Research on Government Data Sharing Mechanism Based on Smart Contracts

Yuanpeng Long [1], Xuena Zhang [2], Luhong Fan [3], Wei Zhang [4, *], Xun Gui [1], Xiaosong Zhang [1], Shimian Hao [4]

[1] School of Computer Science and Engineering (School of Cyber Security), University of Electronic Science and Technology of China, Chengdu 611731, China;

[2] School of Electronic Engineering, Chengdu Technological University, Chengdu 611730, China;

[3] School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;

[4] School of Finance and Economics, Anhui Science and Technology University, 233000 Bengbu, China.

* ZhangWeiAxel@outlook.com

Abstract. Exploring mechanisms for internal data sharing within government departments is important in advancing digital and intelligent society. This paper is based on the establishment of decentralized nodes on the external network of government departments, constructing a decentralized node, and establishing a government internal data sharing model based on blockchain. Subsequently, integrating attribute fields from government data into the shared model, accompanied by the formulation of data-sharing rules through smart contracts, serves to streamline the implementation of efficient and secure cross-validation mechanisms across diverse departments. Finally, this article concludes by conducting a model performance testing experiment, evaluating the model from three perspectives: storage cost, blockchain performance, and security analysis. The test results show that our model enhances the efficiency of querying and retrieving data within the government's internal data-sharing system, effectively addressing challenges such as low efficiency, high costs, and issues related to the security and real-time aspects of data sharing within the government. Overall, our article provides a new way of thinking about government data sharing.

Keywords: Blockchain; E-government; Government Data; Data Sharing; Smart Contract.

1. Introduction

With the development of e-government and digital government construction, government data has received increasing attention. However, e-government also faces some challenges, with data sharing being one of the main ones **(Ndou, 2004, Almarabeh and AbuAli, 2010)**. Additionally, governments at all levels around the world have recognized the importance of this task and actively engaged in practical work. For example, the European Union Public Administration Conference emphasized the technology and challenges related to e-government data sharing among EU member states **(Otjacques et al., 2007)**, while the latest public sector data sharing report in the UK provided a detailed introduction to the practices and plans of the UK government regarding government data sharing **(Report, 2020)**. In China, data sharing among Chinese government departments has become a core issue in developing China's Internet and government services, which has received great attention **(Zhou et al., 2020)**.

The academic community has conducted extensive research on the collaborative process of data sharing **(Caffrey, Dawes and Prefontaine, 2003, Gil-García and Pardo, 2005, Ramon Gil-Garcia et al., 2007). Li (2011)** argue that establishing a data-sharing system or platform is necessary. **Wu et al. (2012)** proposed a general method for the generation, distribution, and use of electronic certificates. This method falls into the category of innovative technologies aimed at improving collaborative processes. **Qin (2019)** summarized the current status of data-sharing platform in different regions, and he noted that there are many valuable data on government-led data sharing platforms that have not been shared. However, the above-mentioned research still lacks sufficient practical evidence, and there are still issues, such as data security and delayed implementation. In summary, the above work faces problems such as high costs, low efficiency, high implementation difficulty, and insufficient protection.

Blockchain technology and smart contracts can, to some extent, address the aforementioned deficiencies, lowering construction costs, reducing human errors, and considering data security and privacy in the process of data sharing. Some scholars have endeavored to apply blockchain technology in the field of government data sharing. On one hand, numerous studies are dedicated to constructing systems, platforms, and infrastructure, or transforming e-government systems into blockchain architectures. **Hou (2017)** introduced the advantages of applying blockchain technology to e-government and how to build blockchain infrastructure for e-government. **Xiao et al. (2019)** proposed a solution aimed at constructing blockchain systems for government data sharing. **Van Engelenburg et al. (2020)** proposed a blockchain-based framework from a governance perspective. On the other hand, some studies focus on technological innovations, such as **Bhaskaran et al. (2018)** who proposed a data sharing scheme based on digital identity authentication using the concepts of blockchain and PKI to address KYC issues in banking.

The above-mentioned relevant work has made great progress in terms of cost and efficiency, but there are still many problems. Specifically, most literature talks about the great possibilities of this emerging technology, or only focuses on the innovation of technology itself, while ignoring the gap between technological innovation and implementation. For instance, enterprises still encounter phenomena such as repeated data submission, multiple verification, and multiple on-site visits during the data reporting process. This study addresses three primary issues: firstly, how to authorize the sharing of unopened government data without departing from physical boundaries; secondly, how to avoid redundant storage between government departments; and thirdly, how to resolve data silos through smart contracts. The article proposes an efficient, cost-effective, and easily deployable lightweight government data sharing model. Utilizing blockchain and smart contract technologies, a finely-grained, reusable sharing mechanism is designed based on data attributes, addressing issues such as high costs and implementation challenges present in previous solutions. Additionally, flexible allocation of access control permissions is employed to achieve data sharing. The implementation of this system aligns with existing government business systems, eliminating the need for complex system reconstruction or modifications to original business systems. Furthermore, it ensures that government business data remains within the intranet. Finally, the paper utilizes smart contracts to establish consensus among government departments regarding data ownership and access permissions, providing contracts that are easily traceable, manageable, and automatically executable.

2. Background

2.1 Alliance Chain

Blockchain is composed of a shared, fault-tolerant distributed database and multi-node network. It is a decentralized database with the characteristics of decentralization, non-intermediary, information transparency, immutability, and security. In a blockchain system, we generally classify blockchains into three categories based on the scope of participants: public chain, private chain, and alliance chain. An Alliance Chain refers to a blockchain in which the participating nodes are predetermined and only open all or some functions to members of the alliance. The internal members of the alliance chain appoint multiple pre-selected nodes as bookkeepers, and the generation of each block is determined collectively by all pre-selected nodes. Other nodes can participate in transactions but are not involved in the bookkeeping process. Third parties can query the blockchain through the API provided by the alliance chain. Alliance chains are transparent and immutable, limit data interconnection within a specific scope, and have good performance to support business operations. China's "14th Five-Year Plan" states that "we should focus on developing blockchain service platforms and applications in financial technology, supply chain management, and government services, with a focus on consortium chains." Alliance chains are a significant future development direction for blockchain technology in China.

2.2 Applicability of Consortium Chain in Government Data Sharing

This paper proposes a platform-type organizational structure for data sharing, consisting of big data management departments, operation centers, and various government functional departments. It is a weak-centralized and flat organizational structure, and alliance chain technology can support government data sharing based on this organizational structure. Led by the big data management department, the operation center is responsible for specific execution, and the government functional departments collaborate to establish data-sharing supervision consensus. Among the government functional departments, they negotiate and set an agreement on government data sharing, which can be achieved through the consensus mechanism of the blockchain. The data supply process of data registration, data demand application, data feedback, and data access can also be stored through the blockchain to maintain consistent log records between the data supplier and the data demander. To fulfill their supervision responsibilities, big data management departments can authorize the operation center to trace data-sharing behavior by viewing the log records on the blockchain. For local governments, the number of data suppliers, data demanders, big data management departments, and operation centers is small, coinciding with the alliance chain's limited node number feature. Therefore, applying the alliance chain in government data sharing is applicable.

2.3 Smart Contracts

Smart contracts are a computer protocol used in blockchains to establish constraints and rules, aiming to provide validation and execution of contractual obligations, allowing for reliable transactions without the need for a trusted third party. Smart contracts are traceable and immutable and can be used to enforce the terms of a contract.

The theoretical concept of smart contracts was proposed earlier than blockchains, first put forward by scholar Szabo in 1996. However, the development of blockchains allowed smart contracts to come true on their own. In most cases, the operation of smart contracts is event-driven. The contract defines relevant events, rules, and constraints. Once the conditions are met, the functions specified in the contract will be triggered and start to execute automatically.

The concept of smart contracts allows for expressing complex operational logic in cross-departmental data sharing. **Zhang and Zhao (2020)** propose a data-sharing scheme that combines the perspective of technical implementation with public management theory, with the key to perspective integration lying in smart contracts. **Ølnes et al. (2017)** suggest that for governments to utilize blockchain technology in their government services, a comprehensive design of critical decisions is required, including control strategies, data ownership, data privacy, access control, and data openness and scope determination.

3. Design of government data sharing model

As shown in Figure 1, this article proposes a lightweight government data-sharing collaboration process model in which all participating government departments jointly develop constraints and rules for data sharing, track and supervise data usage, and write the shared rules and conditions formed by multiple parties into smart contracts. Through the automated execution of smart contracts, government data sharing is achieved while ensuring that the data does not leave the physical boundary, solving the trust issue between departments.

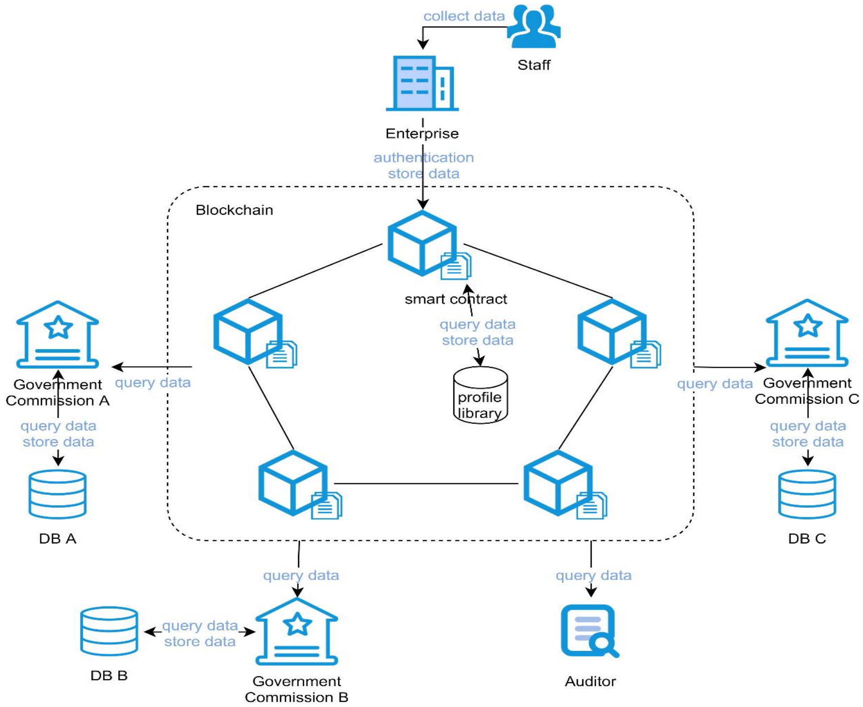

Figure 1: Overview of the model architecture

3.1 Design of Model Construction Ideas

Currently, the role of public sector organizations in the sharing economy is often that of a regulatory agency. However, they can also serve other roles, each with its own corresponding opportunities and challenges **(Hofmann et al., 2019)**. Therefore, we need to overcome these challenges in the model design.

This article begins with the scenario of local government service enterprise policy declaration, aiming to address repeated reporting, multiple verifications, and multiple visits during the policy declaration process. We aim to establish a government data-sharing alliance chain by treating relevant government departments as blockchain nodes.

The node roles include data providers, data users, and regulatory auditors. Data providers are enterprise users collecting and aggregating information about their businesses and employees. After undergoing identity verification, data providers submit data, which will be automatically parsed and analyzed through smart contracts and stored in corresponding private databases. Data users are government departments, and different data users can invoke similar functions (e.g., query data attributes and verify data attributes) to process requests, which are deployed and executed in the form of smart contracts.

3.2 Design of Model Construction Ideas

To ensure that the model can run smoothly based on the actual scenario, it is necessary to address the issues of data source authenticity, data security, data sharing, and sharing efficiency in the framework. Based on the above considerations, this article designs explicitly six mechanisms (as shown in Figure 2), as follows:

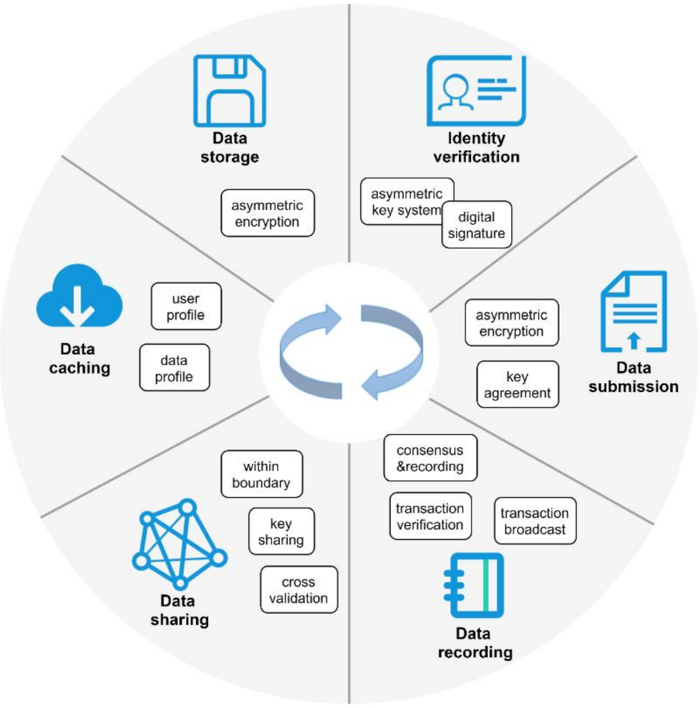

Figure 2: Schematic Diagram of Mechanisms

(1) Authentication: We adopt an asymmetric cryptographic system where each data provider or data user can have one or multiple blockchain nodes. Each node has its own unique public-private key pair and address. A digital signature signed by the private key can uniquely prove the entity's identity.

(2) Data Submission: We adopt encryption algorithms and key-sharing mechanisms. The private data submitted by the data provider will be encrypted before being submitted to the blockchain for verification and recording, thus preventing unauthorized access without the decryption key. The smart contract verifies and parses the data submitted by the data provider and then distributes the corresponding data field values to the appropriate government departments. The allocated data attribute values are encrypted with the public key of the government department before transmission. As shown in Figure 3, for attribute values jointly managed by multiple supervisory departments, there will be a key negotiation process before data distribution, and the private data attribute values will be encrypted with the negotiated shared key.

(3) Data Recording: We employ a blockchain consensus mechanism. Data storage transactions submitted by data providers and data query transactions submitted by data users will be verified, broadcast, and subjected to consensus by blockchain consensus nodes. Once consensus is reached, the transactions are recorded in the shared distributed ledger.

(4) Data Sharing: This paper innovatively proposes a data sharing model based on smart contracts, which allows business data to remain within physical boundaries, with government department's private business data stored in their respective private databases. Blockchain smart contracts are utilized to respond to query requests initiated by other government departments, verifying the existence, authenticity, and integrity of the data. Subsequently, the query verification results are returned to the requesting party, achieving cross-verification and enabling data sharing between government departments. It is noteworthy that the source data remains within physical boundaries throughout the process.

(5) Data Caching and Data Storage: This paper innovatively proposes a portrait library mechanism, comprising user portrait libraries and data portrait libraries. The user portrait library serves as a caching mechanism to further enhance query and retrieval efficiency, while the data portrait library establishes a mapping relationship between data attribute lists and supervisory departments along with their unique public keys. Data storage transactions necessitate the

encryption of private data, requiring the retrieval of the corresponding public key of the supervisory department to encrypt the private data.

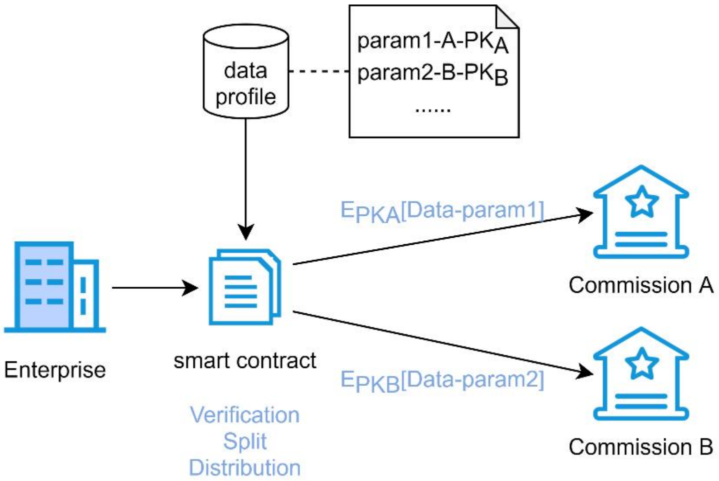

Figure 3: Key Sharing Mechanism

4. Implementation of Government Data Sharing Model

This section demonstrates the model implementation with specific use cases and compares it with previous work from an implementation perspective. Since Ethereum is the first large-scale blockchain application and smart contract platform with a well-developed ecosystem, the model in this paper will be based on the Ethereum blockchain as the underlying foundation **(Buterin, 2014)**. However, the Ethereum blockchain network allows arbitrary nodes to access, meaning that the blockchain data is completely open, which is unsuitable for government service with strict access control.

Therefore, based on the Ethereum, this paper improves the access mechanism to achieve collaborative government data sharing. Additionally, Ethereum's technical features include Proof of Work (PoW), Ethereum Virtual Machine (EVM), Decentralized Autonomous Organization (DAO), payment mechanism, and new technological features introduced in version 2.0 such as Beacon Chain, Sharding, Proof of Stake (PoS), and the new virtual machine environment (eWASM). However, the design goal of this paper is to be directly based on mathematical or cryptographic mechanisms to be independent of any specific platform. For inevitable platform characteristics, this paper will use simple equivalent replacement mechanisms.

4.1 Data Model Implementation Mechanism

In this article, the data source is stored in the government department's private database. The data storage transactions submitted by data providers and the data query transactions submitted by data users are recorded in the distributed ledger shared by each blockchain accounting node. The transaction information in the blockchain is transparent, and the transaction structure is shown in Figure 4. The payload is the data field containing the encrypted data attribute values of the corresponding government department's public key. This method not only specifies the function and parameters to be called but also ensures that the parameters are not leaked or stolen. Another innovative design of this article is the portrait library mechanism, which includes user and data portrait libraries. Each entry in the portrait library has a data structure, as shown in Figure 4. When a government department registers, it submits its data attributes and its own public key. The system then generates a data portrait library entry and adds it to the data portrait library. Each entry in the user portrait library represents a list of attribute values declared by enterprise users who have queried in this system, along with their existence and authenticity lists.

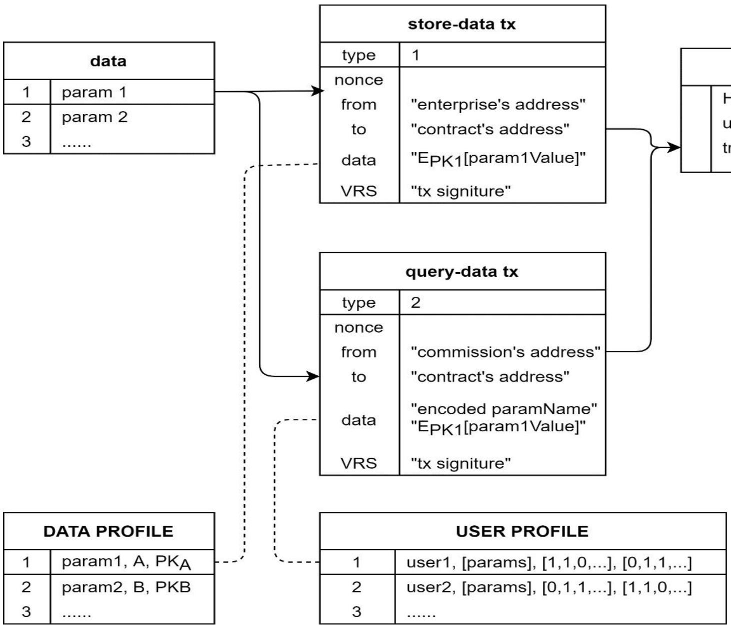

Figure 4: Data Model

The blockchain data structure used in this paper does not adopt the Bitcoin UTXO model but rather the Ethereum model. Each block maintains a world state, as Figure 5 shows. The block structure comprises a block header and a block body. The block header includes the previous block's hash value and the merkle tree root, among other elements. The block body includes transaction data, uncle block data, and additional information.

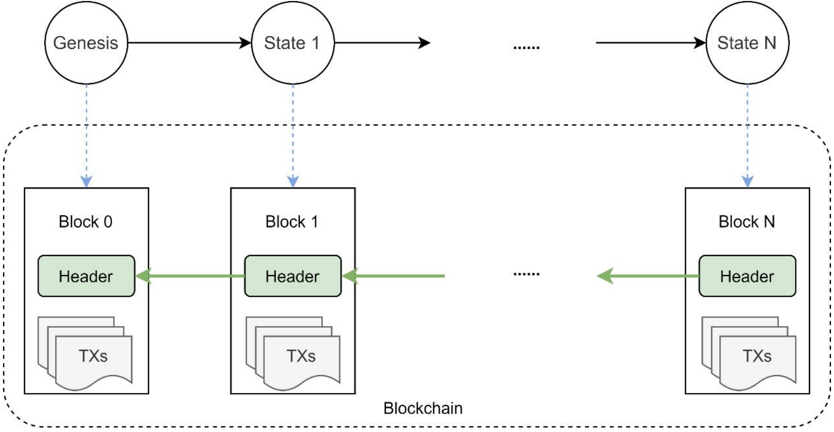

Figure 5: Block Data Structure

4.2 Smart Contract-Based Data Sharing Protocol

The government data-sharing mechanism designed in this paper is based on smart contracts, which require relevant departments to interact and jointly establish rules to specify the rights and responsibilities, data interaction methods, data models, data visibility, exception handling, etc., in order to form smart contracts. Smart contracts are deployed on the blockchain through P2P network technology and broadcast to the entire blockchain. Then, data users can automatically trigger the relevant data-sharing process through smart contracts.

Smart Contract Functions: Smart contract functions take the distributed ledger as the sole source of their state information and support Storage (writes) and Query (reads) requests through RPC connections. Table 1 lists the critical functions of smart contracts.

Table 1: Smart Contract Functions (S==STORAGE, Q==QUERY, I==INTERNAL)

Name	**Role**	**2. 1. 1. Parameters**	**Description**
（S）StoreData	Enterprise	data	Adds enterprise private data to relevant

			commission； validates, splits，distributes data
（I）DataValidation	-	dataParam	Validates data param value
（I）DataSplit	-	data	Splits enterprise private data
（I）DataDistribution	-	dataParam	Retrieve data Profile to find corresponding PK (public key)， PK encrypts data param value
（I）IdentityAuth	-	userID	Verify user identity
（I）KeyAgreement	-	<PK1, PK2，…>	Implement Diffie-Hellman key exchange extension protocol，negotiate shared key
（I）SetUserProfile	-	userProfile	Adds new entry or update old entry
（I）GetUserProfile	-	-	Gets all entries
（I）SetDataProfile	-	dataProfile	Adds new entry or update old entry
（I）GetDataProfile	-	-	Gets all entries
（Q）GetExistence	Commission	uerID, dataParam	Commission requests whether < dataParam> exists
（Q）GetComfirm	Commission	uerID, dataParam	Commission requests whether < dataParam> approved

The government data-sharing mechanism designed in this paper is published to the blockchain system as a smart contract code and interface. This contract code is unrelated to the specific government department's business, while the contract's external interface parameters are related to the particular government department's business. The participating government departments have their databases to store their business data. The participating departments interact with each other to agree on sharing rules and publish the corresponding data field requirements and their node public keys to the blockchain data character library. Users can query relevant information within the authorized scope to handle government affairs. The specific process is as follows: first, identity authentication, after which the smart contract initiates a data query verification request to the corresponding department. The contract automatically executes and judges whether the relevant department has the user's data field and whether it is compliant. This is equivalent to obtaining complete user raw data. In addition, this model proposes a caching mechanism, namely the user character library, which stores the user data summary retrieved from the blockchain to improve the efficiency of the next user query. The core process protocol will be introduced in the next section.

4.3 Protocol Implementation Process

The model in this paper calls the aforementioned smart contract functions to implement two protocols (processes) to meet the permission control and privacy restrictions in the government data-sharing process. The case in this paper will reference the real-world business data fields of government departments in the real world, demonstrating two key process protocols: store data and query data.

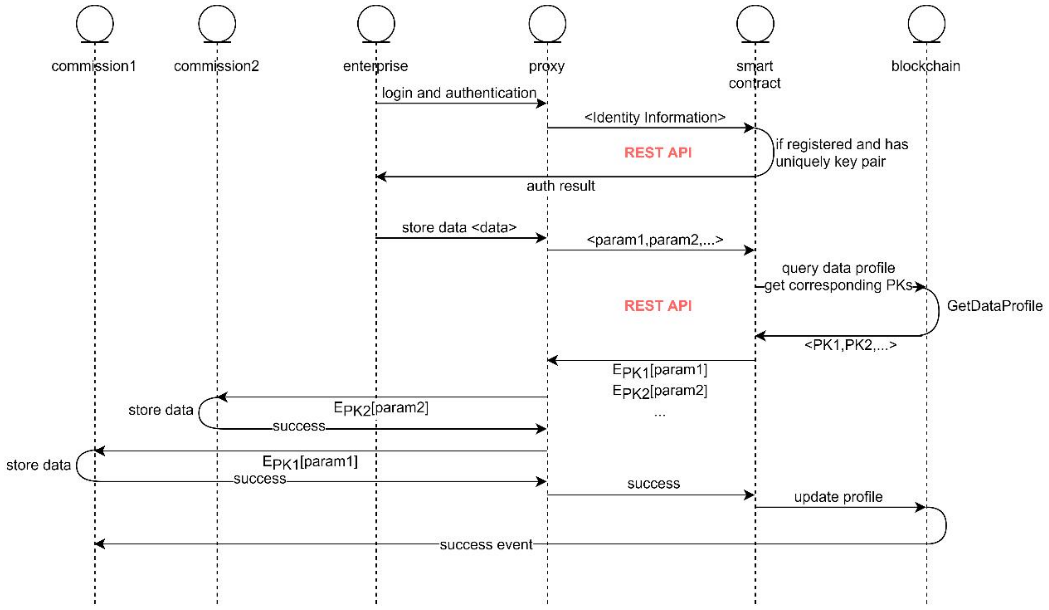

Figure 6: Protocol: Enterprise data-storage on block chain

In the first case, there are two participating government departments, called **Commission 1** and **Commission 2**, and an enterprise user called **Enterprise**. Assuming that these entities have already completed registration on the blockchain, the government departments have published their data fields and requirements, as well as their public keys, to the blockchain's data character library after registration. The data storage protocol process is as follows:

(a) **Enterprise** logs in and undergoes identity authentication. The smart contract determines whether the **Enterprise** has been registered.

(b) **Enterprise** initiates a data storage request and submits complete declaration materials, such as declaration forms, business licenses, intellectual property materials, employee description information, financial audit reports, etc.

(c) The proxy agent parses and unpacks the complete declaration materials and packages them into a list of data attribute values that can be recognized by the contract code <param1, param2, ...> and calls the corresponding interface of the smart contract.

(d) Accessing the data portrait library within the contract, a list of public keys <PK1, PK2, ...> corresponding to the supervisory departments of the queried data fields is retrieved.

(e) Uses the corresponding public key to encrypt the data attribute values and sends the ciphertext to the responsible department. The responsible department uses its unique private key to decrypt the ciphertext and store the user's data attribute values in its business database.

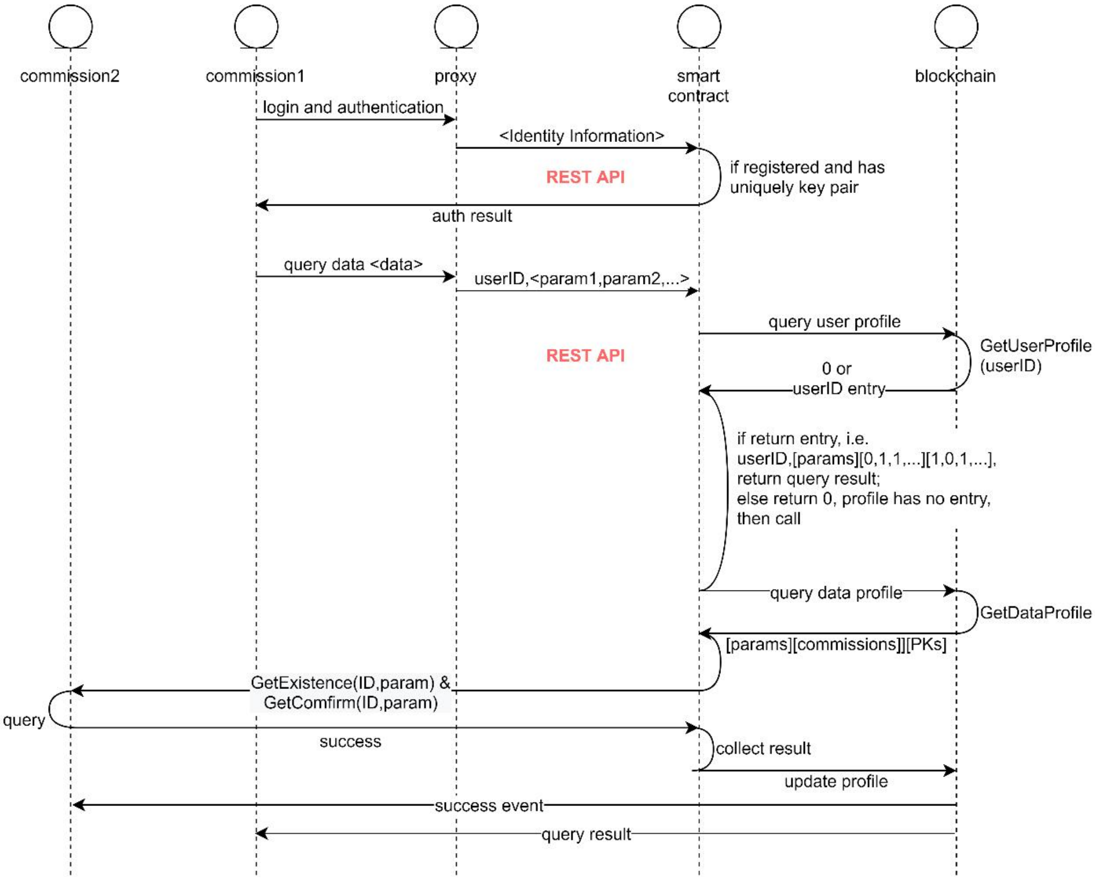

Figure 7: Protocol: Commission data-sharing on block chain

In the second case, there are two participating government departments, referred to as **Commission 1** and **Commission 2**. **Commission 1** requests to query the existence and authenticity of the enterprise user's declaration materials from the blockchain smart contract. The data-sharing protocol process is as follows:

(a) As the data storage protocol states, **Commission 1** logs in and verifies its identity.

(b) **Commission 1** initiates a data query request, which includes the enterprise ID and the declaration materials submitted by the enterprise. The proxy agent parses and packages the data and sends it to the smart contract.

(c) The contract initiates a request to retrieve the user portrait library, checking whether there are search records for the enterprise user in the system. If records exist, it returns the user portrait library entry corresponding to the enterprise ID. This entry comprehensively describes the existence and authenticity of the user-declared materials. In the absence of records, the contract proceeds to request queries and audits from the relevant supervisory government departments.

(d) Retrieve the data portrait library within the contract, obtain supervisory department information corresponding to the data attributes, and then invoke the functions GetExistence(ID, param) and GetConfirm(ID, param) on that department. This process is conducted to inquire about the existence and authenticity of the data attributes in the business database of the respective department.

(e) After obtaining and summarizing the query verification results, update the portrait library file.

(f) Aggregate the query results and return them.

5. Model Performance Testing and Analysis

In this section, we will construct a model performance testing environment to demonstrate the feasibility and performance advantages. The testing experiment is deployed on four independent physical servers, each with the following specifications: processor: Intel Xeon 2.4 GHz 8-core CPU, memory: 8GB, operating system: CentOS 7.2. These servers are named node1, node2, node3, and node4, and all of them serve as consensus nodes. Nodes 1-3 represent three government departments and store the original government dataset, while node 4 serves as the access node. For security reasons, the original dataset used in this testing experiment is constructed based on the fields and attributes required by the real government data. The principle of constructing the dataset is to cover all cases, including cases where the enterprise data is complete, partially complete, missing fields, or vacant. The dataset information for node1-3 is shown in Table 2.

Table 2: Basic Information of Dataset

Node	Number of Records	Attributes
Node1	12000	Company Name, Unified Social Credit Code, Registered Capital, Paid-up Capital, Registration Date, Registration Address, Number of Employees, Number of Employees Paying Social Security.
Node2	10000	Company Name, Account Opening Bank, Bank Account, Legal Representative, ID Number.
Node3	8500	Company Name, Number of Intellectual Property Rights, Invention Patents, Utility Model Patents, Design Patents, Software Copyright.

The experimental model relies on open source software, with blockchain using the Ethereum framework PoA consensus algorithm, smart contracts implemented using the solidity language, and front-end presentation using web pages to display user interaction data.

5.1 Storage overhead test

One major advantage of this model is to achieve internal cross-checking and reduce duplicate data storage among government departments. Therefore, this section tests the storage overhead parameters of this model by increasing the amount of enterprise data and compares them with the data storage and read/write overhead parameters under traditional methods. The results are shown in Figure 8.

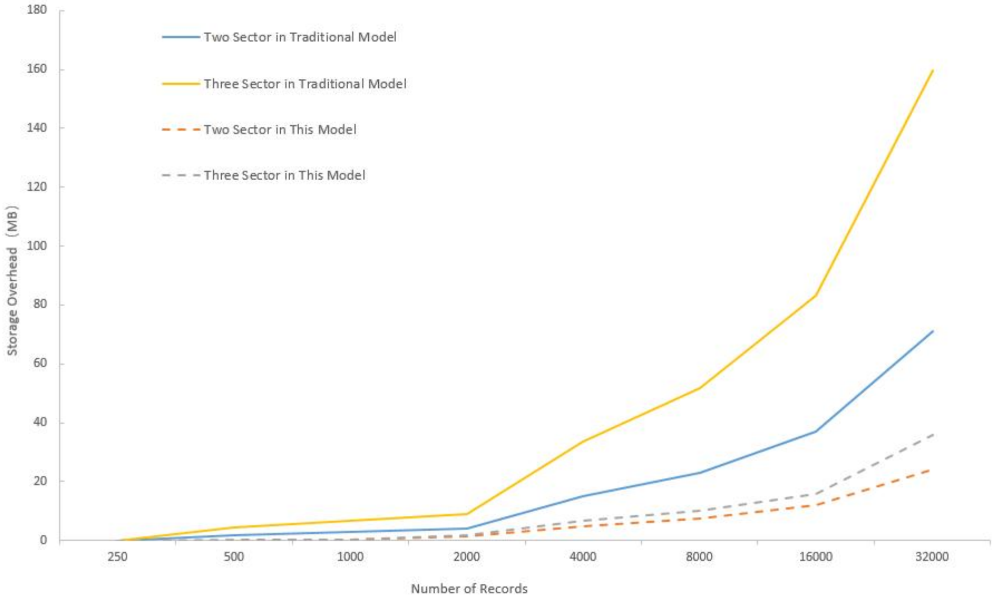

Figure 8: Comparison of Storage Costs between Traditional and our Model

The traditional decentralized approach to storing business data involves each department that uses the data storing its own copy. In other words, the data usage department applies for and imports relevant business data provided by the shared data department. This approach not only carries the risk of data leakage, but also has drawbacks such as large data transmission requirements and high data storage costs. The storage overhead of this model is equivalent to the storage overhead of the centralized traditional approach, meaning there is no redundant storage, and the model avoids the high cost of building a data center with a uniform standard in traditional methods.

As shown in Figure 8, it can be seen that as the amount of data continues to grow, the method proposed in this article significantly reduces the storage overhead.

5.2 Blockchain Performance Test

Furthermore, this section will compare the performance overhead between utilizing blockchain technology and not using blockchain technology to achieve the same data sharing objectives. In other words, based on the same data sharing protocol for an equivalent amount of shared data, performance metrics for both scenarios will be tested to demonstrate that the use of blockchain technology does not significantly impact performance overhead. Additionally, it substantially enhances system security. In general, TPS (transactions per second) is commonly used as an assessment metric for blockchain performance (Fan et al., 2020). Therefore, in this section, performance in terms of time overhead is measured for an equivalent amount of shared data. The time overhead encompasses local query computation, network transmission, and blockchain transaction response time. The experimental results of this article are shown in Figure 9.

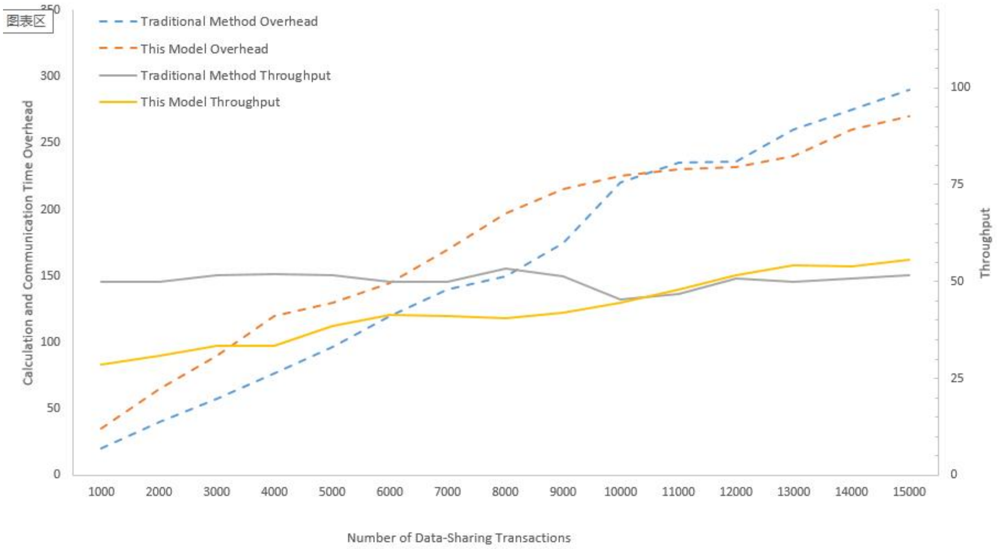

Figure 9: Performance Comparison of Using Blockchain Technology or Not

The experimental results indicate that using blockchain technology does not significantly increase the system performance overhead. When the system's portrait library is not complete, meaning the system does not yet contain all user caches, user query transactions are only then recorded on the chain. After the system's portrait library is filled, query transactions are only invoked as call types, which are not recorded on the chain and do not generate additional network communication overhead. In addition, the network transmission overhead of traditional C/S or B/S architectures is greater than the P2P network overhead used by blockchain. Therefore, after the portrait library is filled, this model's performance overhead growth rate is slightly lower than that of traditional methods.

5.3 Security Analysis

Safety is crucial to the process of cross-departmental collaboration and sharing. Although the design of this system aims to promote the collaborative sharing of resources among multiple government departments, the mechanism should provide sufficient security guarantees, and the use of federated blockchain establishes a security mechanism for various parties without mutual trust. In our proposed blockchain data-sharing scheme, there is no longer a need for a centralized trust with high risks of data leakage. The consortium blockchain replaces the trusted third party by connecting each participant through multi-party data retrieval. Furthermore, the consortium blockchain uses cryptographic algorithms such as elliptic curve digital signature algorithm and asymmetric cryptography to ensure data security. Assuming that attackers can be government departments, enterprises, consortium chain nodes, and third parties, attackers may eavesdrop on communication, drop transactions, create false transactions and blocks, change or delete stored data, connect users' transactions, and sign false transactions to legitimate collusive nodes. However, they cannot break the encryption. In this section, we identify the main threats that may exist in the mechanism and model and provide solutions to ensure the best level of security.

Data Security and Privacy Protection: This threat refers to issues such as insecure data storage, insecure access control, communication data tampering, and repudiation. Our proposed model can ensure that the data source does not leave the local area and that the information transmitted in the external network only includes data attribute existence, legitimacy, and integrity verification results. The model designs a fine-grained access control mechanism, and the blockchain system guarantees trust. The blockchain system ensures secure communication of public data and data tamper-proofing.

Data Misuse Prevention: In traditional solutions, data ownership is unclear after leaving the local area, which can easily lead to data misuse and make it difficult to track records. The model proposed in this article adopts blockchain technology to facilitate accountability. The model is based on secure multi-party computation, and multiple data sources achieve efficient and secure internal data sharing without leaving the local area.

Interoperability, Accessibility, and Reusability: Traditional solutions store data in different departmental databases, adopt different data standards, and form data islands that are difficult to share, reuse, and interoperate. The model proposed in this article is based on a data attribute field question-and-answer mechanism and designs an internal sharing model that satisfies data interoperability. The model stores data and user portraits on the blockchain for easy data accessibility and reusability.

Data Integrity: Traditional sharing methods are prone to data loss during transmission, resulting in incomplete data. In our proposed scheme, the data source does not leave the local government department, and the query verification result is transmitted to the communication endpoint. Regional data integrity is not threatened, and the model's portrait library mechanism further improves issues such as missing items in single-department stored data. The model's storage also adopts distributed storage with multiple backup points to prevent data loss.

Efficiency and Performance: Traditional government data-sharing solutions could be more efficient and cost highly. Our model does not involve inefficient and error-prone manual import processes and does not modify the original government business system.

6. Conclusion

In the information age, government data sharing can gradually solve the long-standing issues of "information islands" and "fragmentation" that have plagued the development of government information technology in China. However, the current government data-sharing mechanism still needs to improve, as it has high costs and low efficiency. By building a lightweight government data-sharing model based on blockchain and smart contracts, this article provides a reliable government data-sharing platform for government departments, citizens, and enterprises. Blockchain ensures data traceability, and the automatic execution of smart contracts provides a guarantee for secure data sharing. The model proposed in this section is a typical scenario of applying smart contracts to government management, with wide scalability and reusability. Future work can include designing a credit mechanism to improve the consensus algorithm, where nodes with high credit scores have higher verification weights for data ownership. Additionally, further research can be conducted to refine the functional design of smart contracts, allowing citizens to complete administrative services without government staff involvement. Furthermore, smart contracts can be used to provide customized government services, providing new research directions for China's government data sharing and openness efforts.

Acknowledgments

This work was supported by Anhui Provincial Higher Education Collaborative Innovation Project(XLYC2002116),
Research Project of Philosophy and Social Sciences in Anhui Universities(2023AH051831), Anhui Federation of Social Sciences Project (2022CX524) and Anhui Science and Technology Uni versity project (CJYJ201906）.

References

[1] Almarabeh, T. and AbuAli, A. (2010). A general framework for e-government: definition maturity challenges, opportunities, and success. European Journal of Scientific Research. 39, 29-42.

[2] Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., et al. (2018). Double-blind consent-driven data sharing on blockchain. doi,

[3] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper. 3, 2-1.

[4] Caffrey, L. 1998. Information Sharing Between & Within Governments.

[5] Dawes, S. S. and Prefontaine, L. (2003). Understanding new models of collaboration for delivering government services. Communications of the ACM. 46, 40-42.

[6] Gil-García, J. R. and Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. Government information quarterly. 22, 187-216.

[7] Hofmann, S., Sæbø, Ø., Braccini, A. M., and Za, S. (2019). The public sector's roles in the sharing economy and the implications for public values. Government information quarterly. 36, 101399.

[8] Hou, H. (2017). The application of blockchain technology in E-government in China. 26th International Conference on Computer Communication and Networks.

[9] Li, Q. (2011). Research on E-government Data Sharing Platform Based on Web Service (In Chinese). Information System Engineering. 118-120.

[10] Ndou, V. (2004). E-government for developing countries: Opportunities and challenges. Electron. J. Inf. Syst. Dev. Ctries. 18, 1-24.

[11] Ølnes, S., Ubacht, J., and Janssen, M. 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Elsevier 34 355-364.

[12] Otjacques, B., Hitzelberger, P., and Feltz, F. (2007). Interoperability of e-government information systems: Issues of identification and data sharing. Journal of management information systems. 23, 29-51.

[13] Qin, S. (2019). Research on the Government Data Openness and Sharing Model (In Chinese). Modern Computer. 53-56.

[14] Ramon Gil-Garcia, J., Chengalur-Smith, I., and Duchessi, P. (2007). Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. European Journal of Information Systems. 16, 121-133.

[15] Report, I. 2020. Addressing trust in public sector data use (Independent Report), https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use.

[16] Van Engelenburg, S., Rukanova, B., Hofman, W., Ubacht, J., Tan, Y.-H., and Janssen, M. (2020). Aligning stakeholder interests, governance requirements and blockchain design in business and government information sharing. International Conference on Electronic Government.

[17] Wu, e., Xie, D., WU, y., Ling, C., Wang, M., and Chen, Y. (2012). Research on e-government data sharing mode (In Chinese). Microcomputer Applications. 28, 16-21.

[18] Xiao, F., He, D., Chi, Y., Jeng, W., and Tomer, C. (2019). Challenges and supports for accessing open government datasets: Data guide for better open data access and uses. 2019 conference on human information interaction and retrieval.

[19] Zhang, N. and Zhao, X. (2020). Understanding Cross-Sector Data Sharing Based on Blockchain: From Collaborative Agreement to Smart Contract (In Chinese). Chinese Public Administration. 77-82.

[20] Zhou, L., Huang, R., and Li, B. (2020). “What is mine is not thine”: Understanding barriers to China's interagency government data sharing from existing literature. Library & Information Science Research. 42, 101031.