Enhancing Collaborative Emergency Management: Leveraging Blockchain Distributed Ledger for Inter-Agency Data Sharing

Qi Wang
School of Safety Science
Tsinghua University
Beijing, China
qi-wang18@mails.tsinghua.edu.cn

Yi Liu
School of Safety Science
Tsinghua University
Beijing, China
liuyi@tsinghua.edu.cn

ABSTRACT

Emergency management involves multi-agency collaborations necessitating the trustful exchange of critical data across multiple entities. Traditional centralized systems struggle to facilitate effective inter-agency data sharing, presenting challenges related to data authenticity, traceability and privacy vulnerabilities. Consequently, there is a pressing demand for a secure and reliable data collaboration solution. This paper proposes a novel approach by leveraging Blockchain technology to create a trusted data collaboration system for emergency management scenarios. Our solution is capable for recording, sharing, verifying and tracing data among multiple entities within a distributed environment. Specifically, we implemented an application system using Hyperledger Fabric, focusing on sharing data in the practice of epidemic prevention in customs. Empirical research and analysis proved the feasibility of our solution and underscored the immense potential of Blockchain technology in Enhancing collaborative emergency management.

CCS CONCEPTS

Information systems---Data management systems---Information integration---Data exchange

Security and privacy---Formal methods and theory of security---Trust frameworks

KEYWORDS

Blockchain, Distributed Ledger, Emergency management, Data collaboration

SIGSPATIAL '23, November 13-16, 2023, Hamburg, Germany

ACM ISBN 979-8-4007-0346-1/23/11.
https://doi.org/10.1145/3615884.3629423

ACM Reference Format:
Qi Wang, Yi Liu. 2023. Enhancing Collaborative Emergency Management: Leveraging Blockchain Distributed Ledger for Inter-Agency Data Sharing. In Proceedings of The 8th ACM SIGSPATIAL International Workshop on Security Response using GIS 2023 (EM-GIS 2023).ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3615884.3629423

1. Introduction

With the increasing complexity and interconnection of emergencies, collaborative emergency management has emerged as an inevitable and imperative trend[1]. The ability to respond swiftly and effectively to emergencies is no longer the sole domain of individual agencies or organizations. Instead, it hinges on the seamless cooperation among multiple stakeholders, ranging from government agencies and first responders to non-governmental organizations and private sector entities.

At the core of collaborative emergency management is sharing information among agencies. In practical scenarios, the fragmented nature of different agencies and the absence of a well-defined data sharing and collaboration framework often give rise to numerous challenges during emergency responses. These challenges include untimely information communication, difficulties in ensuring data integrity, insufficient coordination and ambiguities in assigning responsibilities. The asymmetry of information will ultimately lead to delays or even failures in decision-making. Hence, the establishment of a more efficient, secure and reliable data collaboration mechanism can effectively promote trust and cooperation among different entities.

The development and application of information and communication technology have provided a new perspective on data collaboration in emergency management. Most government agencies have established their own data centers and business systems. However, data sharing still remains centralized within single line of agencies, resulting in a pronounced occurrence of data silos. Additionally, data standards and data sources are varying from different agencies, making it difficult to ensure data consistency. Moreover, data within the realm of emergency management often includes sensitive information such as residents' information. Traditional data sharing tools may pose risks by potentially exposing data to unauthorized individuals,

raising concerns about privacy breaches. Blockchain has the potential to tackle these challenges with its characteristic such as decentralization, immutability and traceability. Its consensus mechanisms can establish a reliable data sharing channel among multiple entities. By utilizing encryption and verification techniques, data integrity and privacy can be guaranteed.

This paper explores the potential of Blockchain technology to enhance inter-agency data sharing, proving a robust and secure framework that transcends the limitations of traditional centralizes systems. By leveraging Blockchain, emergency management agencies can forge trust, ensure transparency and enhance data integrity and privacy. Specifically, we implemented an application system using Hyperledger Fabric, focusing on sharing data in the practice of epidemic prevention in customs. This implementation explains the feasibility of our framework and provide a guidance of how Blockchain technology can be applied to emergency management. This paper first analyzes the demands of emergency data collaboration through literature reviews. Then, we present an in-depth overview of our decentralized data sharing framework. Finally, we provide a detailed description and performance evaluation of our implemented application. Through comprehensive analysis and case studies, this work aims to shed light on the transformative potential of Blockchain as a tool for enhancing collaborative emergency management.

2. Literature review

The concept of collaborative emergency management can be traced back to the 1960s, Quarantelli [2] discovered that emergency response to disasters is not carried out hierarchically but rather in the form of self-organized networks. Kapucu et al. [3] believe that effective information collaboration among multiple organizations can enhance the efficiency of emergency management and reduce the impact of disasters. However, due to management mechanisms and technical limitations, inter-agencies collaboration is hard to be effectively conducted.

With the development of ICT in recent years, many emerging technologies have been applied to emergency management. Sanchez et al. [4] proposed a wireless emergency data sharing method based 5G, Kyungyong et. Al [5] proposed a P2P cloud network to achieve fast and accurate dissemination of disaster information. Meanwhile, researchers noted the value of data integration in emergency management. By integrating and analyzing information from different sources, a more accurate and comprehensive perception of emergencies can be reached[6]. However, this also raise a challenges that how to securely and reliably share data across multiple organizations. There is an urgent need to establish a data collaboration solution to enhance data sharing capabilities while protecting data ownership.

The occurrence of Blockchain technology provides a possible solution. Blockchain can build a trust mechanism among multiple entities, its traceability and immutable nature ensure transparency and authenticity, thus allowing each entities to supervise its data in data sharing process, preventing data tampering or leakage. In recent years, some researches have attempted to introduce Blockchain technology into emergency management. Liu [7] proposed a Blockchain-based mechanism for sharing emergency medical resources. Baharmand [8] discussed that smart contract can be applied to enhance trust and transparency between humanitarian organizations and suppliers of logistics service. Most of these solutions are conceptual and there are few substantive application systems. Integrating Blockchain technology deeply into emergency management remains an unsolved challenge. Hence, we propose this Blockchain-based data collaboration scheme as a pioneering attempt in the realm of emergency management.

3. Blockchain-based scheme

3.1 Self-hosted database

A Blockchain-based data collaboration scheme eliminates the need for members to upload data to a centralized data center. Instead, all entities retain control over their data by maintaining self-hosted databases, either on local servers or cloud servers. For organizations that need to isolate their data within an intranet environment, they can choose to set up data nodes using local servers to share authorized accessible data. Alternatively, for organizations that lack the infrastructure to build their own nodes, they can choose to deploy nodes on cloud servers or entrust their data to a trusted third entity. These nodes collaborated to form a Blockchain network though P2P network communication, enabling users to connect to authorized nodes within the network. This connection facilitates the reading and writing of data to nodes by sending transactions in Blockchain network. The network ensures data consistency across multiple data nodes through consensus mechanism.

3.2 Digital identity

Digital identity is the identification of a user in a network, which defines the exact permissions over resources of network members for and their access to information within the network. Digital identity is typically implemented in the form of PKI (Public Key Infrastructure) certificates. Users or nodes receive digital certificates encoded with identity information from a trusted authority (CA-Certificate Authority). The CA serves as an authoritative source for validating the digital identity of organizational participants. The identity verification mechanism relies on digital signature technology to ensure the integrity of information during transmission.

MSP (Membership Service Provider) is used to define which organizations are trusted by network members. MSP associates identity with organizational membership, determining a user's permissions within nodes or the network and validating whether a user is authorized to execute specific actions. Applying a digital identity system enable the mapping of real-world identity into the digital world, thereby enabling access control for data resources and preventing unauthorized nodes or users from accessing data.

3.3 Data sharing channel

Typically, a Blockchain network maintains identical ledger data on all nodes. Every transactions requires consensus among all nodes in the network, resulting in slow transaction conformation and low efficiency. For a Blockchain network that intended for emergency collaboration, its internal nodes are composed of different organization entities. Different emergency scenarios require the participation of different organizations, and not all organizations need to be engaged. Therefore, maintaining identical data across all nodes is impractical and not conducive to data security. In fact, it's judicious to connect nodes based on collaborative needs according to the task scenario, thus forming a data sharing channel wherein all channel members collectively maintain a ledger. There can be multiple channels in the network, and nodes can join different channels based on tasks, thereby attaining efficient data sharing.

3.4 Private dataset

Establishing channels in blockchain network facilitates data isolation between different organizations. However, even within these channels, organizations may still have requirement to maintain confidentiality for some certain data. Hence, we introduce the concept of private dataset to address this need. Private dataset is securely stored in dedicated databases on authorized organization nodes, while the hash value of this dataset is written into the ledger of each node on the channel. Users can share private dataset with specific users by executing chaincode, and the recipient of private dataset can confirm the authenticity by verifying its hash value on the chain. This data transmission is conducted by peer to peer communication and is not exposed to other organization members within the channel. In addition, for highly sensitive data, users can choose to periodically clear the data from the nodes instead of permanently storing it on the chain, thereby maximizing data privacy protection.

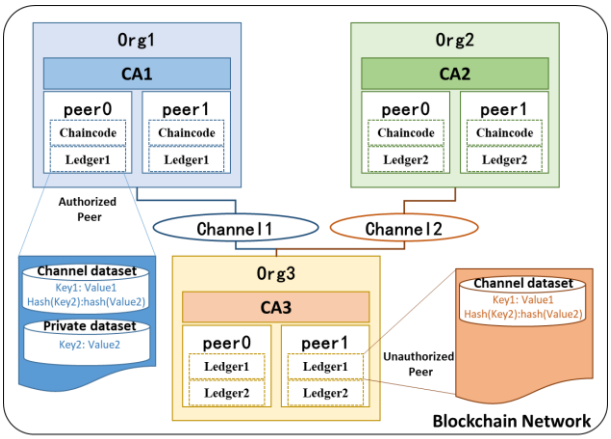

Figure 1: Blockchain-based data sharing scheme

Figure 1 illustrates the architecture of Blockchain-based data sharing scheme. The Org1, Org2, Org3 represent the various organizations engaging in emergency collaboration, which can be government agencies, non-governmental organizations, or other relevant entities. Each organization maintains one or more peers and a CA node. The CA issues identity certificates for peers, and authenticated peers can join the relevant data sharing channel based on their participation in emergency scenarios. The channel ledger data are stored on peers and users can interact with data by invoke chaincode deployed on the peer. For data that should not be publicly exposed within the channel, it can be stored in private databases, only authorized peers can gain access to these data.

4. Implementation

Based on the proposed scheme, we have built a blockchain network for sharing in the practice of epidemic prevention in customs with Hyperledger Fabric. Hyperledger Fabric is an open-source enterprise-grade distributed ledger platform that offers a variety of modular deployment tool for developers to establish their own permissioned blockchain application from scratch.

In this scenario, we considered the collaboration of three main agencies: custom port (Custom), testing laboratory (Lab) and center for disease control (CDC) of local government. The custom port oversees incoming travelers, monitoring their body temperatures, conduct epidemiological investigations and collect nucleic acid samples of travelers with abnormal temperatures. Then the custom sends these samples to the testing laboratory for analysis. The laboratory conducts test on the provided samples and reports the results to both the custom and the local CDC. When suspected cases are identified in the test results, the local CDC requests access to data such as flight information and accompanying passenger details from the custom for further epidemic prevention measures.

In this process, epidemiological investigation records and sample testing results need to be transparent to all three agencies. The flight information and passenger information are considered as private data of the custom and are only authorized for access by the local CDC when suspected cases are identified.

4.1 System architecture

The architecture of application system is illustrated in Figure2. The network contains three agencies mentioned above. Each agencies maintains two peers: an endorsement peer for executing chaincode and a drone peer for backing up ledger data. Each peer is deployed with a couchDB to store and query data. The identity certificates for each agency are generated in an external CA. All peers of these three agencies are joined a channel named "reportchannel" for data sharing. Additionally, three orderer peers are deployed to the network for ordering, packaging, verifying and submitting transaction. Oderers package transaction data into blocks and distribute them to peers on the channel. All peers are running in Docker containers, forming a Docker cluster that can be deployed on a single or multiple host machines.

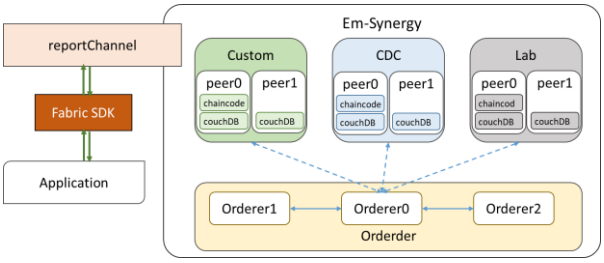

Figure 2: Architecture of application system for epidemic data sharing in customs

External applications can interact with Blockchain data by invoking the chaincode deployed on the channel through the Fabric SDK. Once custom offices write the epidemiological investigation data into the ledger, all peers within the channel automatically update their ledger data due to the consensus mechanism. Similarly, when the laboratory updates the sample test result, the other two agencies also get those data. For sensitive data such as passenger information, the original data is only stored in the custom peers. Other peers can only see the hash value of the data. When the CDC peers are authorized, they can send a request to the chaincode to get the data and verify the data integrity with its hash value.

4.2 Evaluation

To evaluate the performance of our system, we conducted throughput tests to assess the latency of data read and write under different transaction concurrency conditions. Table 1 provides details of the hardware and software environment utilized in the test. "BatchTimeout" refers to the time interval for the blockchain network to generate new blocks, which we configured to 5 seconds to ensure that all nodes in the network have sufficient time to reach consensus. "PreferredMaxBytes" is the maximum block size and "MaxMessageCount" defines the maximum number of transactions that can be packed into each block.

Table 1. Testing environment and network configurations

Operating system	Ubuntu 22.04 x64
CPU	Intel(R) Xeon(R) Platinum 8269CY CPU @ 2.50GHz
Docker Memory Limit	2 GB
Fabric Version	v2.4.2
Number of Organizations	3
Peers per Organization	2
Number of Orderers	3
BatchTimeout	5 s
PreferredMaxBytes	2 MB
MaxMessageCount	500

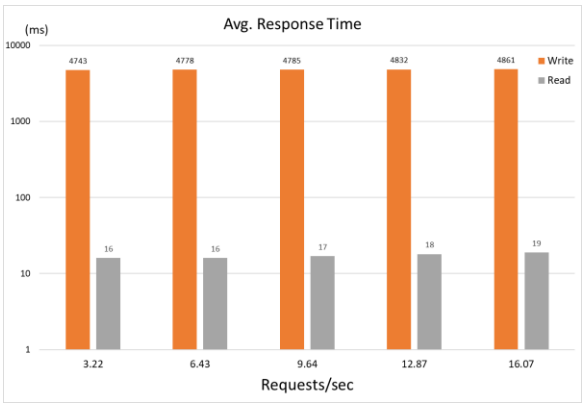

Figure 3: Results of latency tests under different transaction concurrency

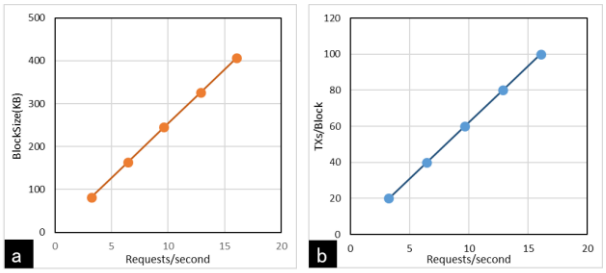

Figure 4: a) Correlation between blocksize and request rate. b) Correlation between number of transactions per block and request rate

The results of latency tests are shown in Figure 3. Overall, our system demonstrates stable performance in high transaction throughput environments. Figure 4 illustrates that transaction packing capacity and storage size of block are still redundant in high concurrency situation. Average response time for reading data from the Blockchain ledger is in the millisecond range, fully meeting the performance requirements for real-time data retrieval. As for writing data to the Blockchain ledger, the average response time is around 4.8 seconds, closely aligned with the network's block generation time. Since real-time data writing is not a critical demand for customs epidemic prevention, our system adequately fulfills the data collaboration demands in this scenario.

5. Conclusion

Blockchain technology has the potential to build a trusted collaboration environment among multiple entities, reshaping collaboration models in many areas. However, there have been few practical applications in the realm of emergency management. This research can be regarded as an attempt of applying Blockchain technology to emergency management. This paper explores the value of Blockchain technology in enhancing inter-agencies data sharing. The consistency, integrity and privacy of data can be guaranteed by leveraging the decentralized, immutable and traceable characteristics of Blockchain. This paper provides a detailed introduction to the Blockchain-based distributed data sharing scheme and builds an application system

for custom epidemic prevention scenario. Empirical research and analysis proved the feasibility of our scheme in enhancing inter-agencies data collaboration in emergency management. In future research, we will explore the introduction of more fine-grained access control schemes into the Blockchain data sharing network and add more channels in the network to verify the applicability of our system in large scale emergency collaboration scenarios.

ACKNOWLEDGMENTS

Funded by National Key R&D Program of China (No.2021YFC0809905) and National Natural Science Foundation of China (No.72174102).

REFERENCES

[1] Wang, Y. Q. and H. Chen (2022). "Blockchain: A potential technology to improve the performance of collaborative emergency management with multi-agent participation." International Journal of Disaster Risk Reduction **72**.

[2] Quarantelli E L (1977). "Response to social crisis and disaster." Annual review of sociology **3(1)**: 23-49.

[3] Kapucu, N., et al. (2010). "Collaborative emergency management and national emergency management network." Disaster Prevention and Management **19**(4): 452-468.

[4] Sanchez, B. B., et al. (2020). "Managing Wireless Communications for Emergency Situations in Urban Environments through Cyber-Physical Systems and 5G Technologies." Electronics **9**(9).

[5] Chung, K. and R. C. Park (2016). "P2P cloud network services for IoT based disaster situations information." Peer-to-Peer Networking and Applications **9**(3): 566-577.

[6] Liaqat, M., et al. (2017). "Federated cloud resource management: Review and discussion." Journal of Network and Computer Applications **77**: 87-105.

[7] Liu, H. and Y. X. Liu (2021). "Construction of a Medical Resource Sharing Mechanism Based on Blockchain Technology: Evidence from the Medical Resource Imbalance of China." Healthcare **9**(1).

[8] Baharmand, H. and T. Comes (2019). "Leveraging Partnerships with Logistics Service Providers in Humanitarian Supply Chains by Blockchain-based Smart Contracts." Ifac Papersonline **52**(13): 12-17.