that each participant can flow correctly through the supply chain. When participants want to stop receiving services from the platform, they can delete them in this module. Also, administrators can publish messages that are visible to all participants on the forum.

(2) Information Traceability Module

The information tracing module mainly provides information recording and query functions. This module records information of different links of smart city respectively, including information uploading record, information use record, information inquiry record, information operation record, information circulation record, etc. Each subordinate module has some key parameters that need to be signed by the responsible parties. After being stored on the blockchain, the system can verify its validity. It provides functions such as information inquiry, responsibility assignment, and account management for different participants such as government, users of each department, and managers to make the system retrieval credible.

(3) Data Sharing Plan

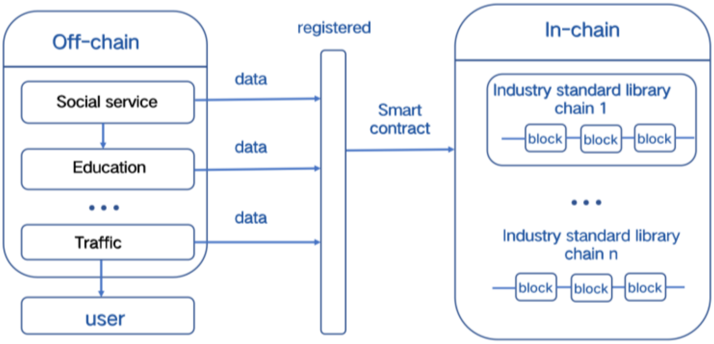

Fig. 4. Development of data sharing standards

Data sharing is a module that sets standards for data of various departments, performs collaborative calculation of data to achieve a win-win situation for both parties, as shown in Figure 4.

Each department can install data sharing nodes on its blockchain at the same time to store its data information, such as transportation, education, social services, etc. The data formats of each department are uneven, and data cannot be exchanged and used immediately. Therefore, the system needs to specify a data standard. Each sector collates and uploads data according to the bar, generates an industry database, and transfers information between the chains by cross-chaining.

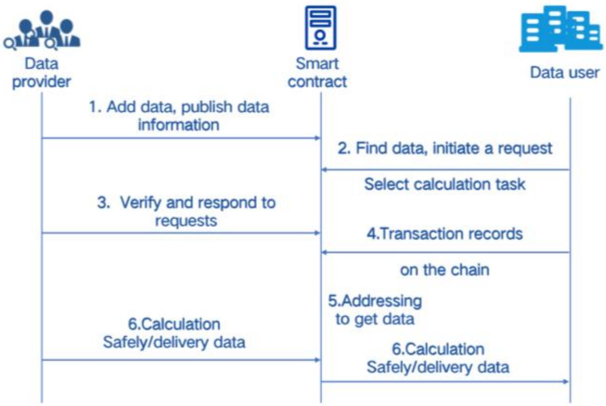

Fig. 5. the information transfer mode

Figure 5 shows the information transfer model. The user reads and finds the data they need, then adds a request for use of the data and the corresponding data run model. The provider decides whether to respond based on the request and the algorithmic model, and the system will follow up based on this response. Assuming that the data provider agrees to share the data information, the local data will be run in the computational model provided by the requester. Then, the final result will be transmitted to the data requester. If the data provider does not agree to the request, it will return a rejection message to the data requester.

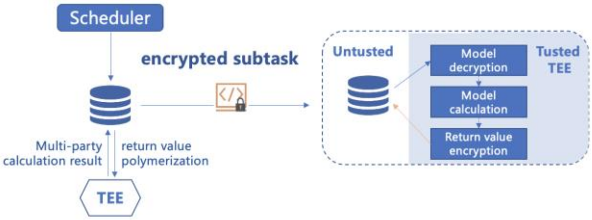

Fig. 6. Computing model based on TEE trusted execution environment

Figure 6 shows that the system uses distributed multi-party secure computation in a TEE trusted execution environment when performing data analysis and computation. Secure multi-party computation allows the establishment of a specific protocol that allows multiple untrusted participants to jointly compute the objective function of their inputs while guaranteeing the accuracy of the output. TEE provides that the server itself can be secure and reliable in its execution environment. Once the computation is complete, each participant should obtain the corresponding result without any other information. This solution maintains the confidentiality of private and security-sensitive data. This solution improves the efficiency of using data and information, reduces the risk of data leakage and tampering, and lowers the probability of data islands.

(4) Visualized Smart Supervision Solution

The data visualization module dynamically visualizes some important consulting information according to the main data information of each department. The intelligent supervision module mainly shows the abnormal situation of data information processing operation in each department to prevent the leakage of data from being tampered, etc. Meanwhile, the data is collected through the mature city operation monitoring index system to form timely and objective monitoring and early warning of city operation.

5 Test Results

The three modules of the system (jurisdiction operation report interface, jurisdiction operation status query interface, and enterprise upload data interface) were tested, and the test results showed that the functions of each module could run normally and achieved the expected effect. The test results of the system functions are shown in Table 2.

In order to evaluate the technology proposed in the smart city framework, we configured eight quad-core, eight-thread Aliyun servers as a server cluster with CentOS Linux as the operating system. The stress test machine was a Mac Book Pro with a 2GHz quad-core Intel Core i5 CPU and the operating system.

Table 2. Results of Systematic Test

interface	Throughput (s)	Throughput (ms)	total number of samples	Abnormal rate
Jurisdiction operation report interface	500	612	150000	0.0050
Jurisdiction operation status query interface	1000	318	318	0.0138
Enterprise upload data interface	500	804	804	0.0154

The blockchain system designed in this paper consists of a number of industry standard chains. The blockchain structure consists of a growing list of blocks, each of which contains a timestamp, transaction data, and a cryptographic hash of the previous block. Because each data modification results in a different hash value for the block being modified, the encrypted hash ensures the trustworthiness of the data stored in the blockchain. Timestamps keep track of when a file was created or modified.

Compared with the traditional system, the security and usability of the smart city data sharing platform based on blockchain technology are greatly improved, as shown in Figure 7. The standard chain can avoid the problem of inconsistent format between data and data. Meanwhile, the two technologies, TEE and MPC, cooperate to protect the privacy of users while using data information. The centralized feature can also prevent the problem of failure EM. This design solution ensures the overall stable operation of the system.

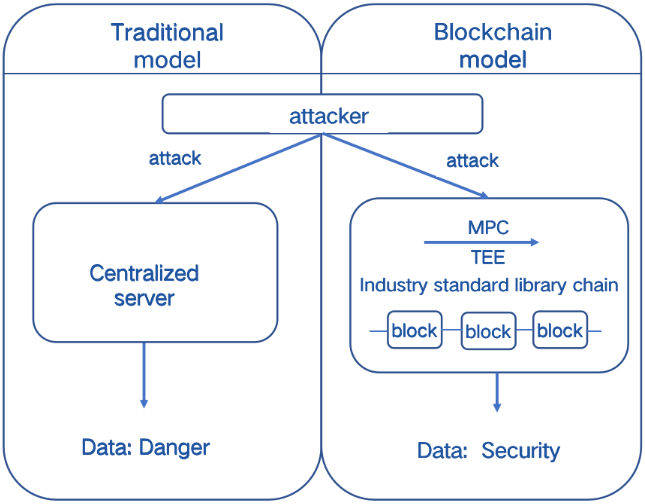

Fig. 7. The comparison of security features

6 Conclusion

Blockchain is a promising computing platform that can support the growing security challenges in innovative urban environments. With the introduction of blockchain technology services in smart cities, its consensus mechanism shifts people's gatekeeping power to algorithms and code. It can mitigate the security threats of databases managed by centralized agencies and, at the same time, overcome issues such as efficiency and effectiveness of transferring datasets to a master repository cost. In this paper, we design a TEE and MPC based data sharing platform for smart cities, which provides a new solution for innovative urban governance and alleviates the security, privacy and trust issues in traditional smart cities. Therefore, this paper can give further support services to help develop security services for smart city blockchain. In the future, we will continue to explore the application and development of blockchain in various segments of smart cities, such as smart education and new energy fields.

References

1. Swan M (2015) Blockchain: Blueprint for a new economy. O'Reilly Media Inc., Newton.
2. Xu Z, Zhang J, Song Z, et al. A scheme for intelligent blockchain-based manufacturing industry supply chain management [J]. Computing, 2021, 103(8):1771-1790.
3. Zhang X, Li X (2018) Application and development path of blockchain in agricultural cold chain logistics. Taiwan Agric Res 153(04):70–73.
4. Zhao L, Bi X, Zhao A (2020) Frame reconstruction of mobile traceability information system for fresh food based on blockchain. Food Sci 41(03):314–321.

5. Zeng X, Peng Y, Wang Q (2018) Research on food safety traceability system based on IoT and blockchain technology. Food Mach 34(09):100–105.
6. Wu S, Yu C (2018) Internet of things and block chain technology in agricultural products traceability. Telecom Eng Tech Stand 31(06):12–15.
7. Shen Z (2019) Storage design for a food traceability system based on blockchain. Telecom World 26(02):304–305.
8. Bocek T, Rodrigues B B, Strasser T et al (2017) Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In: 2017 IFIP/IEEE symposium on integrated network and service management (IM). IEEE, pp 772–777.
9. M. A. Ferrag and L. Maglaras, "Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," IEEE Trans. Eng. Manage., vol. 67, no. 4, pp. 1285–1297, Nov. 2020.
10. T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," IEEE Trans. Eng. Manage.,vol. 67, no. 4, pp. 1298–1309, Nov. 2020.
11. D. Geneiatakis, Y. Soupionis, G. Steri, I. Kounelis, R. Neisse, and I. NaiFovino, "Blockchain performance analysis for supporting cross-border e-government services," IEEE Trans. Eng. Manage., vol. 67, no. 4, pp. 1310–1322, Nov. 2020.
12. W. Meng,W. Li, and L. Zhu, "Enhancingmedical smartphone networks via blockchain-based trust management against insider attacks," IEEE Trans.Eng. Manage., vol. 67, no. 4, pp. 1377–1386, Nov. 2020.
13. Lao L, Li Z, Hou S, et al. A Survey of IoT Applications in Blockchain Systems[J]. ACM Computing Surveys (CSUR), 2020.
14. Mcghin T, Choo K, Liu C Z, et al. Blockchain in healthcare applications: Research challenges and opportunities[J]. Journal of network and computer applications, 2019, 135(JUN.):62-75.