DSI DATA SCIENCE AND INFORMETRICS
VOL.3, NO.3, AUG. 2023

RESEARCH ARTICLE

Construction of a blockchain–based intelligent platform for government data

Zhonglei Zhang, Wanghui Yang*

School of Management, Hangzhou Dianzi University, Hang Zhou, China.

ABSTRACT

The management and application of government data are the bases for the construction of a digital government. Building an intelligent platform for government data by using artificial intelligence, blockchain, and other technical means to achieve open sharing, development, and utilization of data is an important link to promote continuously the construction of a digital government and improve the level of government management and service efficiency. According to the current construction status of government data platforms and the application prospect of blockchain technology, this study proposes to build a blockchain-based intelligent platform for government data. In combination with the technical advantages of blockchain, this study investigates the theory and technical logic of building a blockchain-based intelligent platform for government data and then proposes the theoretical model, architecture, operation mechanism, and core technology of platform construction. This study explores the implementation path of building a blockchain-based intelligent platform for government data from five aspects, i.e., promoting technology upgrading, improving top-level design, strict supervision and regulation, strengthening collaborative research and judgment, and improving technical support.

KEYWORDS

Blockchain; Government data; Platform construction; Implementation path

1 Introduction

The constant promotion of constructing an intelligent platform for government data is an important measure to improve the modernization of the national data governance system and governance capacity in the age of big data. The Proposals of the Central Committee of the Communist Party of China for Formulating the 14th Five-Year Plan for Social and Economic Development and Future Targets for 2035 proposed the following: "We shall strengthen the construction of digital society and digital government and improve the digital intelligence level of public services and social governance. We will expand the orderly opening of basic public information data and build an open platform for unified sharing of national data." (The Central People's Government of the People's Republic of China, 2022a). Govern-

* Corresponding Author: Yangwh96@163.com

ment data are basic, authoritative, professional, and fully covered. It is the most important core data asset in society. Using the Internet, big data, artificial intelligence, blockchain, and other technical means to realize the open sharing, development and utilization of government data has an authoritative leading role in promoting the construction of digital government, smart society, and digital economy. In September 2022, the General Office of the State Council issued the Guidelines for the Construction of the National Integrated Government Big Data System, which requires all regions and departments to promote the construction of the government data platform, implement innovation in the relevant systems and mechanisms of the government big data system and application services actively, enhance the effectiveness of digital government, build good digital ecology, and constantly improve the level of government management and service efficiency to provide strong support for promoting the modernization of the national governance system and governance capacity (The Central People's Government of the People's Republic of China, 2022b).

2 Literature review

2.1 Overview of blockchain-related research

In October 2019, general secretary Xi Jinping proposed in the 18th collective study of the Political Bureau of the CPC Central Committee that we should maximize the role of blockchain in promoting data sharing, optimizing business processes, reducing operating costs, improving collaboration efficiency, and building a trusted system. We shall explore the use of blockchain data sharing mode to achieve cross-departmental and cross-regional common maintenance and utilization of government data, promote business collaboration, deepen the "going out once at most" reform, and bring improved government service experience to the people (Xi, 2019).

As a popular topic at present, blockchain technology has been increasingly used in various fields of social development. Blockchain is a computing paradigm based on a point-to-point network, which uses a chain structure to verify and store data, a distributed node consensus algorithm to generate and update data, cryptography to ensure data transmission and access security, and automated script code to form smart contract operation data (Chao, 2018). Blockchain can be divided into three main types: public chain, alliance chain, and private chain. As the most widely used blockchain type (Zhang et al., 2019), the public chain is more open and free in form; compared with the public chain, the alliance chain has fewer nodes, and the data reading and accounting rules are formulated and applied by the members of the alliance; given its high degree of centralization, the private chain often has higher accounting efficiency than the former two, and the creation, consensus, and maintenance process of data are mastered by its creator.

Given the remarkable characteristics of blockchain technology, such as decentralization, non-tampering, openness, and anonymity, it has been widely applied in many sectors of society. For example, in the field of the Internet of Things, the tamper-proof feature of blockchain technology ensures consistency and security between the physical world's physical assets and the virtual world's digital assets. In the financial field, the decentralization feature of blockchain has solved the practical problems of enterprise financing from multiple dimensions, such as efficiency, cost, and trust, and provided an open and equal platform for multiple participants in the process. In the field of industrial supply chains, blockchain technology is used to store and manage data, and the transparency and reliability of the industry are improved through product traceability, query, and verification (Dai et al., 2021). In addition, the traceability of blockchain technology has been applied in commerce, insurance, e-government, and other fields.

2.2 Overview of relevant research on application practices of government data platform

In the process of practicing the construction of the government data platform, the security supervision of government data is the core to prevent security problems related to government data effectively. Research on security risk assessment of information systems abroad has lasted for more than 30 years. It began with the evaluation criteria for trusted computer systems issued by the US Department of Defense in 1985. Since then, Canada, France, and other developed countries have issued corresponding standards on information security risk assessment (Jahl, 1991; Bacic, 1990; Didraga, 2015). Research on information system assessment in China started late, but in the past decade, with the rapid development of information technology, a series of standards, such as the Code for Information Security Technology Information Security Risk Assessment, the Guidelines for Information Security Technology Information Security Risk Assessment Implementation, the Data Management Capability Maturity Assessment Model, and the Information Technology Big Data Open Sharing Part 2: Basic Requirements for Open Sharing of Government Data, have been promulgated one after another (Gao et al., 2018).

In the current application practice of domestic and foreign government data platform construction, relevant research is mainly conducted from the perspectives of data classification, classification, and labeling management, security protection in the entire life cycle of data, situation awareness of data risk identification, and analysis and early warning technology system, etc.

Data classification and classification and labeling management. While building the government data platform, many local governments have conducted hierarchical management of data. Guizhou Province issued the first local standard, Guidelines for Classification and Grading of Government Data (DB 52/T 1123-2016). According to the Grading Guide for the Security of Government Information Resources, Zhejiang Province has built a classification and grading system for government information data and personal information data. In the system, L1 is shareable and open (general data), L2 is shareable and not open (general data), L3 is restricted sharing (sensitive data), and L4 is personal authorization (sensitive data). In accordance with the Personal Information Security Standards, 1381 items of personal sensitive information were sorted out, including ID number, bank account number, property information, whereabouts, health and physiological information, transaction information, personal information of children under 14 years old, etc., and security measures, such as authorized use and dynamic desensitization, were taken. In the specific implementation process, Zhejiang Province mainly used technical means to achieve data discovery and labeling management of government data. Through the standardized processing of massive data and in accordance with the content features, semantic features, statistical features, and other features, expert rules, graph computing, machine learning, and other methods are used for AI intelligent recognition and output according to data labels and data levels. On this basis, in August 2021, Zhejiang Province issued the local standard Guidelines for Classification and Grading of Public Data in Digital Reform (DB33-T2351-2021), which further specifies the general requirements, dimensions, and methods for classification and grading of public data.

Security protection in the entire life cycle of data. Existing government data platforms actively take certain technical measures to prevent data leakage during the entire life cycle of data. For example, data dynamic desensitization is realized in the data acquisition stage. To ensure that the development and utilization of data are not affected, data access in the collection, storage, processing, sharing, and other links is dynamically desensitized without changing the original data (real-time desensitization is performed when the actual data value remains unchanged). Zhejiang Province formulated 28 types of desensitization rules to desensitize dynamically 19,317 items of data, such as the cleaning warehouse, population warehouse, legal person database, credit database, etc; Guizhou issued a local standard, Guidelines for Desensitization of Government Data (DB 52/T 1126-2016), and a group standard, Guidelines for Desensitization of Information Security Technology Government Data (T/GZBD 4-2020); Shandong Province issued a local standard, Public Data Opening Part 2: Guidelines for Data Desensitization (DB37/T 3523.2-2019). In the data sharing stage, most provinces isolate the production and development environment by building a unified data distribution platform and achieve "available and invisible" data through data dynamic desensitization technology and access data volume control technology. Hangzhou issued a local standard, Data Resource Management (DB3301/T 0322), which covers government data security supervision, government data security responsibility, government data classification, and government data sharing process.

Situation awareness, analysis, and early warning technology system of data risk identification. The current government data platform mainly adopts machine learning, artificial intelligence, and other technologies through log audit, behavior risk analysis, and scenario compliance analysis. Public data platforms in most provinces can analyze the operation behavior of data developers internally (such as frequently querying sensitive data), and the compliance of interface calls externally (such as calling data during nonworking hours in an office system). The existing technology preliminarily realizes log audit analysis based on machine learning, overall situation awareness, and risk early warning and prevention (including database change detection); it also realizes key technical capabilities, such as data watermark, image watermark, and structured data identification.

2.3 Overview of government data platform construction based on blockchain

At present, blockchain technology has been widely used in government affairs in dozens of countries. According to the application results, blockchain technology has helped the government build a high-quality public service platform for citizens. At the same time, it has also enhanced citizens' expectations and trust in the government and further improved the legitimacy of governance.

Estonia is considered the most advanced digital country in the world. As early as 2008, it began to test the application of blockchain technology in "more than 1000 online government services," such as justice, health care, network security, and identity authentication (Liu et al., 2019). The US uses blockchain technology for special information collection, communication platform building, and defense information system control. Australia uses blockchain technology to build an intelligent Internet of Things system (Cheng, 2021). The UK has implemented a meat tracking system for slaughterhouses using blockchain technology to ensure food safety. Russia, Denmark, and Thailand use blockchain technology to vote, simplify the voting process, reduce election costs, and avoid dark box operations. Switzerland uses blockchain technology for identity recognition and encrypted payment, whereas Georgia uses it for land registration; Singapore, Gibraltar, and Sweden use blockchain technology to develop digital and encrypted currencies, and South Korea uses blockchain technology to take over the governance services of the entire city without violating citizens' privacy (Qi, 2018). In addition, many countries have applied blockchain technology to e-government, credit management, civil service management, traffic control, academic supervision, salary review, tax collection, financial audit, cross-regional education, vehicles, logistics, the Internet, medicine (vaccine), guns, and refugee supervision; they also formulated the development plan of blockchain technology and conducted the legislative work of blockchain technology, laying a good foundation for promoting government data governance in a wider range of blockchain.

China also started to explore the application of blockchain technology in government data governance earlier. In the 13th Five-Year Plan, blockchain was regarded as a "strategic frontier technology," and the Ministry of Industry and Information Technology of China issued the White Paper on China's Blockchain Technology and Application Development in October 2016 (Zhu, 2020). Zhejiang, Shanghai, Guangzhou, and Guizhou have all conducted research on projects related to blockchain technology. For example, Guiyang issued a white paper entitled "Guiyang Blockchain Development and Application" in 2018 and formulated a blockchain development plan. At present, government applications for blockchain technology are dominated by pilots in specific areas. For example, the tax department has created an electronic invoice system using blockchain technology, where enterprises can use digital signatures to generate, transmit and store electronic invoices, and the tax department is able to monitor the flow and use of invoices in real time, which effectively reduces forgery and tampering of invoices; a number of local governments have implemented a blockchain land registration system, which utilizes a distributed ledger to record land ownership and transaction information, ensuring the authenticity of land information and security; some regions have begun to pilot blockchain e-license, which realizes the e-licensing and sharing of licenses by uploading the information of various licenses (e.g., business licenses, driving licenses, etc.) onto the chain.

These cases are just some of the government's practical applications of blockchain technology, which shows that there is a lot of expectation for the future development of blockchain technology. Although some theoretical results have been formed in the research of blockchain technology in the construction of government data platforms, there are still more gaps in the deeper application of the technology and the top-level design of the platform construction. Therefore, this paper will explain the logic of constructing a government data intelligent platform based on blockchain, and then put forward a more specific construction model and illustrate the specific path of realization.

3 Building the logical foundation of a blockchain–based intel–ligent platform for government data

3.1 Advantages of applying blockchain technology

The application of various core technologies of blockchain in the construction of an intelligent platform for government data fully reflects the remarkable advantages of blockchain technology in this field.

Blockchain technology is conducive to reducing administrative costs and improving the effectiveness of data governance. Government departments at all levels manage numerous public resources and databases. The centralized political power system has certain stability in management, but in the process of maintaining its normal operation, it often requires considerable management and maintenance costs. The lengthy reporting and approval process also leads to many problems, such as low real-time data and high distortion. The application of a decentralized, disintermediated, and trustless system of blockchain can save substantial research and decision-making time, simplify the government data review and processing process, and reduce the workload of data resource review, circulation, and sharing in the entire process. Thus, it can improve the efficiency of data governance and provide more efficient and convenient services for various departments, social organizations, and people (Zhang, 2020).

Blockchain technology is conducive to enhancing data protection and ensuring data security. As the hub of government data aggregation, the government is vulnerable to various network attacks, which may lead to major security accidents, such as data leakage and loss. How to improve the security management of government data is a major issue that governments have long been concerned about and explored. Blockchain distributed technology, timestamp technology, and other technologies can achieve full node storage of data with traceability and improve the security of data storage; data can be stored in any node and recorded completely, which greatly reduces the possibility of data theft and disclosure; each node has an independent data management key, which makes the operation management and maintenance of government data more secure.

Blockchain technology is conducive to improving the regulatory mechanism and avoiding the risk of data trust. In the development process of data governance, many problems, such as poor data supervision and uneven data quality, have led social institutions and the masses to question the effectiveness of government data. Blockchain technology can record and authenticate all kinds of government data without going through the central database, thus ensuring that data are open, transparent, and traceable. At the same time, given that blockchain technology cannot be tampered with, once the government data is generated, it realizes the unique record and cannot be erased or modified and achieves the purpose of technical supervision, thus avoiding the risk caused by lack of supervision. This data operation mode realizes the supervision of the entire process of data operation, which largely avoids the risks of data fraud and administrative fraud, thus enhancing the trust of social organizations in government data.

3.2 Theoretical logic of building a blockchain–based intelligent platform for government data

The traditional government data governance work mode is attached to the pyramidal centralized structure, with the central government's data platform as the decision-making center. This mode, to a certain extent, restricts the autonomy and openness of local government data governance work. By virtue of its technical characteristics, blockchain can realize the reconstruction of the working mode of government data governance and build a new intelligent platform for government data, thus forcing the restructuring of the government power structure and organizational reform, realizing the voice and participation rights of citizens, social organizations, and other diverse individuals in data governance; and promoting a virtuous circle of government data governance (Zhang et al., 2021).

Decentralization of organizational power structure. The decentralized distributed data storage mode of blockchain technology changes the organizational departments from an independent single center to a multicenter structure. The point-to-point data transmission mode makes all departments (nodes) be in an equal position, and single functional departments no longer have the sole interpretation and voice of data, thus promoting the transformation of government roles and functions and the development of the organizational power structure in the direction of flattening.

De-artificialization of data processing. The tamper-proof feature of blockchain ensures data authenticity and security. In the sorting process, automatic verification and partial processing of data can be achieved to avoid manual verification errors, reduce labor costs, and improve the effectiveness of data processing.

Diversification of departmental data sharing. In the current government service mechanism, government functional departments mainly exhibit serial or parallel multisectoral cooperation and often present a cooperative relationship centered on a certain department in practical work. Blockchain technology can establish a trust mechanism between government departments and aggregate the parallel physical departments in the virtual data level to achieve a decentralized cooperation model among departments and achieve more complex cooperation relationships in data sharing.

3.3 Technical logic of building a blockchain-based intelligent platform for government data

The various technical characteristics of blockchain directly meet the actual demands of building an intelligent platform for government data, such as consensus mechanism, data uploading mechanism, trustless system, and timestamp, which are important for the realization of the technical logic of the intelligent platform for government data.

Consensus mechanism. As a basic technology to ensure the security, decentralization, and expansion of the blockchain, the consensus mechanism can enable multiple interactive agents to reach an agreement on specific data in a certain manner. Once the consensus mechanism of the blockchain is reached, it cannot be modified or forged, thus ensuring the authenticity, openness, and security of data. The government departments can formulate and improve the consensus mechanism in real time according to their own work adjustment, data collection capacity, and regulatory requirements. In this manner, they can gradually form a data management platform that can meet the actual needs to realize the sharing of data and the automatic mechanism of data processing and achieve the entire process supervision of data flow. At present, when countries apply blockchain technology to government governance, they pay special attention to this technical feature, which is mostly used in democratic consultations, elections, and other occasions.

Data uploading mechanism. The uplinking mechanism achieves the goal of unified data integration standards and also ensures that the data block will be tamper-proof. Data block uploading is a highly relevant link with blockchain technology, and in the construction process of data blocks, cryptography principles, asymmetric encryption technology, and other technologies are comprehensively applied; digital identity authentication and data circulation standards are unified and standardized, and the blockchain formed is able to explicitly record the relevant ownership information of the data information, which is targeted at solving the problems of data integration standards not being able to be unified and data attribution authority issues in the governmental data opening and sharing. Uniformity, data attribution authority problems. For example, when a user initiates a transaction application and requests data to be uploaded to the blockchain, the consensus mechanism is generated in the data open-sharing blockchain, and after calculating the eligibility right of the block and obtaining the right to bookkeeping, the smart contract guarantee mechanism can package and store the publisher's information, and attributes into the data block.

Trustless system. A trustless system means that achieves data security and eliminates the need for a trusted third-party notary subject because data storage and validation are distributed across the nodes of the network, and the nodes reach a unanimous endorsement of the data through a consensus algorithm. In the process of the operation of human society, the state, government, and some public institutions act as the subject of trust guarantee of authority, and risks of trust collapse and authority loss often exist; the trustless system of blockchain technology has well avoided this risk, thereby transferring the guarantee responsibility from the state, government, and social institutions to the technology, realizing the transformation from trusting people and government to trusting technology and data, improving the security of data platform operation, and ensuring the integrity of data information.

Time stamp. Time stamp means that all entities involved in bookkeeping leave unique time information on each block. When the blockchain is generated in chronological order, a database containing all information is naturally generated; given that blocks have time stamps, block data are arranged in chronological order and cannot be modified. Time stamps facilitate the verification and traceability of government data processing and change the post-supervision of data to real-time supervision, thus breaking the formalism of data supervision from the source.

4 Construction of a blockchain-based intelligent platform for government data

4.1 Theoretical model of a blockchain-based intelligent platform for government data

The construction of the blockchain-based government data intelligent platform will rely on a number of key technologies such as point-to-point transmission, encryption technology, smart contract mechanism, timestamp, etc., and give full play to the efficacy of each of these technologies in the process of data governance according to the essential characteristics of each technology, so as to achieve the goal of platform construction and operation. According to this logic, this study proposes a theoretical model of a blockchain-based intelligent platform for government data (as shown in Figure 1).

Point-to-point transmission. The essence of blockchain is a decentralized system composed of point-to-point transmission to maintain the consistency of data records among nodes to establish a distributed "ledger"; this transmission mode can effectively realize the transformation of the governance structure from a centralized "one to many" to a balanced "many to many" to achieve the effect of multisubject cooperation and mutual trust and reasonable expansion of the governance subject.

Encryption technology. As the basic technology for blockchain security, encryption technology also plays an important role in platform construction. This technology enables the platform data to be tamper-proof. The platform can realize automatic verification in the process of data collection and processing and improve the security of data operation.

Smart contract mechanism. The smart contract mechanism is an important embodiment of the autonomy and programmability of blockchain technology. The platform operator can embed the independently set rules and protocols in advance, and the platform can automatically process some data, greatly simplifying the cost of manual processing and improving the efficiency of data governance.

Timestamp. Time stamp technology has significant traceability, which is not only conducive to the openness and transparency of data flow and processing but also provides a new idea for data supervision. It realizes the entire process of supervision of data in a technical manner.

The construction of the platform fully applies the above technical means and characteristics to achieve governance effectiveness, such as diversification of trust subjects, automation of data verification, convenience of data processing, and process of data supervision.

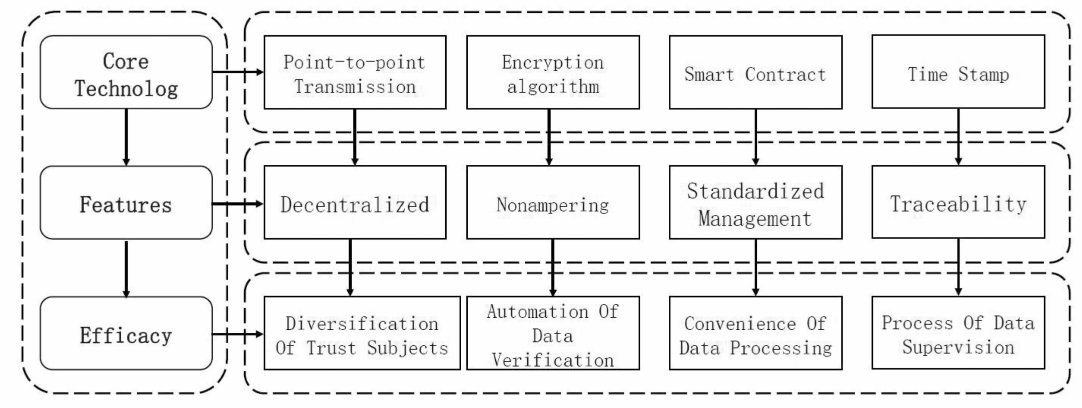
Core Technolog
Point-to-point Transmission
Encryption algorithm
Smart Contract
Time Stamp
Features
Decentralized
Nonampering
Standardized Management
Traceability
Efficacy
Diversification Of Trust Subjects
Automation Of Data Verification
Convenience Of Data Processing
Process Of Data Supervision

Figure 1 Theoretical model of blockchain-based intelligent platform for government data

4.2 Architecture of the intelligent platform for government data

The system construction of the intelligent platform for government data should consider the current era's development background and actual work needs; use various advanced technical means, including blockchain technology; maximize the platform's role as a carrier in government data governance; and coordinate various different types of subject relationships between government functional departments at all levels, central decision-making departments, and social organizations, as well as between internal organizations. This study combines the key technologies and infrastructure logic of the blockchain, and from the perspective of top-level design, constructs the infrastructure of the blockchain-based intelligent platform for government data (Figure 2). It is committed to breaking the data transmission barriers between government departments and the outside, as well as within government departments, and realizing the open sharing of data resources while ensuring data security, supervising data processing throughout the process, and expanding data application fields.

Based on the process of data generation, collection, processing and application, the system construction of the governmental data intelligence platform can be divided into four levels, including the infrastructure layer, the data collection layer, the data processing layer and the data application layer. The central data center platform, as the infrastructure layer, is mainly applied to the aggregation and collection of data from government departments, third-party organizations and other data. The data collection layer applies the mechanism of automatic data collection to collect and sort out data from government departments, third-party agencies, public users, and other parties through the collection of the central data center platform. In the data processing layer, the data collected above are further cleaned and integrated to form effective data resources, which are stored and maintained for application by all parties. The data application layer is mainly open to data users (government departments, think tanks, public users, etc.) to realize the open sharing and interaction of data; at the same time, it establishes a data evaluation and feedback mechanism to provide decision-making references for further optimizing the processing process of the data resources; in addition, it further explores other value-added data services in the application of data according to the actual needs of the data users.

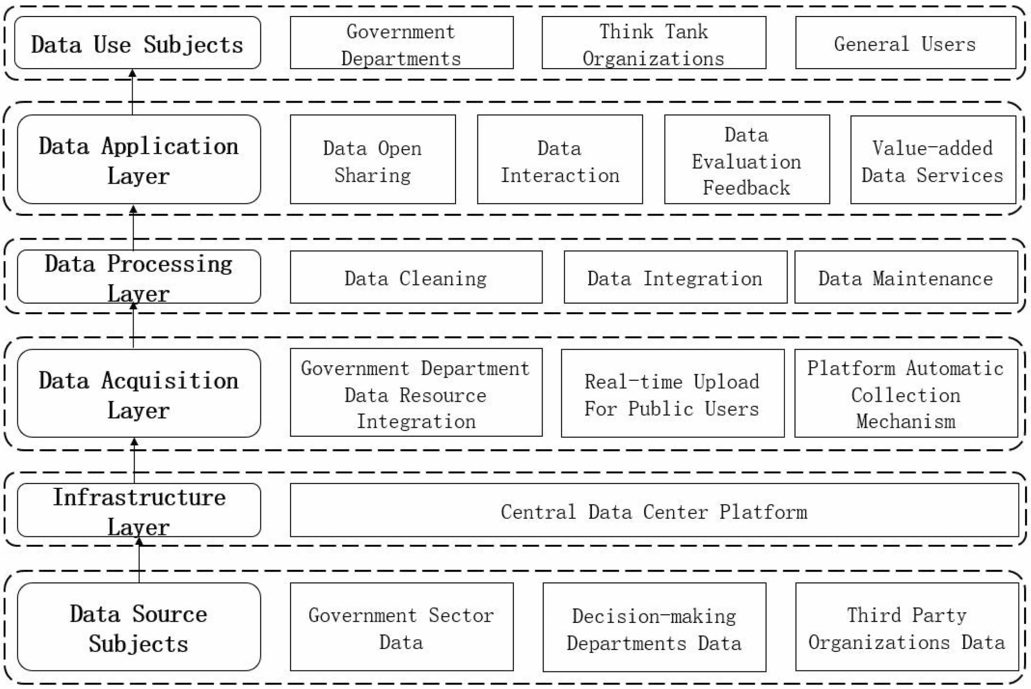

Figure 2 Architecture of the blockchain-based intelligent platform for government data

4.3 Operation mechanism of the intelligent platform for government data

Multisubject mutual trust mechanism. The "decentralized" feature of blockchain technology ensures that all nodes on the chain have relatively equal rights and obligations. All entities in the platform reach a unified consensus and trust and jointly participate in the maintenance and governance of platform data. They have the same authority to store, query, process, and verify data. Data collection, processing, and transmission are achieved in a technical manner, avoiding human errors to the greatest extent. All parallel and vertical associated entities trust each other, achieve maximum data interaction and connectivity, and effectively improve "data islands" and other phenomena.

Data security guarantee mechanism. The hash algorithm, asymmetric encryption algorithm, digital signature, and other encryption algorithms of blockchain technology ensure that data on the chain is tamper proof so that the data collection, storage, verification, processing, and transmission process on the platform are not disclosed while ensuring openness and transparency. "Unless 51% of the nodes in the whole system can be controlled at the same time, the modification of a single node to the database is invalid, and the data content on other nodes cannot be affected" (Wang et al., 2020); to achieve this tampering behavior, huge costs must be invested, which is not feasible in the practical operation level; thus, data security is fully guaranteed.

Data standard management mechanism. During the development of the platform, by using the smart contract mechanism of the blockchain, the rules and protocol contents are set in advance; the rights and responsibilities of each participant for the management and use of platform data are clarified; the detailed requirements of data standards, formats, types, etc. are implemented; and the automatic implementation of technical procedures can achieve the standardized management of platform data, which to a certain extent avoids the problems of inconsistent data standards, confused formats, and fuzzy permissions.

Data process supervision mechanism. The blockchain compresses and encrypts the uplink data through the hash algorithm to form a timing block to ensure that data information is traceable throughout. During the operation of the platform, all data are marked with time marks, and all links and participants in the process of data storage, verification, processing, and transmission are recorded in the chain. In addition, all timestamped data information recorded in the chain is not tampered with, thus realizing the systematic supervision of the entire process of data flow, which helps solve the problem of accurate accountability of relevant participants when data accidents occur.

4.4 Core technology support of the intelligent platform for government data

To realize the effective operation and security supervision of the intelligent platform for government data and prevent the loss and disclosure of sensitive data, we should focus on privacy protection, situation awareness, tracing and traceability, and use machine learning and blockchain-related technologies to achieve government-sensitive information detection, government data authentication and traceability, blockchain-based transaction and node anomaly identification, and other functions.

Government–sensitive information detection technology. The sensitive information detection function of the intelligent platform for government data can effectively reduce the risk of sensitive information leakage. For sensitive electronic documents, the text content containing sensitive information is the core component. It is an important precondition to solve the problem of sensitive information leakage from the internal network to divide electronic documents into different sensitive levels according to the number and importance of sensitive information they contain and archive them. Sensitive information detection technology based on knowledge engineering can classify electronic documents into different sensitive levels according to the number and importance of sensitive information contained in them through certain rules or algorithms. Its workflow is similar to the process of text classification; thus, the detection of the sensitive level of electronic documents can be equivalent to a special text classification method.

Government data authentication and traceability technology. Data validation and traceability are important basic links of government data supervision, recording the evolution information and process of original data in its entire life cycle from generation, transmission, and processing to extinction and emphasizing the process and method of tracking. Blockchain technology provides an effective solution for data authentication and traceability. It uses cryptography and distributed consensus protocols to ensure network transmission and access security. It can achieve multiparty maintenance, cross validation, and network-wide consistency and is not easy to tamper with. The information on the chain is correct, complete, and traceable and thus can provide a unified management method covering the entire life cycle of data collection, transmission, storage, processing, etc., for government data and create conditions for data exchange and information sharing across regions, departments, and levels.

Blockchain-based transaction and node anomaly identification technology. The government affairs data platform based on blockchain technology has frequent transactions and numerous nodes; thus, anomaly detection and real-time supervision must be achieved in the data flow process. On the one hand, blockchain technology is used to explore the correlation between abnormal transactions on the platform to realize real-time prediction of abnormal transactions; on the other hand, in accordance with the data storage mode of blockchain technology, data are divided into blocks in chronological order. The node behavior is chronological, and the behavior of abnormal nodes show abnormal characteristics, which can effectively identify abnormal node operations and avoid risks.

5 Implementation path of building a blockchain-based intelligent platform for government data

5.1 Promotion of technology upgrading and establishment of a data supervision platform based on blockchain

The first step is to establish a data supervision platform based on blockchain. As a decentralized distributed peer-to-peer trusted data network technology, blockchain provides a technical basis for establishing trusted, peer-to-peer data security sharing supervision. Research on a decentralized government information resource sharing model based on blockchain provides a new perspective to understand the decentralized government information resource sharing model. Therefore, exploring a decentralized government data intelligent supervision platform based on blockchain provides a new solution for building a government information resource sharing platform with high security, trustworthiness, traceability, and wide sharing scope. The second step is to use blockchain to realize the authentication and traceability of new sensitive data. Blockchain technology can help meet the requirements of reliable and accurate traceability of sensitive data of government data management in a long and complex environment and support the security and reliability of e-government data and the stable supervision of processes, such as request, handling, query, and traceability of government-sensitive data. The third step is to use the blockchain to improve the new behavioral risk control mechanism. The blockchain system needs a new type of accurate anomaly identification mechanism to achieve efficient prediction of blockchain abnormal transactions and accurate and rapid identification of node abnormal behavior and support the safe flow of government data and reliable multilevel supervision.

5.2 Improving the top-level design and the system of platform construction

The first step is to improve the market access system. The market access permit and access system must be established and improved in accordance with the security assurance capability. A strict standard system must be set for the system developer's independent technology research and development capability, data security assurance capability, and emergency response capability. Solutions to possible network security problems and personal information protection plans must be formulated and reviewed by the competent department. The second step is to refine the market operation system. The production and operation specifications of system suppliers and network operators should be further refined to improve information collection, use and disclosure specifications of consumers, and establish the insurance system, network security system and user information protection system after entering the market. The third step is to restrict the use of scenarios strictly. Personal information processors shall standardize personal information processing and strengthen personal information protection in accordance with the Personal Information Protection Law of the People's Republic of China and other legal provisions. The fourth step is to establish punishment measures for violations. With reference to the relevant provisions of the Data Security Law (draft) and in accordance with the risk level of violations and consequences, violations are further classified and detailed, and detailed and perfect punishment measures for violations are set. The competent department shall continuously supervise and regularly review the implementation of relevant specifications, standards, and systems and strictly punish violations.

5.3 Strict supervision and regulation and improvement of the safe and controllable supervision system

The first step is to establish a local government central data center for data supervision. Data centers at all levels are connected to the central data center. The central data center supervises, collects, cleans, stores, and transmits enterprise data in a unified manner to avoid loopholes in enterprise cloud servers. The department needs to apply for data, and the central data center desensitizes data or conducts privacy calculation after review and transfers or delivers the data to the enterprise as needed. The second step is to establish a hierarchical dispatching command platform. The central, provincial, and local dispatching command platforms are established, connecting the central data center, system suppliers, and network operators to make real-time decisions; the local platform is commanded by the central and provincial platforms. In case of emergency, the local platform conducts unified dispatching in accordance with the command. The third step is to strengthen the supervision of foreign platforms. Foreign systems and related products must strictly comply with China's market access and operation regulations and build cloud servers (data centers) in China. Personal information and important data that are collected and generated in China must be stored in China and managed by the central data center and cannot be provided overseas. If overseas information must be provided due to business needs, it shall apply and report to the central data center.

5.4 Strengthening collaborative research and judgment and forming a hierarchical emergency management system

The first step is to establish a coordination mechanism between departments. With reference to the practices of Shenzhen and other places, the data management department takes the lead in establishing a network vulnerability prevention mechanism and emergency response mechanism for cooperation among departments and maintaining the timely involvement of security protection when necessary. The second step is to dispatch technical management supervisors. The government assigns technical management supervisors to system suppliers and network operators to supervise and manage technology and data and ensure that all data must be uploaded to the central data center. The enterprise sets up an emergency contact group for network security issues, with senior managers in charge of dealing with possible security issues in a timely manner. The third step is to improve the ability to study, judge, and warn. We should establish a dynamic security monitoring mechanism; continue to monitor the platform operation dynamically; analyze, evaluate, and dispose of potential security threats in time; form a case database; use intelligent analysis tools, such as artificial intelligence and cloud computing, to prestudy and prejudge potential security problems; deploy corresponding solutions in advance; and improve security defense capabilities.

5.5 Improving technical support and building an operational talent team with appropriate capabilities

The first step is to implement responsibility training for relevant personnel. Government data governance involves the confidentiality requirements of corresponding levels. Before it is formally implemented, job responsibility requirements, confidentiality timeliness, etc., should be clearly standardized. At the same time, in the operation and maintenance of the supervision platform, a certain degree of technical ability is required. Training and assessment standards should be set for its relevant technical application level to achieve the matching of talents and technology and form a professional operation team. The second step is to strengthen management participation in the platform development process. A professional operation team should not only meet the current work needs but also deeply participate in the development process of the early-stage platform, make the design and conform to the established operation and maintenance management requirements, strictly manage the entire process of software development, grasp the progress of the project, and improve the quality of project construction effectively. The third step is to conduct the cooperative training of scientific research units in colleges and universities. The government, enterprises, universities, and research institutes should maximize their respective advantages and expertise, strengthen cooperation, and form a cooperative talent training mechanism combining government, industry, university, and research. We should take various policy incentives to cultivate professional and technical talents to meet the needs of the development of the field based on demand.

6 Conclusion

The government data intelligence platform based on blockchain technology is a promising research field. Other current theories are more based on a certain area of government work to carry out application research, while this paper builds a government data intelligence platform that can provide a safe and trustworthy solution for data collection, supervision, and application sharing, which is more pervasive and universal in specific applications; in addition, in terms of the path of realization is also put forward based on technological upgrading, top-level design, institutional support, and other dimensions, which is richer. However, the field also faces challenges such as performance scalability, compliance, and standardization. Future research should focus on solving these problems and continuously improving the application of blockchain technology in the field of governmental data. Overall, a government data intelligence platform based on blockchain technology has great potential to enhance government effectiveness, safeguard data security, and promote digital transformation.

References

Bacic, E. M. (1990, December). The Canadian trusted computer product evaluation criteria. In *Proceedings of the Sixth Annual Computer Security Applications Conference* (pp. 188–196). IEEE.

Chao, N. P. (2018). The foreign governments´ practice and governance of the blockchain technology. *Frontiers, 148* (12), 44–50.

Cheng X. J. (2021). International experience and Chinese strategy of blockchain technology regulation. *China Business and Market, 2021* (3), 31–43.

Dai, C. C., Luan, H. J., Yang, X. Y., Guo, X. B., Lu, Z. H., Niu, B. F. (2021). Overview of blockchain technology. *Computer Science, 48* (S2), 500–508.

Didraga, O. (2015). Risk management in future Romanian e–government 2.0 Projects. *Studia Universitatis Vasile Goldis, Arad–Seria Stiinte Economice, 25* (3), 11–22.

Gao, Y. N., Liu, F., & Chen, Y. G. (2018). Summary of information security risk management standard system. *Journal of Information Security Research, 4* (10), 928–933.

Jahl, C. (1991, January). The information technology security evaluation criteria. In *Proceedings–13th International Conference on Software Engineering* (pp. 306–307). IEEE Computer Society.

Liu, J., Zhou, X. L., & Bai, X. Y. (2019). Research on the application of blockchain in government affairs system. *Cyberspace Security, 2019* (11), 15–20.

Qi, X. X. (2018). Application of blockchain technology in government data governance: Advantages, challenges and countermeasures. *Journal of Beijing Institute of Technology (Social Sciences Edition), 2018* (5), 105–111.

The Central People´s Government of the People´s Republic of China. (2022a). *The proposals of the central committee of the communist party of China for formulating the 14th five–year plan for social and economic development and future targets for 2035.* http://www.gov.cn/zhengce/2020–11/03/ content_5556991.htm

The Central People´s Government of the People´s Republic of China.(2022b). *Circular of the general office of the state council on issuing the guidelines for the construction of the national integrated government big data system.* http://www.gov.cn/zhengce/content/2022–10/28/content_ 5722322.htm.

Wang, Q., Li, F. J., Wang, Z. L., Liang, G. J., & Xu, J.(2020). Principle and core technology of blockchain. *Journal of Frontiers of Computer Science & Technology, 14* (10), 1621–1643.

Xi, J. P. (2019, October 26). *Taking blockchain as an important breakthrough in independent innovation of core technology, and accelerating the development of blockchain technology and industrial innovation.* The People´s Daily.

Zhang, L., Liu, B. X., Zhang, R. Y., Jiang, B. X., & Liu, Y. J. (2019). Overview of blockchain technology. *Computer Engineering, 45* (05), 1–12.

Zhu, W. J. (2020). Theoretical investigation on social governance innovation driven by blockchain technology. *E–Government, 2020* (3), 41–53.

Zhang, N. D. Y. (2020). Blockchain governmental services: Empowerment and administrative decentralization. *Chinese Public Administration, 2020* (1), 69–76.

Zhang, C. M., & Fang, Y. (2021). On government data open sharing and its management from the architecture of block chain. *Journal of Nantong University (Social Sciences Edition), 37* (6), 60–70.