Scientific and Social Research, 2025, Volume 7, Issue 2
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Constructing a Data Security and Sharing Mechanism for Smart Cities Based on Blockchain Technology

Yu Wu*

Guangxi City Vocational University, Nanning, Guangxi, China

Corresponding author: Yu Wu, y1u2@hotmail.com

Abstract: With the rapid advancement of smart city construction, data has become a core element of urban development. However, traditional data management models face numerous challenges in ensuring data security and promoting data sharing. Blockchain technology, with its decentralized, tamper-proof, and traceable characteristics, provides a new approach to address data security and sharing issues in smart cities. This article elaborates on the principles and features of blockchain technology, deeply analyzes the current status and dilemmas of data management in smart cities, and focuses on exploring specific schemes for constructing a data security and sharing mechanism based on blockchain technology. The article also demonstrates the application effects through practical cases and concludes with an outlook on the technology's application prospects in smart cities, aiming to provide theoretical support and practical reference for promoting the healthy development of smart cities.

Keywords: Smart city; Blockchain technology; Data security; Data sharing

Online publication: March 10, 2025

1. Introduction

In today's digital era, the construction of smart cities is in full swing. According to relevant data, more than half of the global population already lives in cities, and this proportion is expected to reach 70% by 2050. The rapid development of cities has brought massive amounts of data, covering various fields such as transportation, healthcare, energy, and the environment. For example, in the transportation sector, intelligent transportation systems collect data on vehicle speed, location, and traffic flow through sensors. In the healthcare sector, hospital electronic health record systems store large amounts of data such as patient information, diagnosis results, and treatment records. This data holds significant value and can provide powerful support for city planning, management, and services.

However, issues of data security and sharing are also increasingly prominent. On the one hand, frequent data breaches have caused severe losses to individuals and society. For instance, in 2023, a well-known e-commerce platform experienced a data breach, exposing the personal information and shopping records of millions of users and sparking widespread social concern. On the other hand, the phenomenon of data islands is severe, and data sharing and circulation between different departments and institutions are difficult, resulting in wasted data resources and hindering the coordinated development of smart cities. For example, the difficulty of sharing data between the healthcare and insurance sectors leads to patients providing a large amount of duplicate information during the claims process, increasing costs and time [1].

This study aims to explore how to utilize blockchain technology to build a secure and efficient data-sharing mechanism, addressing the challenges of data security and sharing in smart city construction. This not only helps improve city management efficiency and service quality but also promotes sustainable city development. In terms of theoretical significance, this study enriches the application research of blockchain technology in the field of smart cities, providing new ideas and methods for the development of related disciplines. In terms of practical significance, the research results can provide valuable references for city managers, technology developers, and related enterprises, driving the progress of smart city construction.

2. Analysis of smart city data security status

2.1. The importance of smart city data

Data plays a crucial role in the construction and development of smart cities. It is not only the link connecting various intelligent systems but also the core driving force for achieving intelligent city management. The operation of smart cities relies on the collection, transmission, storage, and analysis of massive amounts of data, covering various aspects of city management, including traffic flow monitoring, environmental quality analysis, energy consumption statistics, public safety monitoring, and resident life services. Through deep mining and analysis of this data, city managers can achieve optimal resource allocation, precise public service provision, and significant improvements in city operation efficiency [2].

For example, in traffic management, real-time traffic flow data can help traffic departments optimize signal light control and alleviate congestion. In environmental monitoring, air quality data can provide a scientific basis for pollution control. In public safety, the analysis of surveillance data can prevent crime and quickly respond to emergencies. It can be said that the security and integrity of data are directly related to the normal operation of cities and the quality of life of residents. Any problems with the data can affect intelligent city management and may lead to severe social and economic consequences.

2.2. Challenges faced by data security

Despite the irreplaceable importance of data in smart cities, data security issues are increasingly prominent with the continuous increase in data volume and the growing complexity of the technological environment. As the level of city intelligence increases, more and more devices and systems are connected to the network, and data collection and transmission links are constantly increasing, which significantly raises the risk of data breaches. For example, vehicle driving data in intelligent transportation systems, surveillance video data in intelligent security systems, and personal medical data in resident health management systems may all be leaked due to network attacks, system vulnerabilities, or human error [3]. Once this sensitive data falls into the hands of

lawbreakers, it not only violates residents' privacy but may also lead to identity theft, financial fraud, and other criminal activities, causing huge losses to residents and society.

Smart city data security faces not only technical challenges but also management constraints. From a technical perspective, although encryption technology, access control technology, and data backup technology can ensure data security to a certain extent, the protective capabilities of existing technologies are still insufficient as attack methods continue to evolve. For example, the development of quantum computing technology may pose a threat to traditional encryption algorithms, while the low-security protection capabilities of IoT devices also bring new hidden dangers to data security. From a management perspective, issues such as incomplete data security management systems, weak personnel security awareness, and missing emergency response mechanisms also affect data security to some extent. For example, many city government departments and enterprises lack clear data security responsibility divisions, making it difficult to implement data security management responsibilities. In the event of a data security incident, it is difficult to handle it effectively and timely [4].

3. The application of blockchain technology in smart city data security

Blockchain technology is a data storage and transmission technology based on decentralization and distributed ledgers, featuring tamper-proof data, high transparency, and strong security. Its application scope has far exceeded the financial field, gradually expanding into multiple areas such as smart cities, supply chain management, and the Internet of Things. The core advantage of blockchain lies in its decentralized architecture. Data is no longer centrally stored in a single server or institution but is distributed across multiple nodes, each storing a complete ledger copy. This distributed storage approach significantly enhances data security and reliability because any attempt to tamper with the data requires simultaneous modification of the ledgers on all nodes, which is technically almost impossible. Another important feature of blockchain is the tamper-proof nature of data. Once data is written to the blockchain, it cannot be modified or deleted, providing a powerful guarantee for data authenticity and integrity. Simultaneously, the transparency of the blockchain also offers significant advantages for its application in data security [5]. All transaction records and data changes are transparent to participants, facilitating supervision and auditing and effectively preventing data abuse and fraud. These characteristics make blockchain technology an ideal choice for addressing data security issues in smart cities.

3.1. Applications of blockchain in data security

3.1.1. Encrypted data storage

In smart cities, secure data storage is fundamental to ensuring data security. Blockchain technology encrypts data using encryption algorithms and stores it in a distributed ledger. Each data block generates a unique hash value through a hash function and is linked to the previous data block, forming an immutable chain structure. This encrypted storage method not only ensures data confidentiality but also enhances data integrity and reliability through the redundant storage mechanism of the distributed ledger. For example, in a smart healthcare system, patients' personal health data can be encrypted and stored using blockchain technology. Only authorized medical staff and the patients themselves can access and use this data, effectively protecting patients' privacy.

3.1.2. Data access control

Data access control is a critical aspect of data security management in smart cities. By utilizing the smart contract function of blockchain, fine-grained control over data access can be achieved. Smart contracts are automatically executed contract terms deployed on the blockchain in code form. When preset conditions are met, the contract automatically executes corresponding operations. In smart cities, smart contracts can set permissions and rules for data access, ensuring that only authorized users can access specific data. For example, in a smart transportation system, traffic management departments can set access permissions through smart contracts, allowing only certified traffic management personnel and related technical staff to access traffic flow data and surveillance video data. This blockchain-based access control mechanism not only improves data security but also reduces human intervention and management costs [6].

3.1.3. Data traceability and verification

Data traceability and verification are essential for data security management in smart cities. Blockchain technology can record the source and change history of data. Each data block includes a timestamp of data generation, data content, and data source information. Through the distributed ledger of the blockchain, users can easily trace the source and change process of data, verifying its authenticity and integrity. For example, in the energy management system of a smart city, blockchain technology can record the generation, transmission, and usage of energy consumption data, ensuring data accuracy and reliability. Once data abnormalities are detected, the source of the problem can be quickly located through the blockchain's traceability function, and measures can be taken promptly. This data traceability and verification mechanism not only helps prevent data tampering but also provides strong support for data auditing and regulation.

3.2. Practical cases of blockchain technology in smart cities

Shenzhen, as one of the leading cities in China's smart city construction, actively explores the application of blockchain technology in the field of data security. In the field of smart government services, the Shenzhen government has built an electronic license sharing platform using blockchain technology, storing residents' ID cards, driver's licenses, business licenses, and other electronic license information on the blockchain. Through smart contracts, different departments can share and verify license information safely and efficiently, greatly improving the efficiency and transparency of government services [7]. Simultaneously, blockchain technology is also applied to the smart transportation system, ensuring the security and integrity of traffic flow data and surveillance video data through encrypted storage and data traceability functions. These applications not only enhance the intelligence level of city management but also effectively protect residents' privacy and data security.

Amsterdam is one of the global models for smart city construction. The city has introduced blockchain technology in the field of energy management. Through the blockchain platform, Amsterdam has achieved distributed energy trading and management. Residents and businesses can buy, sell, and exchange energy through the blockchain platform. All transaction records are encrypted and stored on the blockchain, ensuring transaction transparency and security. Simultaneously, blockchain technology can monitor energy production, transmission, and consumption processes in real time, providing accurate data support for energy management. This blockchain-based energy management system not only improves energy utilization efficiency but also promotes the development of renewable energy, providing strong support for the sustainable development of the city [8].

4. Constructing a data-sharing mechanism for smart cities based on blockchain

4.1. Demands and challenges of data sharing

In the construction of smart cities, data sharing is a key link to achieve efficient city management and services. Various departments need to share and exchange data to break information islands and improve the city's operational efficiency and collaborative abilities. For example, traffic management departments need to share data with meteorological departments to optimize traffic signal control, and the medical system needs to share data with social security departments to provide precise medical services. However, traditional data-sharing methods face many challenges, limiting the efficiency and security of data sharing.

Firstly, the problem of data islands is a prominent contradiction in smart city construction. Different departments have difficulties in data circulation and sharing due to differences in system architecture, data format, and management mechanisms. For example, public security department monitoring data, environmental monitoring data from environmental protection departments, and traffic flow data from transportation departments are often stored independently, making it difficult to integrate and collaboratively analyze them [9].

Secondly, data inconsistency seriously affects the effectiveness of data sharing. Due to different data update frequencies, data formats, and standards among departments, there are significant discrepancies in the accuracy and consistency of shared data. For example, different departments may have different descriptions of the same location's geographic information, leading to misunderstandings and errors when data is used across departments.

Finally, the risk of data leakage is a non-negligible security hazard in the data-sharing process. In the traditional data-sharing model, data is often transmitted and stored through centralized servers, making it a target for network attacks. Once data is leaked, it can damage residents' privacy and may cause serious social and economic problems.

4.2. Data sharing mechanism based on blockchain

To solve the aforementioned problems in data sharing, a data-sharing mechanism based on blockchain technology has emerged. The decentralization, immutability, and transparency of blockchain provide a new solution for efficient data sharing in smart cities.

4.2.1. Establishing a distributed data-sharing platform

Utilizing blockchain technology to establish a distributed data-sharing platform can effectively solve the problem of data islands. On this platform, data from various departments is no longer centrally stored on a single server but is distributed across multiple nodes, with each node storing a complete data copy. This distributed architecture not only enhances data security but also increases the system's fault tolerance. For example, when one node fails, other nodes can still operate normally, ensuring data availability. Additionally, the consensus mechanism of the blockchain ensures data consistency and integrity across different nodes, preventing data tampering or loss.

4.2.2. Developing data sharing standards and protocols

To ensure data accuracy and consistency, it is essential to establish unified data-sharing standards and protocols. In smart city construction, differences in data formats and standards among departments can pose significant difficulties for data sharing. Through blockchain technology, data sharing standards and protocols can be embedded in smart contracts, ensuring that data follows unified rules during the sharing process. For instance,

the transportation and environmental protection departments can negotiate and develop a common data format and standard, encoding it into a smart contract. When data is shared between the two departments, the smart contract automatically verifies the data format and content, guaranteeing accuracy and consistency.

4.2.3. Utilizing smart contracts for automated data exchange

Smart contracts are a core function of blockchain technology, capable of automatically executing preset contract terms without human intervention. In data sharing for smart cities, smart contracts enable automated data exchange and verification among departments, improving the efficiency and security of data sharing. For example, when the transportation management department needs real-time meteorological data from the meteorological department, a smart contract can automatically trigger the data exchange process based on preset rules. The meteorological department's server sends data to the blockchain platform. After the smart contract verifies the data's integrity and accuracy, it automatically transmits the data to the transportation management department. The entire process requires no manual operation, saving time and labor costs while reducing the possibility of human error.

5. Conclusion and outlook

This article explores the construction of a data security and sharing mechanism for smart cities based on blockchain technology. By establishing a distributed data-sharing platform, developing data-sharing standards and protocols, and utilizing smart contracts for automated data exchange, this mechanism offers significant advantages in improving data security and sharing efficiency. Experimental results demonstrate that the data-sharing mechanism based on blockchain can effectively address issues such as data islands, data inconsistency, and data leakage present in traditional data-sharing models. This provides strong support for efficient management and collaborative services in smart cities [10].

Disclosure statement

The author declares no conflict of interest.

References

[1] Zhang QH, Gao Q, 2024, Exploring the Application of Big Data and Blockchain Technology in Smart City Data Security Management. Information Recording Materials, 25(11): 117–119 + 123. https://doi.org/10.16009/j.cnki.cn13-1295/tq.2024.11.051

[2] Zhou Y, 2024, Research on Data Storage and Sharing Scheme Based on Blockchain Supporting Fair Payment, thesis, Xi'an University of Technology. https://doi.org/10.27398/d.cnki.gxalu.2024.000316

[3] Guo J, 2023, Smart City Communication Data Security Sharing Method Based on Blockchain Attribute Encryption. Proceedings of the 2023 Third International Academic Conference on Innovative Talent Training and Sustainable Development. https://doi.org/10.26914/c.cnkihy.2023.014404

[4] Zhao WJ, 2022, Blockchain Has Huge Potential in Smart City Applications. China Information World, 2022(3): 62–65.

[5] Zeng HX, 2022, Decentralized Ciphertext Data Security Sharing Based on Blockchain in Smart Cities, thesis, Xidian

University. https://doi.org/10.27389/d.cnki.gxadu.2022.002877

[6] Li CF, Shi MY, 2021, Introduction to Big Data Technology. Communication University of China Press, Beijing.

[7] Lu J, 2022, Blockchain Engineering Practice. Machinery Industry Press, Beijing.

[8] Han YS, 2021, Exploring the Application of Government Big Data in Smart City Construction — Taking the Construction of "Cloud Yangzhou" as an Example. New Industrialization, 11(10): 38–44. https://doi.org/10.19335/j.cnki.2095-6649.2021.10.005

[9] Li Y, 2019, Winning the Financial Security 3.0 Era — New Finance + New Technology + New Security. Posts and Telecommunications Press, Beijing.

[10] Rao ZH, 2020, Internet of Things Network Security and Applications. Electronic Industry Press, Beijing.