# A Emergency Big Data Management System Model Based on Blockchain

Yu Hong

E-mail: 154945907@qq.com

School of Mathematics and Computer Yuzhang Normal University, Nanchang, 330103, China

**Abstract.** Blockchain, with its technical characteristics of decentralization, consensus mechanism, smart contracts, and non tampering, provides an effective technical means to address issues such as information silos, data security risks, and ineffective collaboration between management departments in the field of emergency management. Analyzed the technical characteristics of blockchain, the compatibility between blockchain technology and emergency management intelligence work, and the compatibility between blockchain technology and emergency logistics systems, based on this, a emergency big data management information system model based on blockchain was proposed, which utilizes blockchain's identity verification, consensus mechanism, traceability, and smart contract functions to improve the quality of emergency management data and achieve a safe and efficient data sharing mode. This has certain guiding significance for the construction of emergency management systems.

**Keywords:** Blockchain; Emergency Management; Big Data Management; System Model

## 1. Introduction

With the rapid development of social economy and technology, the regional public safety situation has become increasingly complex and volatile, and various public emergencies occur frequently. Therefore, improving the comprehensive emergency management ability and modern governance level of the government is particularly urgent and important. However, the current emergency management system still has issues such as data silos, insufficient transparency of information, difficulty in collaboration, and insufficient sensitivity in monitoring checkpoints and public opinion responses, which have reduced the overall efficiency of emergency management collaboration in China's society.The advantages of blockchain technology, such as distributed data storage, decentralization, smart contracts, traceability, and non tampering, naturally align with the basic requirements of efficient collaboration, multi-agent participation, decentralization, effective resource supply, information traceability, and public opinion response in emergency management[1]. At the same time, it can provide sufficient security level. Therefore, how to apply blockchain technology to emergency big data management[2], how to build a blockchain network that can meet the authoritative and trustworthy, efficient interaction, privacy protection, and intelligent sharing needs of emergency big data resources, and then establish an emergency big data management model supported by blockchain network technology, has become the research topic of this article.

ICMEIM 2023, September 08-10, Wuhan, People's Republic of China

DOI 10.4108/eai.8-9-2023.2340071

## 2. Characteristics and Classification of Blockchain Technology

### 2.1 Characteristics of Blockchain

Blockchain is similar to a distributed database, which maintains a chain like structure of data blocks to maintain continuously growing and tamper resistant data records. In a narrow sense, blockchain is a chain data structure that combines data blocks in chronological order, and ensures that it is a distributed ledger that is guaranteed to be tamperproof and unforgeable through encryption[3].

Blockchain is based on multiple core technologies such as distributed storage, consensus mechanism, smart contracts, and data encryption, and has the characteristics of decentralization, security, reliability, traceability, and high degree of automation[4].

Firstly, decentralization. Blockchain is essentially a database that adopts distributed storage and management, without a centralized management center. Unlike traditional centrally managed databases, blockchain adopts end-to-end connections, where the blocknodes on the blockchain have equal status[5]. Each node on the blockchain can access transaction information in the entire blockchain system, and the data on the chain is updated and jointly maintained by each node to achieve decentralization.

Secondly, the reliability of the data is high. When data is uploaded to the blockchain, it needs to be processed through technologies such as encryption and timestamp to ensure the security of the data block. Under the consensus mechanism, modifications to data on the blockchain must be approved by more than half of the nodes in order to take effect[6]. A single person cannot tamper with the data on the chain, thus ensuring the safety and reliability of the data on the chain.

Once again, the traceability of data. The data blocks on the blockchain are organized through a chain structure, with each block connected to the previous block through a hash pointer and connected in chronological order to form a chain[7]. Therefore, any data block information on the blockchain can be viewed as needed, achieving data traceability.

Finally, the degree of automation is high. Blockchain achieves a "trust" state between nodes on the chain through consensus algorithms and smart contract mechanisms, and then automatically exchanges data or executes related programs without human intervention when preset conditions are met.

### 2.2 Classification of Blockchain

Blockchain can be divided into public, private, and consortium chains based on different participants.

***Public BlockChains:*** Refers to the unrestricted use and maintenance of participating blockchains. Any participating party can send transaction information to the chain and obtain effective confirmation, and the information is completely public[3]. Public chain is a completely decentralized blockchain that utilizes cryptographic principles to establish consensus in unfamiliar network environments and form a decentralized credit mechanism. The consensus mechanism in the public chain generally adopts Proof of Work (PoW) or Proof of Interest (PoS).

***Private BlockChains:*** A blockchain whose write permissions are controlled by a certain institution or organization. Private chains are usually built internally by a certain institution, completely closed, and the qualifications of participating nodes are strictly restricted. The operating rules of blockchain systems are set by the institution according to its own needs. The value of private chain is mainly aimed at providing a secure, reliable, traceable, and highly automated computing platform for exchanging data within the organization, while effectively preventing external and internal security threats to data.

***Consortium BlockChains:*** Several organizations collaborate to maintain a blockchain, limited to the participation of alliance members. The read and write permissions and participating accounting permissions on the alliance chain are determined according to alliance rules. Alliance chains are often considered to be partially decentralized. Suitable for application scenarios such as inter institutional transactions and settlements.

The comparison of the characteristics of public chain, consortium chain, and private chain is shown in Table 1.

**Table 1.** Comparative analysis of the characteristics of three types of blockchains

| | **Private Block Chains** | **Consortium Block Chains** | **Public Block Chains** |
|---|---|---|---|
| **Participant** | Within a organization | Alliance members | Anyone |
| **Consensus mechanism** | Distributed consistency algorithm | Distributed consistency algorithm | PoW/PoS/DPoS |
| **Bookkeeper** | Internal determination within the organization | Alliance members to negotiate and determine | All participants |
| **Centralization degree** | Centralization | Polycentrism | Decentralization |
| **Advantage** | Fast transaction speed, low cost, and high security | Fast transaction speed and wider applicability | Low access threshold |
| **Disadvantage** | Easy to manipulate | High performance requirements for nodes, prone to power concentration | Low throughput and slow transaction speed |

## 3. Analysis of the Compatibility Between Blockchain Technology and Emergency Management Work

As a new application mode, blockchain adopts computer technologies such as decentralized storage, encryption algorithms, peer-to-peer transmission protocols, consensus mechanisms, etc., providing a shareable, traceable and distributed database that allows multiple parties to participate in data updates and maintenance, but not tampered, and improves the transparency, security, and operational efficiency of data operations. The above characteristics of blockchain naturally align with the requirements of decentralization and multi-party participation in emergency management.

### 3.1 Analysis of the Compatibility Between Blockchain Technology and Emergency Management Intelligence Work

Blockchain technology enables all entities involved in emergency intelligence work to participate in the collection, processing, and organization of emergency intelligence, and automatically execute various work tasks under the constraints of smart contracts, providing a new and efficient intelligence management and sharing mechanism.

#### 3.1.1. The openness, transparency, and decentralization of blockchain align with emergency management intelligence work.

In the context of information globalization, the flow of emergency management elements and resources is accelerating, and cross domain collaboration among multiple entities has become a new feature of emergency intelligence work. The emergency intelligence work network is essentially a distributed network structure that integrates "human-machine-object" and "citizens social-organizations-government". Sharing real-time updated intelligence information and allocation overview information of personnel, finance, and materials through the public chain of emergency management is beneficial for relevant personnel and the public to timely understand the progress of emergencies and the countermeasures taken by the government. All emergency management agencies and individuals can upload emergency management related data through the public chain, allowing the entire society to participate in emergency management information work, making emergency information resources transparent and open, in order to optimize emergency management of emergencies.

#### 3.1.2. The consensus mechanism of blockchain and the automatic execution feature of smart contracts align with emergency management intelligence work

Smart contracts play a role in automatic execution and application in blockchain. Once an emergency meets the threshold and triggering conditions, relevant operations can be automatically executed without the need for third-party manipulation. Use smart contracts to write emergency warning thresholds and triggering conditions, and automatically execute monitoring and warning tasks in the early stages of emergency management. When an emergency warning is triggered, the emergency intelligence dissemination threshold is automatically triggered, enabling various emergency intelligence work entities to quickly collaborate and collaborate.

#### 3.1.3. The traceability and non tampering characteristics of blockchain align with emergency management intelligence work

Emergency management intelligence information is generally transmitted between government departments and emergency management related organizations, with the characteristics of massive volume and privacy. The alliance blockchain constructed by the government, emergency management departments, and relevant enterprise units is formed through identity authentication services, consensus services, and database services. The data in the blockchain is encrypted using an asymmetric encryption mechanism. Alliance chain members upload data using encryption keys. If they want to obtain information resources on the chain, they must obtain decryption keys to ensure the accuracy of emergency intelligence collection sources. Alliances upload data to the alliance chain to generate a new block, which requires verification and audit from other alliance nodes to ensure the traceability of the generated block data. This helps to reduce disputes arising from intelligence resources and responsibility attribution, while avoiding emergency decision-making failures and management failures caused by false intelligence or malicious tampering.

### 3.2 Analysis of the Compatibility Between Blockchain Technology and Emergency Logistics Systems

In terms of post emergency rescue scheduling for public emergencies, the application of blockchain is conducive to solving key problems such as the allocation of rescue materials and personnel.

#### 3.2.1. Combining blockchain with big data can achieve informationization of emergency logistics management

Firstly, effective processing of emergency materials and personnel information through big data can improve the accuracy of emergency material demand prediction, achieve effective integration of data from various departments and links of emergency logistics, and solve the problem of "fragmentation" of emergency logistics information. Then, further quantify and analyze the indicators of various aspects of emergency logistics, and establish common logistics operation standards and collaborative cooperation models for emergency material suppliers, demanders, and emergency logistics managers through consensus mechanisms, achieving emergency logistics informatization and effectively improving the management efficiency of emergency logistics.

#### 3.2.2. Blockchain enables traceability of emergency logistics

By utilizing the real-time accounting and tamper proof functions of blockchain in data management, emergency logistics management can provide strong technical support for the traceability and anti-counterfeiting of emergency supplies in various logistics links[8]. By introducing various operational links of emergency logistics (including the production, procurement, and storage of emergency materials, as well as the transportation and distribution of materials, etc.) into the blockchain, the full traceability of emergency logistics can be effectively achieved, providing assurance for the quality of emergency materials. When problems occur in logistics, the investigation area for problems can also be accurately located[9].

#### 3.2.3. Smart contracts in blockchain enhance logistics management efficiency

Firstly, blockchain smart contracts enable rapid response to sudden public events. After the occurrence of a public emergency, information should be reported to the government, and materials and resources should be mobilized through the government. Blockchain smart contract technology can achieve rapid response to sudden public event information, providing peer-to-peer human and material services, and improving emergency management efficiency. In addition, through the smart contract function of blockchain, a complete chain of responsibilities can be formed on the blockchain, which can effectively reduce and enhance the trust between emergency logistics management participants and reduce trust costs.

## 4. A Emergency Big Data Management Information System Model Based on Blockchain

Establishing a unified emergency management information system platform is the foundation for blockchain technology to play a role in emergency management. Building an emergency big data management blockchain network with three interconnected public, alliance, and private chains can provide technical support for improving the management efficiency of emergency big data and achieving intelligent emergency management. The emergency big data management system model based on the blockchain network architecture is shown in Figure 1. The blockchain data exchange network consists of network layer, data layer, consensus layer, contract layer, and application layer from bottom to top; Correspondingly, the emergency big data management process from bottom to top includes four functional parts: emergency data collection, data processing, data analysis, and emergency management decision-making and services.

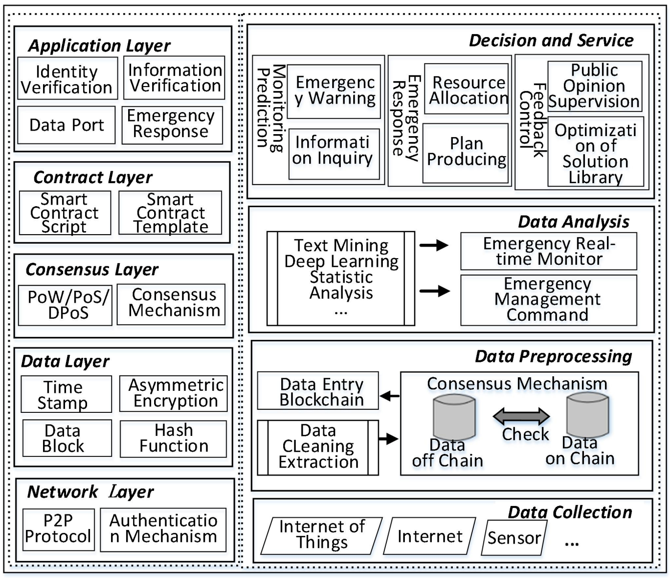


**Fig. 1.** Emergency big data management system model based on the blockchain

### 4.1 Blockchain Data Exchange Network Architecture

***Network Layer:*** mainly providing the most basic distributed data storage and network transmission services, providing P2P data transmission and identity verification mechanisms, ensuring that nodes in the blockchain can perform legitimate operations on blockchain data within their permissions, and jointly maintaining the consistency of the entire blockchain data.

***Data Layer:*** It mainly provides the basic hardware infrastructure and underlying protocols of blockchain, and solves the problems of distributed data storage, data security, and collaborative work through chain structured data blocks, hash functions, timestamps, and asymmetric encryption.

***Consensus Layer:*** Encapsulates consensus algorithms in blockchain systems, such as PoW algorithm, PoS algorithm, DPoS algorithm, etc[10]. Decentralized nodes on the blockchain reach consensus on the effectiveness of block data on the chain through consensus mechanisms, providing guarantees for data consistency on distributed storage nodes.

***Contract Layer:*** The core of the contract layer is smart contracts, which enable the blockchain system to automatically perform data operations when triggering conditions are met through various algorithms and script codes embedded in the blockchain. These operations are traceable but irreversible, effectively improving the trust level of the blockchain and reducing the operational costs of the system.

***Application Layer:*** The application layer provides data application access ports, provides blockchain access services through identity verification, and provides emergency management response services for users. For example, link to user systems of various social organizations and ordinary people by public block chain, link to emergency management security information confidential agency systems by private block chain, and link to systems of various emergency management related departments by alliance block chain.

### 4.2 Emergency Big Data Management Process Based on Blockchain

#### 4.2.1. Emergency data collection

It mainly senses and collects various information related to the management of sudden public events in real-time, and provides it to the data preprocessing layer. The business systems of various emergency management departments act as separate nodes for data collection, which mainly includes the following three aspects:

***Spatiotemporal Big Data:*** mainly includes geographic spatiotemporal basic data and regional specialized spatiotemporal data of a certain region, which can be used to locate and identify risk sources and their real-time changes in the geographical environment, providing data assistance for risk warning and emergency response decision-making.

***Internet of Things System Data:*** mainly includes the physical location and real-time on-site situation information of sudden public events collected by various sensors, intelligent security, intelligent logistics systems, etc., providing data support for emergency management and decision-making.

***Management Information of Government Websites and Public Opinion Data on the Internet:*** By calling the API interfaces of websites and social media platforms to obtain government management information and public opinion related data, public opinion guidance is clarified, providing data support for public opinion control and policy behavior guidance.

#### 4.2.2. Data preprocessing

Emergency data processing mainly includes two stages: data preprocessing and data uploading and publishing.

***Phase 1: Data Preprocessing.*** Clean, filter, and transform the collected raw data according to relevant preprocessing standards, and compare the integrity and consistency of the processed data with the same category of data on the blockchain to meet the requirements of the blockchain consensus mechanism.

***Phase 2: Data Input Blockchain and Fusion Correction.*** The data stored on distributed nodes in the blockchain will be confirmed for validity and entered into the blockchain after meeting the consensus mechanism constraints of both off chain and on chain. Block data is released on public, private, and alliance chains under the supervision of relevant departments in accordance with confidentiality, openness, and compliance requirements.

#### 4.2.3. Emergency data analysis

On the basis of sharing massive emergency data in different chains, aiming at the two major functions of real-time monitoring and emergency management command of the emergency management system, existing algorithms such as data mining, deep learning, and statistical analysis are utilized to fully utilize the technical support functions of big data analysis for management decisions such as public emergency prediction, emergency response, post feedback, and control. Various emergency response plans for public emergencies are constructed to handle models, And componentization is carried out to facilitate the scheduling and use of data and resources by various units involved in management interaction. The typical real-time monitoring system for emergency management includes subsystems such as public opinion monitoring, environmental monitoring, and health and epidemic prevention monitoring. The typical emergency management command system includes: early warning information release subsystem, emergency logistics management subsystem, etc.

#### 4.2.4. Emergency management decision-making and services

From the perspective of the entire lifecycle of emergency management, it can be divided into three parts: pre monitoring and warning, emergency response during the event, and post feedback and recovery.

Before the occurrence of public emergencies, the risk monitoring and early warning system collects real-time data through the data collection layer, preprocesses it in the data layer, and combines it with big data mining models for analysis and prediction in the data analysis layer to form early warning information. Emergency departments can perform intelligent retrieval through the application layer interface of the emergency management system, obtain real-time abnormal dynamics of monitoring checkpoints, and improve their risk prevention capabilities for sudden public events.

When a sudden public event occurs, the emergency management department can obtain the supporting data required for emergency decision-making in real-time across public, alliance, and private chains. For example, the abnormal data of the Internet of Things in the location of the emergency event, emergency plans that can be referenced in the emergency case library, etc., comprehensively improve the quality and efficiency of emergency management decision-making, and minimize the losses caused by the emergency event.

After a sudden public event occurs, it enters the normalized management stage of combining peacetime and wartime. This stage mainly involves monitoring and guiding online public opinion, providing feedback on the previous emergency management results, and adjusting corresponding emergency response plans to address existing problems. In addition, it is necessary to comprehensively evaluate and analyze emergency management, optimize emergency response plans, and update them into the system's case library, forming a virtuous cycle of evaluation and feedback.

## 5. Conclusion

The technical characteristics of blockchain technology in privacy protection, information fidelity, multi-party collaboration, and responsibility traceability naturally align with the requirements of emergency management business. Applying blockchain technology to the field of emergency management can effectively improve the quality and efficiency of emergency management. On the basis of analyzing the compatibility between blockchain technology and emergency management work, this article proposes a blockchain based emergency big data management information system model. This model has the following advantages: (1) utilizing the identity verification and consensus mechanism of blockchain helps to identify the legitimacy and integrity of data collection sources, which is conducive to improving the quality of data on the chain; (2) Through the traceability and smart contract functions of blockchain, a secure and efficient data sharing mode can be achieved. Blockchain technology provides a new approach for government emergency management, but it also brings some challenges: (1) large-scale emergency management data is recorded and circulated through blockchain. In the absence of a unified top-level design, how to achieve cross platform circulation and sharing of data is a challenge. (2) The decentralized characteristics of blockchain have broken the traditional data centralization and centralized management, dispersing the responsibility for data security and confidentiality, and posing a risk of data privacy leakage.

**Acknowledgments.** This work was financially supported by Jiangxi Social Science Planning Project (NO: 19TQ07).

## References

[1] Fan Z.Q, Dai L. The Application of Blockchain Technology in Emergency Management: Hotspots, Challenges, and Prospects[J]. Chinese Journal of Security Sciences,2023, 33 (5):182-190. DOI: 10. 16265/j.Cnki.issn1003－3033. 2023. 05. 1377.

[2] Wu W.J, Sun Y. Research on the Construction of Liaoning Smart Emergency Big Data Management System - Based on the Blockchain Network Perspective [J]. Journal of Liaoning Economic Management Cadre College, Feb 2022.

[3] DOC88.(2018). Analyzing the principles and trends of blockchain technology on the air vent, https://www.doc88.com/p-7724993452680.html.

[4] Wang H.Y, Peng X.C. Architecture Design of Traffic Datacenter Based on Blockchain Technology[J]. Post and Telecommunications Design Technology,2021（10）：73-77. doi：10.12045/j.issn.1007-3043.2021.10.015.

[5] Chen M.H. Analysis on the Application of Blockchain Technology in Emergency Logistics [J], Journal of Sichuan Vocational and Technical College, 2021,31(6):82-86. DOI:10.13974/j.cnki.51-1645/z.2021.06.016.

[6] Jiang Y, Lu Z.B.etc. Research on the Mechanism of Emergency Information Resource Based on Blockchain Technology[J]. New Century Library,2021.2:62-66. DOI: 10.16810/j.cnki.1672-514X.2021.02.010.

[7] Meng H.S, Qu J. Research on the Application of Blockchain Technology in Emergency Intelligence of Public Health Emergencies[J]. Network Security Technology and Applications,2022.5:127-130.
[8] KHAN M, IMTIAZ S, PARVAIZ G S, et al. Integration of internet-of-things with blockchain technology to enhance humanitarian logistics performance [J]. IEEE Access, 2021, 9: 25 422－25 436.
[9] NAWARI N O, RAVIND RAN S. Blockchain and building information modeling ( BIM ) : review and applications in post-disaster recovery[J]. Buildings, 2019, 9(6): DOI: 10. 3390/buildings9060149.
[10] Li G, Wang L.Q, etc. Research on the Collaborative Mechanism of Urban Emergency Management Based on Blockchain Middle Platform Architecture - Taking Sudden Public Health Events as an Example [J]. Journal of Shandong University of Science and Technology (Social Sciences Edition), 2021.23(4):64-72. DOI:10.16452/j.cnki.sdkjsk.2021.04.008