JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 25, No. 6, pp. 1621-1630, Jun. 2024

Check for updates

의료 정보 탈중앙화를 위한 컨소시엄 블록체인 모델

시 정[1] · 신 승 수[2*]
[1]동명대학교 컴퓨터미디어공학과 박사과정
[2]동명대학교 정보보호학과 교수

Consortium Blockchain Model for Decentralized of Healthcare Information

Chai Ting[1] · Seung-Soo Shin[2*]

[1]Ph.D. Course, Dept. of Computer and Media Engineering, Tongmyong University, Busan 48520, Korea
[2]Professor, Dept. of Information Security, Tongmyong University, Busan 48520, Korea

[요 약]

의료 분야는 정보 보안과 효율적인 관리에서 많은 문제에 직면하고 있다. 전통적인 중앙 집중식 의료 정보 시스템은 특히 데이터 유출, 상호 운용성 부족 및 환자 개인의 정보 보호 측면에서 부적절하다. 의료 데이터 관리 시스템의 보안, 투명성 및 효율성 문제를 해결하기 위한 컨소시엄 블록체인 모델을 제안한다. 제안 모델은 의료 정보 교환 준수를 자동화하기 위해 스마트 계약과 함께 암호화 및 불변성 등 블록체인의 보안 기능을 활용하는 것이 목적이다. 또한, 혁신적인 솔루션을 제공하며 높은 동시성 환경에서 데이터 처리 능력과 정보 처리 속도를 검증하기 위해 실질적으로 테스트를 하였다. 이는 의료정보를 관리할 수 있는 권한을 부여함으로써 환자의 프라이버시와 자율성을 존중하면서 데이터 교환의 효율성과 투명성을 향상시킬 것이다.

[Abstract]

The healthcare sector faces increasing challenges in information security and efficient management. Traditional centralized healthcare information systems are inadequate, particularly for data leakage, lack of interoperability, and patient privacy protection. The paper proposes a consortium blockchain model to address security, transparency, and efficiency issues in the healthcare data management system. The model leverages the security features of blockchain, such as encryption and invariance, along with smart contracts to automate compliance of healthcare information exchange. This innovative solution has been practically tested to verify its data processing capability and information processing speed in a high concurrency environment. This provides a theoretical and practical foundation for the future direction of healthcare information systems. This will enhance the efficiency and transparency of data exchange while honoring the privacy and autonomy of patients by empowering them to manage their healthcare information.

색인어 : 하이퍼레저 패브릭, 블록체인, 의료정보, 체인코드, 탈중앙화

Keyword : Hyperledger Fabric, Blockchain, Healthcare Information, Chaincode, Decentralized

http://dx.doi.org/10.9728/dcs.2024.25.6.1621

Received 17 April 2024; **Revised** 27 May 2024
Accepted 11 June 2024

***Corresponding**; **Seung-Soo Shin**
Tel: ※ 개인정보 표시제한
E-mail: shinsss@tu.ac.kr

Ⅰ. Introduction

Current healthcare information systems face problems such as data silos, inadequate privacy protection, and inefficient data sharing. These problems make it difficult for patient data to circulate among organizations, increasing the complexity and cost of healthcare services. Therefore, there is an urgent need for a new technological solution to improve the deficiencies of the existing system[1].

Blockchain technology, which is decentralized, tamper-proof, and transparent, shows great potential in healthcare information management. Among them, consortium blockchain combines the advantages of public and private chains, which is very suitable for healthcare information systems with multi-party participation. IPFS (Interplanetary File System), as a decentralized file storage system, can effectively solve the problem of large-scale data storage[2].

Sameera et al.[3] proposed blockchain-enabled federated learning (BCFL) systems, emphasizing the increasing significance of integrating blockchain technology with federated learning to tackle crucial issues like privacy and security in healthcare data management. Bautista et al.[4] proposed a blockchain -based decentralized healthcare information management platform (MediLinker) that enables patient-centric data sharing to enhance data mobility and interoperability among electronic health record (EHR) systems. Dwivedi et al.[5] proposed decentralized privacy-preserving healthcare blockchain for the internet of things (IoT), describing a system to securely and efficiently transmit healthcare data through IoT devices in smart cities.

This paper proposes a consortium blockchain-based framework that aims to transform healthcare information management by addressing the challenges inherent in current healthcare data management systems, such as security breaches, a lack of transparency, and inefficient data exchange processes.

The proposed model aims to enhance the security and privacy of healthcare data by leveraging the inherent security features of blockchain, such as encryption and immutability. Smart contracts are implemented to ensure automated compliance with healthcare regulations and standards, streamline the exchange of healthcare information between various stakeholders and improve the efficiency and transparency of data exchange[6]. Respect patients' privacy and choices by giving them control over their healthcare information. Utilize standardized data formats such as HL7 FHIR (Health Level Seven Fast Healthcare Interoperability Resource) to ensure data compatibility across various systems and organizations[7].

The proposed model utilizes the hyperledger fabric modular blockchain framework, through which healthcare data is managed on a consortium blockchain network that ensures secure and efficient sharing of data between authorized parties. Encrypted patient healthcare data is stored in IPFS and the hash value of the data is recorded on the blockchain to ensure data immutability. Use Fabric CA for user authentication and role and attribute based access control (RBAC and ABAC) via smart contracts. Design and implement a secure data sharing mechanism that enables authorized users to efficiently query and share healthcare data[8].

The proposed model has the following features: first, it eliminates single points of failure and reduces the risk of a centralized data management system. Secondly, it ensures seamless communication and data exchange among various healthcare systems and stakeholders. Thirdly, it can cope with the growing volume of healthcare data and the expanding network of stakeholders. Finally, the system is patient-centered, giving patients control over their own health information. The proposed model offers transparent and auditable tracking of data transactions through access control policies. Smart contracts guarantee that all transactions and data processing are automatically comply with healthcare regulations. Additionally, and the use of off-chain and on-chain service authorization controls empowers patients the ability to determine who can access their health data[9].

Ⅱ. Blockchain and Healthcare Information

2-1 Current Status of Blockchain Applications in Healthcare Information

Healthcare information encompasses to the essential components of a healthcare information system within

the framework of blockchain technology. The underlying infrastructure, including servers, networks, and databases, is also crucial. Various blockchain systems have similar essential roles, including data providers, data consumers, blockchain nodes, and system administrators. Each of these roles is crucial for maintaining the integrity, privacy, and accessibility of healthcare information.

However, ensuring patient privacy while allowing necessary access remains a significant challenge in traditional blockchains, despite their security features. Blockchain solutions must efficiently manage large volumes of healthcare data without compromising speed or escalating costs. Consortium blockchains can help address common challenges in healthcare data management, such as interoperability, security, and patient privacy, through the use of distributed ledgers, smart contracts, consensus mechanisms, and permissioned access[10].

The current research on the application of blockchain or consortium blockchain technology in healthcare information can be categorized into several key areas. These areas include data privacy and security, interoperability, patient engagement, regulatory compliance, and scalability. The aim of researchers and technologists is to explore how these technologies can address the challenges prevalent in healthcare information systems[11].

2-2 Previous Works of Blockchain Applications in Healthcare Information

There is a growing trend towards integrating blockchain technology to address long-standing issues in healthcare data management. This includes ensuring data privacy, improving interoperability, and enhancing the security of healthcare records. Blockchain and smart contracts can provide a decentralized framework that ensures patient data privacy and secure data sharing between authorized parties, making them a viable solution to overcome the limitations of current Electronic Health Record systems.

Purohit et al.[12] proposed a health information sharing system that utilizes a consortium blockchain to facilitate secure, incentive-based cooperation among organizations for sharing healthcare records. The system aims to address the security and reliability of healthcare image sharing while enhancing the data decision-making capability of healthcare providers through a reputation-based system. The system is scalable and can handle tens of thousands of transactions per block. Shahnaz et al.[13] proposed a transforming of electronic health records through blockchain, focusing on scalability and data governance. The proposed solution aims to address scalability issues by establishing fine-grained access rules and utilizing off-chain storage to offer a scalable, secure, and comprehensive solution for revolutionizing the EHR system through blockchain technology.

Duo Zhang et al.[14] proposed a secure storage and sharing scheme for healthcare data using blockchain, ensuring privacy and supporting fine-grained access control. They propose a blockchain-based system for secure storage and sharing of healthcare data that offers privacy and security assurances, as well as supports fine-grained access control and key management. This approach aims to facilitate the sharing of healthcare data and address the current issue of information silos by providing enhanced functionality, security, and efficiency.

Liu et al.[15] proposed a system aimed at enhancing privacy and data security in healthcare applications using blockchain and distributed ledger technology. The authors introduced an enhanced biomedical security system based on blockchain and distributed ledgers to improve privacy and data security in healthcare applications. The system aims to empower patients to use data to support their care and incorporates a robust consent system for sharing data between different organizations.

Ⅲ. Decentralized of Healthcare Information

3-1 Overview

Existing healthcare information systems technology is a broad and complex field. The various types of healthcare information systems models, such as electronic health records (EHRs), Healthcare practice management software (PMS), Healthcare information exchanges (HIEs), Mobile health (M-health), and Big data and analytics, differ in their structure and functionality, but they typically rely on centralized databases to store and manage patient data.

These systems are interconnected through

centralized databases that share and update information to provide comprehensive patient care and optimize healthcare processes. Within this framework, the interaction of systems guarantees the smooth flow and availability of healthcare information while safeguarding the privacy and security of patient data.

For example, a patient's EHR can be updated and accessed with information from various healthcare providers, including specialists, laboratories, or emergency services, through the HIE system. Meanwhile, M-health solutions can provide real-time data, such as heart rate or blood glucose levels, that can be uploaded directly into a patient's EHR for a physician to assess.

In summary, although EHRs, PMSs, HIEs, M-health, and big data and analytics systems each have unique components and functionalities, they all rely on the integration of centralized databases to improve the efficiency, quality, and personalization of healthcare delivery. Through effective data management and exchange, these systems can complement each other to provide more comprehensive and coordinated care for patients. Fig. 1 depicts a typical operating model for healthcare information systems.

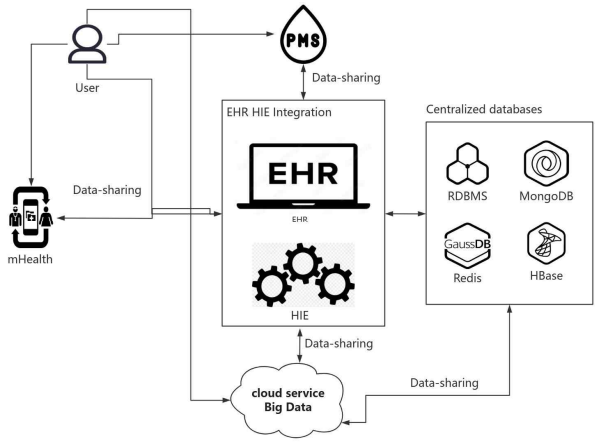

Fig. 1. Overview of healthcare information systems

We propose a decentralized healthcare information system based on the consortium blockchain. This system uses the consortium blockchain to establish a mechanism that who can get permission to access the healthcare information. The consortium node and the patient get the identity tokens by the consortium blockchain, then use this identity tokens to access the healthcare data.

3-2 System Design

The purpose of this section is to detail the system architecture of a consortium blockchain model decentralized healthcare information system (CBMDHI) constructed on the basis of federated blockchain technology. The CBMDHI system adopts a specific node configuration consisting of seven main nodes. Smart contracts are written using chain codes to define and execute the business logic of healthcare information. The combined use of IPFS off-chain data storage achieves efficient and secure healthcare data processing and sharing.

1) System Nodes

The proposed system is configured through specific nodes, where each node interacts with data on and off the chain, and is divided into seven important components based on their functions, and the system node architecture diagram is shown in Fig. 2.

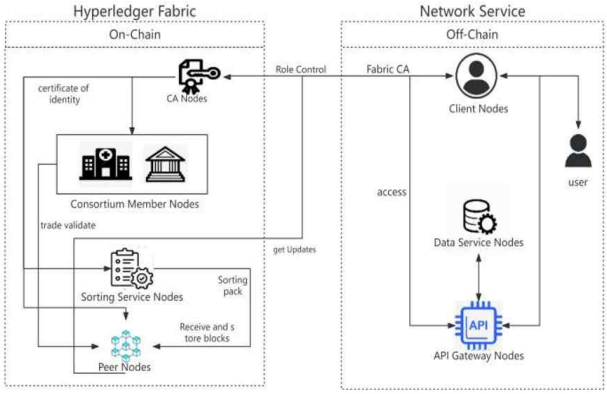

Fig. 2. System nodes architecture diagram

The CBMDHI system nodes are divided into 7 important nodes with the following functions:

① Peer Node : The core of the CBMDHI system is a network of peer-to-peer node. These nodes are responsible for executing and processing transaction requests and ensuring that healthcare data is transferred and updated in accordance with system rules. Peer node is responsible for maintaining a persistent ledger that records the history and current state of all transactions. Peer node is categorized into endorsement nodes and submission nodes according to their functions.

② Sorting Service Node : Sorting service nodes are responsible for receiving transaction proposals

from client nodes and peer nodes and sorting the transactions according to certain rules. The sorting service node packages the sorted transactions into blocks. Once the block is created, it is sent to the peer nodes in the network for further validation and updating the ledger.

③ CA Node : The CA node provides the authentication infrastructure for the CBMDHI system. CA nodes issue digital certificates to users, nodes, and other entities within the system. Digital certificates contain essential identity information, including public keys, identifiers, and more. These certificates enable network participants to authenticate each other's identity, ensuring the security of transactions and data exchange.

④ Client Node : The client node represents end-users in the CBMDHI system, which can include patients, doctors, researchers, and other types of healthcare-related participants. End-users submit healthcare data (e.g., electronic health records, healthcare images, etc.) or query stored data to the system through client nodes. These operations are executed through chaincode (smart contracts) to ensure consistent data processing and compliance with business logic.

⑤ Data Service Node : The data service node is connected to an off-chain data storage system. Since blockchains are suitable for storing transaction records and other lightweight data, data service nodes act as a bridge between the blockchain and the off-chain data storage system. They are responsible for storing large amounts of data off-chain while also storing the hashes and metadata of the data on the blockchain. Data service nodes can also facilitate data sharing and interoperability among various healthcare organizations. Standardized interfaces and protocols make it possible to securely exchange and utilize data, even for systems from different institutions.

⑥ API Gateway Node : The API gateway node serves as a bridge connecting external applications to the CBMDHI system. The API gateway node authenticates and authorizes requests before processing them. In addition to authentication and authorization, the API gateway is responsible for encrypting data transmissions. The API gateway node is responsible for properly routing requests from external applications to the appropriate services within the CBMDHI system.

⑦ Consortium Member Node : The blockchain network is maintained by consortium member nodes, which are healthcare institutions and organizations that have joined the network. This node is responsible for maintaining the network's ledger data, which includes healthcare records, patient information, and transaction history.

2) Chaincode

The design of the chaincode (smart contract) is one of the core components, responsible for implementing the business logic of the system and ensuring data integrity and security. The proposed system utilizes the Java language to write the chaincode.

3) Data Storage and Access Control

The proposed CBMDHI system adopts a hybrid data storage approach, utilizing a federated chain and an off-chain data storage solution (IPFS). Transaction records (including metadata and access logs) are stored on the blockchain, while large-scale healthcare data such as imaging files are stored off-chain in IPFS.

IPFS is utilized to store extensive healthcare datasets and ensure high data availability without affecting the performance of the blockchain network. When data is added to IPFS, it returns a unique hash representing the content. The hash is then stored on the blockchain, securely linking off-chain data to on-chain records. This design ensures data integrity because the content behind the hash cannot be changed without altering the hash itself, which can be detected on the blockchain.

The CBMDHI system implements fine-grained access control policies that specify who can view or modify data stored both on and off the chain. These policies are enforced through smart contracts for on-chain data, as well as access control lists or similar mechanisms for data stored in the IPFS. The access control logic provides a dynamic and secure framework for accessing data, considering the role of the user's role, the attributes of the data being accessed, and the context of the access request.

Sensitive data stored off-chain in IPFS is encrypted

before storage, and decryption keys are managed securely. On-chain data, primarily of transaction logs and hashes, is safeguarded using private data sets or similar technologies that limit data access to authorized parties only.

3-3 System Process

In modern healthcare information systems, it is critical to ensure that patient data is accurately entered, updated, and securely shared. The CBMDHI system is designed to optimize this process and enhance the quality and efficiency of healthcare services.

1) Patient-centered System Processes

The core patient-centered processes in the system include key aspects such as patient identity registration, healthcare information data collection, access, updating, and sharing. The process diagram of the patient-centered system is shown in Fig. 3.

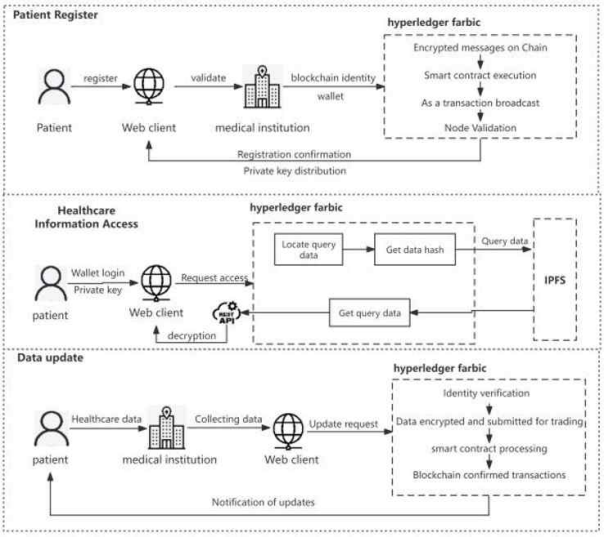

Fig. 3. Patient-centered system flow diagram

The patient registration process requires the patient to provide personal and healthcare information, including their name, contact details, and healthcare history. The patient then submits this information to the client of the healthcare system. The system verifies the patient's identity by cross-checking it with existing healthcare records or requesting an identification document. In a consortium blockchain, multiple members, such as hospitals and insurance companies, are responsible for reviewing registration requests. Once the patient's information is verified as correct, the system will create a blockchain identity for them. This identity is a unique digital wallet address that represents the patient in the system. The patient's personal and healthcare information is linked to their blockchain identity through encryption. The patient will receive a private key to access and manage their identity and data on the blockchain. Validated and encrypted patient information will be recorded on the blockchain through the automated execution of smart contracts.

The consortium blockchain network collectively verifies and confirms the patient's blockchain identity and related information when a transaction is broadcasted by the nodes in the network. After the patient's information is recorded on the blockchain, they receive a notification confirming their registration.

To access healthcare information through the client, the patient enters their wallet address and private key

to initiate the login request. The client then verifies the patient's identity by ensuring that the private key matches the public key on the blockchain network. Once the login is successful, a request with an access identifier is submitted, and the system initiates a location retrieval process. The system retrieves the data file from the IPFS network using the IPFS hash stored on the blockchain. Then, it decrypts the data using the patient's private key and presents it to the patient via a Rest API.

Healthcare providers, such as doctors and nurses, collect information about a patient's visit, including diagnostic results, treatment plans, and prescribed medications. They use a dedicated healthcare information system connected to the federated blockchain network to update the patient's healthcare record by submitting a request.

The patient's blockchain identifier is then indicated. Before sharing the updated healthcare record with a third party, such as a research organization, it is necessary to obtain the patient's explicit consent. This can be done through the eConsent form function. The system verifies the identity of the healthcare provider to ensure that only authorized personnel can submit updates to healthcare records.

The system encrypts updated healthcare records and patient consent information before submitting them

as a single transaction to the federated blockchain network. A smart contract on the federated blockchain processes the submitted transaction, verifying its legitimacy, and accurately stores the updated healthcare record on the blockchain. After the blockchain network confirms and adds the transaction to the block, the updated healthcare records and shared consent are securely stored. The system notifies the patient of the updated or shared healthcare record through an in-app notification. All update and data sharing operations leave a tamper-proof audit log on the blockchain.

2) Patient Access System Timing

The process of patient identity registration and accessing the system to obtain data typically involves several key steps. We utilize a timing diagram to clarify the order of interaction among the participants. The patient access timing diagram is shown in Fig. 4. The patient requests access to their healthcare information through the client application. The client application then sends a request via a REST API to Fabric CA for local authentication. Fabric CA verifies the patient's digital certificate. Once the digital certificate is successfully verified, the client application utilizes the patient's identity to send a request to the federated blockchain network through the REST API. The federated blockchain network receives the request and authenticates it using Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) via a smart contract. The smart contract checks if the request has the necessary permissions to access information based on the patient's role and attributes.

Once the authentication is successful, the smart contract retrieves the hash value of the information stored in IPFS by accessing the blockchain data. The client application uses the hash value to initiate a query request directly to IPFS. IPFS then returns matching healthcare information that matches the provided hash value. The client application receives the data returned by IPFS, decrypts it, and sends the decrypted healthcare information back to the patient via a REST API.

IV. Evaluation and Result

4-1 Experimental Method

To evaluate the feasibility and performance of the system design, IPFS nodes are run in Docker and set to private network mode to simulate a real healthcare data storage environment. Hyperledger Fabric network is deployed to upload the healthcare data used for testing to the IPFS node and record the returned IPFS

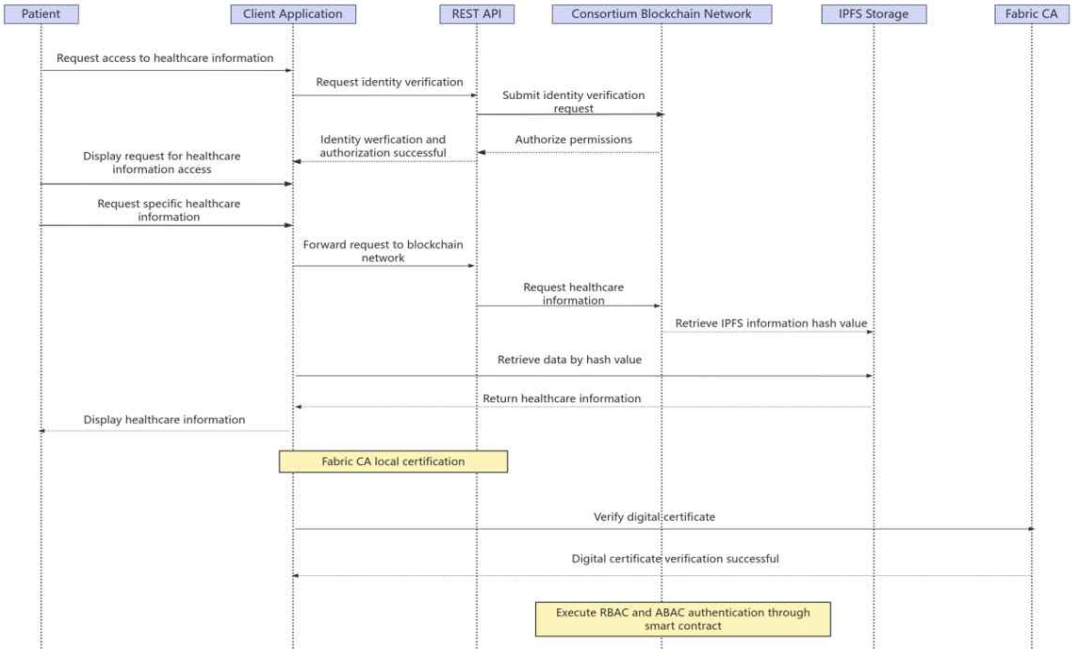

Fig. 4. Patient access system timing diagram

hash values. Utilized chaincode to store the IPFS hash of the data on the blockchain, implement chaincode logic to retrieve the data from IPFS using the IPFS hash, and verify the integrity of the data.

4-2 Performance Evaluation

1) Data-Processing Capability

In order to evaluate the data processing capacity of the proposed CBMDHI system, the processing capability of the system under high concurrency is evaluated through local tests. This is achieved by simulating multiple endpoints or clients concurrently submitting transactions to the blockchain network for registering a new healthcare record. The the execution of these test cases is automated using testing tools such as JMeter. System throughput is the number of transactions that can be successfully processed per unit of time, and it is a key measure of a system's data processing capability. The system throughput for concurrent users is shown in Fig. 5.

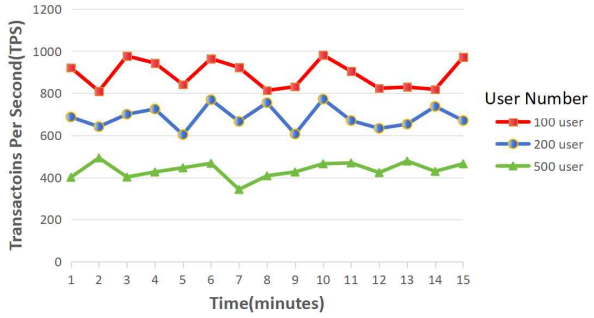

Fig. 5. System throughput with concurrent users

2) Response Time

Response time in the proposed CBMDHI system is defined as the total time from when a user makes a request to when Hyperledger Fabric processes it, completes the transaction, and responds. In order to reduce the amount of data that needs to be stored on the blockchain, the combination of IPFS for storing sensitive data and large capacity data. This division helps in reducing the time required to confirm the completion of the transaction on the blockchain and the time needed to confirm it on the blockchain after storing and retrieving the hash on IPFS. Response time is a crucial indicator for assessing the information processing speed of the system. Tests are conducted

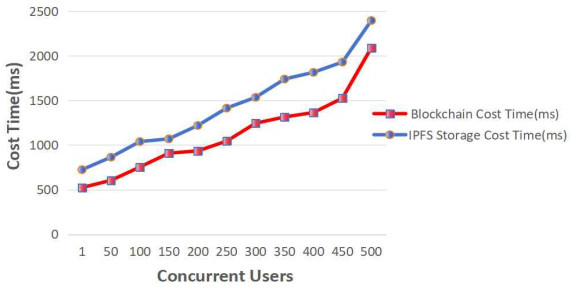

Fig. 6. Concurrent user response time

in a local LAN, with the average size of transactions set to 1KB. The response time for concurrent users is shown in Fig. 6.

4-3 Analysis of the CBMDHI System

The proposed CBMDHI system demonstrates significant advantages in terms of federated blockchain, fast transactions, no transaction fees, content addressing and user-centered. The proposed CBMDHI system uses the hyperledger fabric consortium blockchain, which is jointly maintained by multiple institutions, allowing the system to balance the advantages of decentralization with the efficiency and management of centralization.

The CBMDHI system evaluation analysis shows that the CBMDHI system is able to operate stably in high concurrency situations and process a large number of transactions efficiently. In the coalition blockchain, the number of nodes is relatively small compared to the public chain, and the transaction speed is faster. It is proposed that the system uses the consortium blockchain to exempt the transaction fee, which reduces the economic burden of users and healthcare organizations, makes the system more popular and easy to accept, and improves the system's usage rate.

The proposal CBMDHI system uses IPFS in combination with blockchain to use content addressing function, which is stored on the blockchain through its hash value, to quickly locate the healthcare information, reduce the pressure of blockchain storage, and make the response speed and transaction speed faster. The overall design of the proposed system is user-centered, emphasizing user autonomy and convenience. Fine-grained access control is used during user registration, information access and updating, and users take better control of their

Table 1. Comparison to related systems

	[12]	[13]	[14]	[15]	Proposed system
Consortium Blockchain	Y	N	Y	N	Y
Cost Time	Low	High	Medium	High	Low
Gas Fee	N	Y	N	Y	N
Content Addressable	N	Y	N	N	Y
User-Centered	N	N	N	N	Y

healthcare data and decide who can access and use it. We discuss some of the parameters present in our system and use them for comparison with related work in the field. The comparison parameters are shown in Table 1.

Cost time and Gas fee are important metrics to measure the system. Cost time is the total time taken to complete a transaction. Purohit et al.[12], Shahnaz et al.[13] and Liu et al.[15], using a public blockchain, due to the number of nodes involved in the transaction, the time to complete the transaction is 2 minutes, according to Duo Zhang[14]. Using quorum consortium blockchain, the time to complete the transaction is 40 seconds. Proposed CBMDHI system uses hyperledger fabric consortium blockchain, which is able to complete the transaction in 2 seconds under high concurrency and has a significant advantage in terms of transaction time. Gas fee is the transaction cost of the user while using the system. Purohit et al.[12], Shahnaz et al.[13] and Liu et al.[15] used the gas fee to be paid for each transaction on the ethereum blockchain and Duo Zhang[14] used the quorum consortium blockchain which also has a lower gas fee. We propose when the system is designed without gas fees to reduce user costs to enhance transaction speed and efficiency and to promote decentralized.

V. Conclusion

The field of healthcare information has encountered growing challenges. The traditional centralized healthcare information system is inadequate to address these issues. Blockchain technology has emerged as a solution to integrate its inherent characteristics into the field of healthcare information.

This paper proposed the CBMDHI system effectively improves the data security and sharing efficiency of healthcare information systems. By introducing joint blockchain and IPFS technologies, the system solves the problems of data silos and privacy protection in traditional healthcare information systems. Performance evaluation shows that the system performs well in terms of data processing speed and storage capacity.

Compared with existing decentralized healthcare information systems, the CBMDHI system adopts a consortium blockchain model. Compared with the public chain, the consortium blockchain has significant advantages in performance and security, which is especially suitable for scenarios where multiple parties participate in the healthcare information system. Using IPFS to store large-scale data reduces the storage pressure on the blockchain while ensuring data reliability and availability. The research focuses on optimizing off-chain data storage by combining IPFS with blockchain technology. It is proposed that the system use fine-grained access control to provide more flexible and detailed permission management through RBAC and ABAC policies to meet the needs of different users.

The CBMDHI system operates stably in a highly concurrent environment, with an average system throughput of 900 in the test network environment. The system processes transactions within one second. The system not only ensures the security and privacy of healthcare data but also processes data transactions efficiently. This demonstrates its potential for use in healthcare information management.

Future research will focus on optimizing system performance and exploring additional features to accommodate a wider range of healthcare application scenarios. The aim is to improve the system's scalability, enhance the user interface's user-friendliness, and develop more advanced data analysis tools. These efforts will make CBMDHI a more secure and efficient data management platform for the healthcare industry.

References

[1] M. A. Engelhardt, “Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector,” *Technology Innovation Management Review*, Vol. 7, No. 10, pp. 22-34, 2017. http://doi.org/10.22215/timrevi

ew/1111

[2] M. S. B. Kasyapa and C. Vanmathi, “Blockchain Integration in Healthcare: A Comprehensive Investigation of Use Cases, Performance Issues, and Mitigation Strategies,” *Frontiers in Digital Health*, Vol. 6, April 2024. https://doi.org/10.3389/fdgth.2024.1359858

[3] K. M. Sameera, S. Nicolazzo, M. Arazzi, A. Nocera, K. A. Rafidha Rehiman, P. Vinod, and M. Conti, “Privacy-Preserving in Blockchain-Based Federated Learning Systems,” *Compute Communications*, Vol. 222, pp. 38-67, June 2024.

[4] J. R. Bautista, D. T. Harrell, L. Hanson, E. de Oliveira, M. Abdul-Moheeth, E. T. Meyer, and A. Khurshid, “MediLinker: A Blockchain-Based Decentralized Health Information Management Platform for Patient-Centric Healthcare,” *Front Big Data*, Vol. 6, June 2023. http://doi.org/10.3389/fdata.2023.1146023

[5] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A Decentralized Privacy-Preserving Healthcare Blockchain for IoT,” *Sensor*s, Vol. 19, No. 2, 326, January 2019. https://doi.org/10.3390/s19020326

[6] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, “An Overview on Smart Contracts: Challenges, Advances and Platforms,” *Future Generation Computer Systems*, Vol. 105, pp. 475-491, April 2020. https://doi.org/10.1016/j.future.2019.12.019

[7] R. Saripalle, C. Runyan, and M. Russell, “Using HL7 FHIR to Achieve Interoperability in Patient Health Record,” *Journal of Biomedical Informatics*, Vol. 94, 103188, June 2019. https://doi.org/10.1016/j.jbi.2019.103188

[8] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. de Caro, ... and J. Yellick, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in *Proceedings of the Thirteenth EuroSys Conference*, New York: NY, No. 30, pp. 1-15, April 2018. https://doi.org/10.1145/3190508.3190538

[9] K. Miyachi and T. K. Mackey, “hOCBS: A Privacy-Preserving Blockchain Framework for Healthcare Data Leveraging an On-Chain and Off-Chain System Design,” *Information Processing & Management*, Vol. 58, No. 3, 102535, May 2021. https://doi.org/10.1016/j.ipm.2021.102535

[10] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, “Metrics for Assessing Blockchain-Based Healthcare Decentralized Apps,” in *Proceedings of IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, China, pp. 1-4, 2017. https://doi.org/10.1109/HealthCom.2017.8210842

[11] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications,” *Journal of the American Medical Informatics Association*, Vol. 24, No. 6, pp. 1211-1220, November 2017. https://doi.org/10.1093/jamia/ocx068

[12] S. Purohit, P. Calyam, M. L. Alarcon, N. R. Bhamidipati, A. Mosa, and K. Salah, “HonestChain: Consortium Blockchain for Protected Data Sharing in Health Information Systems,” *Peer-to-Peer Networking and Applications*, Vol. 14, pp. 3012-3028, May 2021. https://doi.org/10.1007/s12083-021-01153-y

[13] A. Shahnaz, U. Qamar, and A. Khalid, “Using Blockchain for Electronic Health Records,” *in IEEE Access*, Vol. 7, pp. 147782-147795, October 2019. https://doi.org/10.1109/ACCESS.2019.2946373

[14] D. Zhang, S. Wang, Y. Zhang, Q. Zhang, and Y. Zhang, “A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain,” *Security and Communication Networks*, Vol. 2022, 2759787, May 2022. https://doi.org/10.1155/2022/2759787

[15] H. Liu, R. G. Crespo, and O. S. Martíne, “Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts,” *Healthcare*, Vol. 8, No. 3, 243, July 2020. https://doi.org/10.3390/healthcare8030243

시정(Chai Ting)

2023년 8월 : 동명대학교 컴퓨터미디어공학과 (공학 석사)

2024년 3월～현 재: 동명대학교 컴퓨터미디어공학과 박사과정
※관심분야 : Blockchain, DID, IoT

신승수(Seung-Soo Shin)

2001년 2월 : 충북대학교 수학과 (이학박사)
2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)

2005년 3월～현 재: 동명대학교 정보보호학과 교수
※관심분야 : 네트워크 보안, 딥러닝, IoT, 데이터분석