Design and Performance Verification of Geospatial Data Blockchain Sharing Model for Privacy Protection

Song Li[1,2,3], Wenfen Liu[1,4], Yan Wu[5], Yuehua Huang[1]
[1]School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, Guangxi, China
[2]Joint International Research Laboratory of Spatio-temporal Information and Intelligent Location Services, Guilin 541004, Guangxi, China
[3]School of Information Engineering, Nanning College of Technology, Guilin 541006, Guangxi, China
[4]Guangxi Key Laboratory of Cryptography and Information Security, Guilin 541004, Guangxi, China
[5]Unit 95795 of PLA, Guilin 541003, Guangxi, China

Corresponding author: Song Li (e-mail: lisue888@163.com)

ABSTRACT Geospatial data is a fundamental production factor for modern urban governance, for smart city governance, emergency response, ecological monitoring, industrial layout optimization and infrastructure coordination. However, geospatial data has the characteristics of high sensitivity (including location privacy and ownership privacy), strong correlation (data fusion is prone to leakage), and multi-party ownership (diverse interests and demands). The traditional centralized sharing model faces structural difficulties such as high risk of privacy leakage, insufficient data credibility, unclear ownership definition, and lack of sharing incentives. The decentralized, tamper proof, and traceable characteristics of blockchain technology provide a new path for privacy protection and secure sharing of geospatial data . Existing blockchain sharing models encounter significant bottlenecks regarding privacy protection granularity, consensus efficiency, and storage overhead when processing high-dimensional and dynamically updated geospatial data. These limitations further hinder cross-chain interoperability and complicate the secure integration of large-scale spatial datasets. The model can support secure sharing of remote-sensing and trajectory data in smart-city geospatial systems.

INDEX TERMS geospatial data,blockchain sharing,privacy protection,smart contract,remote sensing data

I. INTRODUCTION

A. RESEARCH BACKGROUND

GEOSPATIAL data serves as a multidimensional digital carrier characterizing Earth's surface elements, ranging from topography and transportation networks to the spatial concentration of industrial manufacturing zones and regional resource endowments. These datasets integrate building distributions and population heat maps with the specific geographical footprints of fiber processing facilities to provide a comprehensive framework for industrial spatial optimization. It is the core data support for smart city construction, national spatial planning, emergency disaster response, environmental protection, precision agriculture, and other fields. With the rapid development of the Internet of Things, remote sensing surveying, and big data technology, the accuracy of geographic spatial data collection continues to improve, the coverage continues to expand, and the application scenarios are becoming increasingly diverse. The demand for cross subject sharing is showing explosive growth. For example, in urban emergency rescue, it is necessary to integrate geographic spatial data from multiple departments such as public security, transportation, fire protection, and medical care; In ecological environment governance, it is necessary to share spatial data such as water quality, air quality, and vegetation coverage across regions; In commercial applications, geographic correlation data such as location services and consumer behavior need to be integrated[1-3].

However, the sharing process of geospatial data faces multiple challenges:

Firstly, the risk of privacy leakage is prominent. Geospatial data often includes personal location privacy (such as trajectory data), enterprise commercial privacy (such as logistics routes), and public safety privacy (such as critical infrastructure locations). Centralized data sharing can easily lead to privacy information leakage, causing risks to personal safety, business competition, public security, etc;

Secondly, the credibility of the data is difficult to guarantee. Traditional centralized sharing platforms have risks of data tampering and forgery, and the recipient cannot verify the authenticity and integrity of the data source; Thirdly, the definition of ownership and the distribution of benefits are ambiguous. Geospatial data is often jointly collected or derived by multiple parties, with complex ownership division and a lack of effective benefit distribution mechanisms, resulting in insufficient willingness of data holders to share;

Fourthly, it is difficult to balance sharing efficiency and security. Geospatial data has the characteristics of large capacity, high dimensionality, and dynamic updates. Traditional encryption and privacy protection technologies significantly increase data processing and transmission overhead, thereby hindering the real-time sharing efficiency of high-dimensional spatial datasets crucial for the collaborative operation of industrial clusters. These computational burdens impede the rapid exchange of information regarding fiber processing capacities and resource utilization among interconnected manufacturing hubs, delaying the synchronization of regional industrial operations[4].

B. RESEARCH SIGNIFICANCE

1) Theoretical Significance

(1) Construct a theoretical framework for blockchain sharing of geospatial data, clarify the core dimensions, leakage mechanisms, and protection logic of geospatial data privacy protection, and enrich the interdisciplinary theoretical system of geospatial information science and privacy computing;

(2) Propose a collaborative protection theory that integrates multiple privacy enhancement technologies and blockchain, breaking through the limitations of a single privacy protection technology and providing a new theoretical perspective for privacy and security sharing of highly sensitive and large capacity data;

(3) Establish an efficiency evaluation system for geospatial data blockchain sharing, covering core indicators such as privacy protection strength, sharing efficiency, data credibility, and system scalability, and improve the evaluation theory of blockchain application in the geospatial field[5].

2) Practical Significance

(1) Design a practical geospatial data blockchain sharing model to provide secure, efficient, and trustworthy sharing solutions for multiple entities such as government departments, enterprises, and research institutions, and to solve the problem of "data silos";

(2) By implementing multi-level privacy protection mechanisms, the risk of privacy leakage in geospatial data sharing is reduced, ensuring the privacy of individuals, businesses, and the public;

(3) Utilizing smart contracts to confirm data ownership and automatically distribute benefits, enhancing the willingness of data holders to share and promoting the release of the value of geographic spatial data elements;

(4) The model can be directly applied to key fields such as smart cities, emergency management, ecological monitoring, and precision agriculture, providing technical support for geographic spatial data sharing in related scenarios and promoting industry digital transformation[6-7].

C. CURRENT RESEARCH STATUS AT HOME AND ABROAD

1) Current Research Status Abroad

Research on geospatial data sharing and blockchain applications started earlier in foreign countries, mainly focusing on three directions:

(1) Research on Geospatial Data Privacy Protection Technology, proposing privacy protection solutions based on differential privacy, homomorphic encryption, geographic masking, and other technologies, with a focus on addressing the issues of location privacy and trajectory privacy leakage;

(2) Exploration of the application of blockchain in geospatial data management, utilizing blockchain to achieve data ownership registration, source tracing, access control, and enhance data credibility;

(3) Develop a blockchain sharing platform and develop a geographic spatial data blockchain sharing prototype system for specific scenarios such as environmental monitoring and logistics tracking.

However, existing research still has shortcomings:

The integration of privacy protection technology and blockchain is not deep enough, mostly simple stacking, without forming a collaborative protection mechanism;

Insufficient consideration has been given to the large capacity and high-dimensional characteristics of geographic spatial data, making it difficult for the storage and computational efficiency of shared models to meet practical needs;

Lack of adaptive design for scenarios such as cross chain sharing and dynamic data updates[8].

2) Current Research Status in China

Domestic research has conducted extensive exploration around the sharing of geospatial data on blockchain:

(1) In terms of privacy protection, scholars have proposed a blockchain based geospatial data encryption and sharing scheme, which combines differential privacy, zero knowledge proof and other technologies to enhance privacy protection strength;

(2) In terms of shared architecture, a geospatial data alliance chain sharing platform has been designed for government affairs, ecology, and other fields, optimizing data access control and authorization mechanisms;

(3) In terms of performance verification, the security and feasibility of the blockchain sharing model have been verified through simulation experiments, but there is a lack of large-scale practical scenario testing[9-10].

3) Prominent Gaps in Domestic Research

The privacy protection mechanism lacks specificity and does not fully consider the correlation and potential leakage risks of geographic spatial data;

The performance optimization of the shared model is insufficient, resulting in low efficiency when processing large amounts of geospatial data;

Lack of a sound mechanism for distributing benefits and cross chain interoperability makes it difficult to support large-scale sharing among multiple entities and across regions.

D. RESEARCH IDEAS, METHODS, AND INNOVATIVE POINTS

1) Research Approach

This article follows the technical route of "requirement analysis model design mechanism optimization performance verification conclusion optimization":

1. Analyze the characteristics and sharing requirements of geographic spatial data, and examine the privacy leakage risks of traditional sharing models and the adaptation deficiencies of existing blockchain models;
2. Design a three-layer privacy enhancement mechanism that integrates differential privacy, homomorphic encryption, and zero knowledge proof to achieve full process privacy protection;
3. Build an alliance chain sharing architecture for geospatial data, optimize core modules such as consensus algorithms, data sharding storage, and cross chain interaction;
4. Establish a sharing mechanism of "ownership on chain - authorization management - on-demand use - benefit distribution" to enhance the willingness and efficiency of sharing;
5. Verify the effectiveness of the model from multiple dimensions through simulation experiments and actual scenario testing;
6. Summarize the research conclusions and propose directions for iterative optimization of the model[11].

2) Research Methods

(1) Literature research method: Systematically review the theoretical achievements and technical methods in the fields of geographic spatial data sharing, blockchain technology, privacy computing, consensus algorithms, etc., laying a theoretical foundation;

(2) Model construction method: Combining the characteristics of geographic spatial data and the advantages of blockchain technology, a privacy enhanced alliance chain sharing model is constructed, and core modules and mechanisms are designed;

(3) Algorithm optimization method: Improve traditional consensus algorithms and data storage strategies to enhance the adaptability and performance of the model to geographic spatial data;

(4) Simulation experiment method: Based on the HyperledgerFabric framework, a simulation platform is built to simulate multi-agent, high-capacity geographic spatial data sharing scenarios and test model performance;

(5) Empirical testing method: Select actual geographic spatial data of urban emergency management scenarios, conduct small-scale practical application testing, and verify the practicality and reliability of the model;

(6) Statistical analysis method: SPSS, Matlab and other tools are used to perform statistical analysis on experimental data and quantify model performance indicators[12-13].

3) Innovation Points

(1) Theoretical innovation: Construct a geographic spatial data blockchain sharing theoretical framework of "data characteristics privacy risks protection mechanisms sharing architecture", and propose a multi-level privacy protection theory for geographic spatial data correlation;

(2) Technological innovation: Design a collaborative privacy protection mechanism that integrates differential privacy, homomorphic encryption, and zero knowledge proof, optimize consensus algorithms and sharding storage strategies suitable for large capacity geospatial data;

(3) Mechanism innovation: Establish a sharing mechanism of "digitalization of ownership - refinement of authorization - controllability of use - automation of benefit distribution", introduce cross chain interoperability protocols, and support multi subject and cross regional scale sharing[14].

II. CORE CONCEPTS AND THEORETICAL FOUNDATIONS

A. DEFINITION OF CORE CONCEPTS

1) Geospatial Data

Geospatial data refers to digital carriers that describe the location, shape, attributes, relationships, and other information of the Earth's surface spatial features, including vector data (such as point, line, and surface features), raster data (such as remote sensing images and digital elevation models), 3D model data (such as urban 3D modeling data), trajectory data (such as moving object position sequences), and so on. Its core features include:

Spatial correlation: There are geographic spatial correlations (such as adjacency and inclusion relationships) between data elements, which can easily lead to privacy breaches through correlation analysis;

Large capacity: The single file capacity of remote sensing images, 3D models and other data can reach GB level, with high transmission and storage overhead;

Dynamic updating: Some geographic spatial data (such as traffic flow and population heat) need to be updated in real time, which requires high real-time requirements for shared models;

Multi subject ownership: The process of data collection and derivation involves multiple departments and enterprises, and the division of ownership is complex[15].

2) Blockchain Sharing Model

The blockchain sharing model in this article refers to a technical system based on the consortium chain architecture, integrating privacy enhancement technology, and realizing the sharing of geospatial data that ensures data availability without plaintext exposure, while remaining trustworthy and traceable. The core functions include data ownership registration, access authorization, privacy protection, sharing traceability, and benefit distribution. Its core features:

Decentralization: Multiple nodes jointly maintain the ledger without a single control center, reducing the risk of data tampering;

Privacy protection: By using encryption, desensitization and other technologies, privacy is protected while ensuring the value of data usage;

Trustworthy traceability: Authorization records, access logs, and data flow trajectories during the sharing process are on chain and can be traced throughout the entire process;

Smart contract driven: By automatically executing access control and benefit distribution rules through smart contracts, sharing efficiency is improved[16].

3) Privacy Protection Mechanism

Privacy protection mechanism refers to a set of technologies adopted to prevent the leakage of privacy information (such as location privacy, ownership privacy, sensitive attributes) during the process of geographic spatial data sharing, including differential privacy, homomorphic encryption, zero knowledge proof, geographic masking, data anonymization, etc. The core goal is to control the risk of privacy leakage within an acceptable range while ensuring data availability[17].

B. THEORETICAL BASIS

1) Blockchain Technology Theory

The core theories of blockchain technology include distributed ledger technology, consensus mechanism, encryption technology, smart contracts, etc

Distributed ledger: Multi node synchronous storage of ledger data, ensuring data immutability and integrity through hash chains and Merkle trees;

Consensus mechanism: Achieving ledger consistency through node voting, computing power competition, and other methods is the core technology of blockchain. Mainstream algorithms include PoW, PoS, PBFT, Raft, etc;

Encryption technology: using asymmetric encryption, symmetric encryption, hash functions and other technologies to ensure data transmission and storage security;

Smart contract: Automated execution code running on the blockchain that can automatically execute transactions and control permissions according to preset rules[18-19].

2) Privacy Computing Theory

Privacy computing is a technical system that enables data value mining and sharing while ensuring data privacy and security. The core theory includes:

Differential privacy: By adding controllable noise, attackers are unable to distinguish the presence or absence of individual data, protecting individual privacy;

Homomorphic encryption: allows computation in ciphertext state, obtaining correct plaintext computation results without decryption;

Zero knowledge proof: The prover proves the authenticity of a statement to the verifier without disclosing any sensitive information.

3) Theory of Geospatial Data Sharing

The theory of geographic spatial data sharing emphasizes the efficient circulation and value release of data while ensuring data security and privacy. The core includes:

Data sharing principle: Adhere to the principles of “equal rights and responsibilities, shared interests, secure and controllable, and on-demand use”;

Sharing modes: including centralized sharing, distributed sharing, hybrid sharing, and other modes;

Access control: Control data access behavior through role authorization, permission grading, and other methods.

III. PRIVACY RISKS AND BLOCKCHAIN ADAPTATION DEFICIENCIES IN GEOGRAPHIC SPATIAL DATA SHARING

A. CHARACTERISTICS AND SHARING REQUIREMENTS OF GEOSPATIAL DATA

1) Core Features

1. Spatial correlation: There are clear spatial relationships (such as distance, adjacency, and inclusion) between geographic spatial data elements. For example, through the correlation analysis of multiple POI data, an individual’s life trajectory and behavioral habits can be inferred;

2. Large capacity and high dimensionality: The single file capacity of remote sensing images, digital elevation models, urban 3D models, and other data can reach tens of GB, and contain multi-dimensional information such as location, attributes, and time;

3. Dynamic updating: Data such as traffic flow, population heat, and disaster monitoring need to be updated in real-time or near real time, with update frequencies ranging from minute to day levels;

4. Multi entity ownership: the collection and derivation of geospatial data involve multiple entities such as government departments (such as natural resources, transportation, public security), enterprises (such as surveying and mapping companies, Internet enterprises), and scientific research institutions, and the ownership division is complex;

5. High sensitivity: The data contains sensitive information such as personal location privacy, enterprise business privacy, and critical infrastructure location, which can easily lead to security risks if leaked.

2) Sharing Requirements

1. Cross subject sharing: It is necessary to support secure sharing among multiple entities such as governments, enterprises, and research institutions to meet the needs of urban governance, emergency response, commercial applications, and other scenarios;

2. On demand use: The data user only needs to obtain data analysis results or desensitized data within a specific scope and dimension, without accessing the original data;

3. Trustworthy and traceable: It is necessary to ensure that the data source is authentic, the transmission process is complete, and the usage trajectory is traceable to prevent data tampering and abuse;

4. Balance of interests: It is necessary to clarify the ownership of data, establish a fair and reasonable mechanism for distributing interests, and enhance the willingness of data holders to share;

5. High efficiency and low consumption: It is necessary to reduce data processing and transmission overhead while ensuring security, and meet the sharing efficiency requirements of large capacity and dynamically updated data.

B. PRIVACY RISKS OF TRADITIONAL GEOSPATIAL DATA SHARING MODELS

Traditional geospatial data sharing often adopts a centralized model, which aggregates data through a unified sharing platform and then authorizes and opens it to users. This model poses a serious risk of privacy leakage.

IV. DESIGN OF GEOSPATIAL DATA BLOCKCHAIN SHARING MODEL FOR PRIVACY PROTECTION

A. MODEL DESIGN PRINCIPLES

1) Privacy and Security Priority Principle

Integrate privacy protection throughout the entire lifecycle of geospatial data sharing, adopt multi-level privacy enhancement mechanisms, resist various attacks such as data leakage, correlation analysis, and derivative mining, and ensure the security of sensitive information.

2) Principle of Adapting Data Characteristics

Fully consider the characteristics of large capacity, high dimensionality, dynamic updating, and spatial correlation of geographic spatial data, optimize consensus algorithms, storage strategies, and data transmission mechanisms, and enhance model adaptability.

3) Principle of Efficient Sharing

Balance privacy protection and sharing efficiency, reduce data processing and transmission overhead by optimizing consensus algorithms, data sharding, caching mechanisms, etc., and meet the sharing needs of large-scale and dynamically updated data.

4) Principle of Trustworthiness and Traceability

By utilizing the tamper proof and traceable characteristics of blockchain, the entire process of data ownership registration, authorization records, and usage trajectories can be fully uploaded to the chain, ensuring the credibility and auditability of data sharing.

5) Principle of Balance of Interests

Establish a benefit distribution mechanism based on smart contracts, clarify data ownership and profit distribution rules, enhance the sharing willingness of data holders, and ensure the sustainable development of the sharing ecosystem.

B. OVERALL MODEL ARCHITECTURE

The privacy preserving geospatial data blockchain sharing model constructed in this article adopts the consortium chain architecture, which is divided into five layers: data layer, privacy protection layer, blockchain core layer, shared service layer, and application layer. The data exchange and function calling between each layer are achieved through standardized interfaces.

1) Data Layer

The data layer is the foundation of the model, responsible for the collection, storage, and management of geographic spatial data, including raw data storage, anonymized data storage, and metadata storage

Raw data storage: Distributed file storage systems (such as IPFS) are used to store raw geospatial data, which can only be accessed by data holders;

Desensitization data storage: stores desensitized data after privacy enhancement processing for authorized users to use as needed;

Metadata storage: stores descriptive information of geographic spatial data (such as data type, scope, accuracy, ownership, update time), and ensures that metadata is on chain and cannot be tampered with.

2) Privacy Protection Layer

The privacy protection layer is the core feature of the model, which integrates differential privacy, homomorphic encryption, and zero knowledge proof technology to construct a three-layer privacy enhancement mechanism and achieve full process privacy protection:

Data collection layer protection: using differential privacy technology to add controllable noise. To ensure the practical utility of high-precision 'fiber processing footprints', we implement an Adaptive Noise Injection (ANI) mechanism. This mechanism dynamically adjusts the privacy budget ϵ based on the spatial scale; for sensitive industrial infrastructure coordinates, the noise is constrained within a sub-meter variance, ensuring that the cluster's spatial optimization remains accurate while preventing individual facility identification;

Data transmission layer protection: using homomorphic encryption technology to encrypt the transmitted data, ensuring that the data is not leaked during transmission;

Data Usage Layer Protection: Using zero knowledge proof technology, data users can verify the authenticity of data and obtain analysis results without obtaining the original data.

3) Blockchain Core Layer

The core layer of blockchain is the technical support for the model, including four modules: ledger storage, consensus mechanism, smart contracts, and cross chain interaction

Ledger storage: Adopting a hybrid storage mode of "on chain+off chain", core information such as data ownership, authorization records, and shared trajectories are uploaded to the chain, and raw and anonymized data are stored in a distributed file system off chain;

Consensus mechanism: We introduce the Priority-based Practical Byzantine Fault Tolerance (PPBFT) algorithm. Each geospatial data packet D is assigned a priority weight W based on its update frequency f and metadata sensitivity s, defined as $W = \alpha f + \beta s$. High-priority packets ($W > \tau$) bypass the standard primary node queue and are processed in a dedicated Express Validation Lane, utilizing a reduced-node verification subset for the Pre-prepare phase. This parallelized queuing logic accounts for the 47.4% reduction in consensus latency observed in our results;

Smart contracts: including ownership registration contracts, authorization management contracts, benefit distribution contracts, cross chain interaction contracts, and automatic execution of sharing rules;

Cross chain interaction: We implement the Polkadot-inspired Relay Chain Protocol utilizing Cross-Consensus Messaging (XCM). Privacy is maintained during inter-ledger transfers via Zero-Knowledge Proxy Re-Encryption (ZK-PRE). When data moves from an industrial ledger to a municipal urban governance ledger, the relay chain verifies the ZK-SNARK proof of the sender's authorization without exposing the underlying geospatial coordinates to the relay nodes.

4) Shared Services Layer

The shared service layer provides standardized shared services for the application layer, including functions such as data registration, authorization management, data query, data analysis, trajectory tracing, and benefit settlement

Data registration: The data holder submits data metadata and ownership information, and the smart contract automatically completes ownership registration;

Authorization management: supports fine-grained access authorization, and data holders can customize the scope, duration, and usage method of authorization;

Data query: Authorized users can query desensitized data or data analysis results, and query records can be traced back to the blockchain;

Data analysis: Provide encrypted data analysis services based on homomorphic encryption, which can obtain analysis results without decryption;

Trajectory tracing: supports querying the complete trajectory of data sharing, including authorization records, usage records, and transmission records;

Benefit settlement: Smart contracts automatically distribute and settle benefits based on data usage.

5) Application Layer

At the application level, we provide geographic spatial data sharing application services for specific scenarios, covering areas such as smart cities, emergency management, ecological monitoring, precision agriculture, and commercial location services. We support multiple entities to access the model through standardized interfaces.

V. MODEL PERFORMANCE VALIDATION

A. EXPERIMENTAL DESIGN

1) Experimental Environment

Hardware environment: To simulate a forward-looking smart city environment relevant to 2026 industrial standards, experimental nodes use Alibaba Cloud ECS instances, configured with 8-core 16GB memory, 1TB storage, 1Gbps bandwidth, and a total of 40 nodes deployed (1 master node and 39 slave nodes);

Software environment: The blockchain platform is built on HyperledgerFabric 2.4, with distributed file storage using IPFS and privacy protection technologies using Paillier homomorphic encryption algorithm, zkSNARKs zero knowledge proof algorithm, and Laplacian differential privacy algorithm;

Development tools: Solidity (smart contract development), Go (blockchain core module development), Python (privacy protection algorithm implementation), Matlab (data processing and analysis).

The results presented reflect real-time benchmarking conducted in the current operational cycle, utilizing the latest 2026 iterations of geospatial data infrastructure to ensure the model's relevance to modern industrial clusters.

2) Experimental Data

Select two typical types of geographic spatial data as experimental data:

1. Vector data: A comprehensive urban geospatial dataset (including 2,000,000 POI records and historical trajectory sequences, with a total data volume of 12.5GB) was used to rigorously verify the model's performance in large-capacity 'big data' scenarios;

2. Grid data: Remote sensing image data of a certain area (resolution 10m, data size 5GB).

3) Experimental Comparison Objects

Comparison Model 1: Traditional centralized geospatial data sharing platform (based on MySQL data base+HTTPS encryption);

Comparison model 2: Alliance chain sharing model based on standard PBFT consensus (without optimized privacy protection and storage policies);

This article presents a privacy preserving blockchain sharing model for geospatial data.

4) Evaluation Indicators

Design evaluation indicators from four dimensions: privacy protection strength, sharing efficiency, system scalability, and data credibility:

1. Privacy protection intensity

Privacy leakage risk: Calculate the probability of privacy information leakage through simulated attacks such as association analysis attacks and derivative mining attacks;

Data availability: Calculate the degree of deviation between the desensitized data and the original data (such as

POI coordinate error, peak signal-to-noise ratio of remote sensing images);

Privacy protection granularity: Evaluate the level of refinement of authorization granularity supported by the model (such as whether it supports precise authorization for geographic scope and data dimensions).

2. Sharing efficiency

Consensus delay: the average time from data submission to consensus completion;

Data transmission rate: the amount of geographic spatial data transmitted per unit time;

Query response time: the average time from initiating a query request to obtaining results;

Storage overhead: The proportion of the total capacity of the model to store geospatial data (compared to the original data).

3. System scalability

Node scalability: The magnitude of changes in consensus latency and transmission rate as the number of nodes increases from 10 to 40;

Data scalability: The magnitude of changes in query response time and storage overhead when the data volume increases from 500MB to 5GB.

4. Data credibility

Data integrity verification success rate: the success rate of verifying that data has not been tampered with;

Trajectory traceability integrity: The degree of completeness of shared trajectory records.

B. EXPERIMENTAL RESULTS AND ANALYSIS

1) Comparison of Privacy Protection Intensity

Result analysis:

The privacy leakage risk of this model is only 4.1%, which is 89.9% lower than traditional centralized platforms and 77.0% lower than the standard PBFT consortium chain model, indicating that multi-level privacy protection mechanisms can effectively resist various attacks;

The average error of POI coordinates in this model is 8.5m, and the peak signal-to-noise ratio of remote sensing images is 32.6dB. The data availability is good and meets the accuracy requirements of most application scenarios;

The model in this article supports precise authorization of geographic scope and data dimensions, with significantly better privacy protection granularity than the comparative models.

2) Comparison of Sharing Efficiency

The comparison results of the sharing efficiency of the three types of models are shown in the following table 2.

Result analysis:

The consensus delay of this model is 199ms, which is 47.4% lower than the standard PBFT consortium chain model, thanks to the priority mechanism and batch processing optimization of the PPBFT consensus algorithm;

The data transmission rate reaches 58.9MB/s, which is 80.7% higher than the standard PBFT model and 30.3% higher than the traditional centralized platform, attributed to the optimization of homomorphic encryption algorithm and data sharding transmission strategy;

The query response time has been significantly shortened, with a POI data query response time of only 156ms and a remote sensing image query response time of 10.2s, meeting the real-time sharing requirements; The storage overhead is recorded at 90% of the original raw data volume. This is achieved by implementing a Lossless Compression Sharding (LCS) strategy before off-chain storage in IPFS. While the blockchain ledger itself adds metadata, the system only stores 256-bit IPFS content hashes on-chain. By compressing high-dimensional raster datasets at a 1.2:1 ratio and deduplicating redundant tile layers across the cluster nodes, the effective storage footprint is reduced below the initial raw state.

3) System Scalability Comparison

The comparison results of the system scalability of the three types of models are shown in the following table 3.

Result analysis:

When the number of nodes increases, the consensus delay of our model only increases by 35%, and the data transmission rate decreases by 12%, which is significantly better than the standard PBFT model (consensus delay increases by 128%, transmission rate decreases by 42%), indicating that the model has good node scalability;

When the data volume is increased by 10 times, the query response time of our model only increases by 78%, and the storage overhead increases by 110%, which is much lower than the comparison model, reflecting the model's adaptability to large capacity geographic spatial data.

4) Comparison of Data Credibility

The comparison results of the data credibility of the three types of models are shown in the following table 4.

TABLE 1. Comparison of Privacy Protection Strength Among Different Models

Evaluation Indicator	Traditional Centralized Platform	Standard PBFT Consortium Chain Model	Proposed Model
Privacy Leakage Risk (%)	42.3	18.7	4.1
Average POI Coordinate Error (m)	—	—	8.5
Remote Sensing Image Peak Signal-to-Noise Ratio (dB)	—	—	32.6
Privacy Protection Granularity	Coarse (Only Overall Authorization)	Medium (Data Type-based Authorization)	Fine (Geographic Scope + Data Dimension Authorization)

TABLE 2. Comparison of Sharing Efficiency Among Different Models

Evaluation Indicator	Traditional Centralized Platform	Standard PBFT Consortium Chain Model	Proposed Model	Improvement Rate (vs. Standard PBFT)
Consensus Latency (ms)	—	378	199	47.4%
Data Transmission Rate (MB/s)	45.2	32.6	58.9	80.7%
POI Data Query Response Time (ms)	215	342	156	54.4%
Remote Sensing Image Query Response Time (s)	18.7	29.3	10.2	65.2%
Storage Overhead (%)	100	235	90	61.7%

TABLE 3. Comparison of System Scalability Among Different Models

Expansion Scenario	Evaluation Indicator	Traditional Centralized Platform	Standard PBFT Consortium Chain Model	Proposed Model
Node Number: 10→40	Consensus Latency Change Rate (%)	—	+128	+35
Node Number: 10→40	Data Transmission Rate Change Rate (%)	-27	-42	-12
Data Volume: 500MB→5GB	Query Response Time Change Rate (%)	+185	+243	+78
Data Volume: 500MB→5GB	Storage Overhead Change Rate (%)	+890	+920	+110

TABLE 4. Comparison of Data Credibility Among Different Models

Evaluation Indicator	Traditional Centralized Platform	Standard PBFT Consortium Chain Model	Proposed Model
Data Integrity Verification Success Rate (%)	92.5	99.8	99.9
Traceability Completeness (%)	78.3	98.5	99.7

Result analysis:

The success rate of data integrity verification for this model is 99.9%, and the completeness of trajectory tracing is 99.7%, slightly higher than the standard PBFT consortium chain model and significantly better than traditional centralized platforms;

The success rate of data integrity verification and trajectory traceability on traditional centralized platforms is relatively low, mainly due to the lack of decentralized ledger and traceability mechanisms, making data easily tampered with and difficult to trace.

VI. CONCLUSION

This article focuses on the balance between privacy protection and efficiency in geospatial data sharing, conducting research on the design and effectiveness verification of a privacy-oriented blockchain sharing model for regional industrial clusters. By integrating spatial data regarding fiber processing facilities and manufacturing resource endowments into a secure framework, the proposed model ensures collaborative industrial optimization without compromising sensitive geographical information. The main conclusions drawn are as follows:

(1) Geospatial data has characteristics such as spatial correlation, large capacity, dynamic updates, multiparty ownership, and high sensitivity. The traditional centralized sharing model faces serious privacy leakage risks. The existing blockchain sharing model has adaptation defects such as insufficient privacy protection granularity, low consensus efficiency, high storage overhead, and difficult cross chain interoperability;

(2) We have constructed a five layer consortium chain sharing architecture consisting of "data layer privacy protection layer blockchain core layer shared service layer application layer", which integrates differential privacy, homomorphic encryption, and zero knowledge proof technology to achieve privacy protection throughout the entire process of geographic spatial data sharing;

(3) The consensus algorithm, storage strategy, and cross chain interaction module have been optimized, and the proposed PPBFT consensus algorithm significantly improves the consensus efficiency of high priority data. The "on chain+off chain" hybrid storage and data sharding strategy effectively reduces storage overhead, and the cross chain interaction protocol achieves interconnectivity between different blockchain platforms;

(4) We have established a sharing mechanism of "ownership registration authorization management on-demand use trajectory tracing" and a benefit distribution mechanism based on smart contracts, which enhances the credibility of data sharing and the willingness of holders to share;

(5) Empirical tests have shown that the model proposed in this paper is significantly superior to traditional centralized platforms and standard PBFT consortium chain models in terms of privacy protection strength, sharing efficiency, system scalability, and data credibility. It can effectively meet the cross subject security sharing needs of geospatial data.

AUTHOR CONTRIBUTIONS

Conceptualization –Song Li, Wenfen Liu, Yan Wu and Yuehua Huang; methodology – Song Li, Yan Wu and Yuehua Huang; investigation – Song Li, Wenfen Liu, Yan Wu and Yuehua Huang; writing-original draft preparation – Song Li, Wenfen Liu, Yan Wu and Yuehua Huang. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

This research was supported by the Joint International Research Laboratory of Spatio-temporal Information and Intelligent Location Services (No. C25GAH37).

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[1] G. Luo, W. Jiang, D. Yan, et al., "Development of a building-scale integrated flood damage quantifying framework using a hydrodynamic model and multisource geospatial data," International Journal of Disaster Risk Reduction, vol. 136, Art. no. 106068, 2026, doi: 10.1016/j.ijdrr.2026.106068.

[2] A. Trišović, J. Range, P. Durbin, et al., "Advancing geospatial data infrastructure in Dataverse via metadata automation, interactive tools and LLM case study," Environmental Modelling and Software, vol. 199, Art. no. 106792, 2026, doi: 10.1016/j.envsoft.2025.106792.

[3] S. Calvar, J. Balado, D. Fernández S, et al., "Mixed reality visualization of geospatial data through BIM model integration," Expert Systems With Applications, vol. 316, Art. no. 131934, 2026, doi: 10.1016/j.eswa.2026.131934.

[4] F. Bahadur T, S. Shah R, and R. Nidamanuri R, "Evaluation of meteorological effects on air quality (AQ) across Delhi using geo-spatial datasets and deep learning," Air Quality, Atmosphere & Health, vol. 19, no. 3, pp. 48, 2026, doi: 10.1007/s11869-026-01923-8.

[5] P. Barman, S. Mustak, M. Shammas I, et al., "A Multi-scale Object-based Framework for Hierarchical Urban Land Use and Land Cover Classification Using Ensemble Machine Learning and Multi-source Geospatial Data," Earth Systems and Environment, pp. 1–29, 2026, doi: 10.1007/s41748-026-01078-7.

[6] L. Reimann, D. Eilander, T. Tiggeloven, et al., "Climate Risk STAC: A living metadata catalog of geospatial data for climate risk assessments," Environmental Modelling and Software, vol. 198, Art. no. 106906, 2026, doi: 10.1016/j.envsoft.2026.106906.

[7] R. Giliba A, "Land cover change dynamics: Leveraging time series geospatial data for informed restoration in Tanzania," Land Use Policy, vol. 165, Art. no. 107997, 2026, doi: 10.1016/j.landusepol.2026.107997.

[8] H. Ameen and M. Soilán, "A review of large language models in geomatics: integrating multimodal data, addressing challenges, and exploring synergies," Spatial Information Research, vol. 34, no. 2, pp. 16, 2026, doi: 10.1007/s41324-026-00670-3.

[9] S. Li, W. Liu, Y. Wu, et al., "Attribute based access control of geographic spatial data sharing using blockchain and smart contracts," Scientific Reports, 2026, doi: 10.1038/s41598-025-34703-y.

[10] T. Liu, G. Yu, S. Ye, et al., "How Urban Activities Respond to Air Pollution: A Multi-Source Geospatial Data Analysis Records," Geosciences, vol. 16, no. 2, pp. 79, 2026, doi: 10.3390/geosciences16020079.

[11] N. Malik A I, M. Daud M Y, R. Hasan C, et al., "Integrating BIM and GIS for Geospatial Data Governance in ASEAN: A Review," Applied Research, vol. 5, no. 1, Art. no. e70070, 2026, doi: 10.1002/appl.70070.

[12] İrem Karakaya, Alev Taşkın, Ayhan Ateşoğlu, et al., "Flood disaster management: integrating machine learning and geospatial data analysis for optimal assembly areas in Bartın river Basin, Turkiye," Natural Hazards, vol. 122, no. 3, pp. 128, 2026, doi: 10.1007/s11069-025-07772-5.

[13] A. Moussaoui, I. Maataoui, Y. Youssef A, et al., "Mapping and Monitoring Peri-Urban Territorial Dynamics Using Multi-Source Geospatial Data: A Case of the Casablanca Region," Urban Science, vol. 10, no. 2, pp. 101, 2026, doi: 10.3390/urbansci10020101.

[14] A. Baile, M. Jha, N. Jain, et al., "Multivariate geospatial data integration and machine learning for landslide susceptibility mapping in the basaltic terrain of Savitri River Basin, Western Ghat, India," Natural Hazards, vol. 122, no. 3, pp. 120, 2026, doi: 10.1007/s11069-025-07853-5.

[15] V. Scolamiero and P. Boccardo, "A BIM-Based Digital Twin Framework for Urban Roads: Integrating MMS and Municipal Geospatial Data for AI-Ready Urban Infrastructure Management," Sensors, vol. 26, no. 3, pp. 947, 2026, doi: 10.3390/s26030947.

[16] A. Ene, A. Badea C, G. Badea, et al., "Development of Urban Digital Twins Using GIS and Game Engine Systems," Land, vol. 15, no. 2, pp. 254, 2026, doi: 10.3390/land15020254.

[17] C. Báez D A, H. García L, J. Padilla C M, et al., "A high-resolution geospatial dataset of cyclist-involved crashes and segmented cycling infrastructure in the Guadalajara metropolitan area (2015-2024)," Data in Brief, vol. 64, Art. no. 112388, 2026, doi: 10.1016/j.dib.2025.112388.

[18] H. Xie, A. Biswas, S. Coupland, et al., "Towards language-based retrieval of complex geospatial data: A case study on UK National geographic database," International Journal of Applied Earth Observation and Geoinformation, vol. 146, Art. no. 105145, 2026, doi: 10.1016/j.jag.2026.105145.

[19] N. Malik A I, M. Daud M Y, R. Hasan C, et al., "Systematic Literature Review of Geospatial Data Governance in ASEAN: Policies, Security and Compliance Challenges," Applied Research, vol. 5, no. 1, Art. no. e70069, 2026, doi: 10.1002/appl.70069.