

A Blockchain-Driven Framework for Auditable and Tamper-Proof PHR Data Management

Sang Young Lee

Department of Health Administration, Namseoul University, South Korea

sylee@nsu.ac.kr

Abstract. This paper proposes a permissioned blockchain framework to enable secure sharing of electronic medical records between healthcare institutions. Encryption mechanisms grant access control to authorized users while ensuring data integrity. The system leverages blockchain properties like decentralization and immutability to mitigate security risks of cloud-based storage. A detailed architecture illustrates member authentication, transaction protocols, and interconnected blockchain components. By decentralizing medical data, the system aims to facilitate trustless sharing and prevent unauthorized data modification. We can create a distributed database that offers functions such as data storage, backup, and restore for medical information. This involves transmitting and saving medical information in each existing base medical institution. This design aims to enable secure data sharing using an extensible and lightweight blockchain, ensuring privacy by comparing it to shared data pools and blockchain networks. Through this approach, the Blockchain Server in each participating base of the Blockchain Network can function as an interface for utilizing medical information, in addition to storing medical data securely.

Keywords: blockchain, smart, PHR

1. Introduction

As the healthcare industry transitions towards precision, predictive, personalized, and preventive medicine, personal healthcare is gaining increasing interest and importance. The digital healthcare industry, fueled by advancements in information and communication technology during the fourth industrial revolution, is expected to provide highly valuable medical services centered around users. Personal Health Record (PHR) is a crucial aspect of the digital healthcare industry, enabling personalized health management for prevention and management purposes through comprehensive personal health record data (Abel et al., 2017; Shapiro et al., 2006).

With the technological advancements of the fourth industrial revolution and growing concerns about health, the healthcare service paradigm is shifting from traditional diagnosis and treatment towards predictive medicine, personalized medicine, and participatory medicine that focus on disease prevention. Personal health records serve as platforms that provide comprehensive information related to personal health and health management services. As a result, they are part of the subdivided industry of digital healthcare. PHR data plays a critical role in systematically supplementing modern individuals' health management efforts for disease prevention and management, representing a global trend in digital healthcare (Roehrs et al., 2017; Azaria et al., 2016).

In general, medical information systems encompass various aspects such as hospital management, prescription transmission, examination and treatment support management, management information management, picture archiving and transmission, and electronic medical records. Essentially, they are comprehensive hospital management systems that enhance hospital competitiveness by supporting management and maximizing effectiveness. As interest in personal health has grown, the concept of medical information has evolved into Electronic Health Records (EHR), expanding its application scope in conjunction with the development of wearable devices, IoT, and smart devices (Zhang et al., 2018; Maslove et al., 2018; Wong et al., 2019).

The digital healthcare industry represents the convergence of the healthcare and ICT industries for personal health and disease management. Data-driven healthcare brings innovation to the entire process related to healthcare data, including measurement, integration, analysis, and application. Personalized services, which are gaining prominence as the next-generation paradigm for prevention and management, are heavily reliant on personal health record data. PHR records encompass individual health examinations (biological), medical records, genome information, and life logs. PHR consists of three main elements: data, infrastructure (data storage, processing, and exchange), and applications (information exchange, analysis, and content provision). Due to the increasing demand for preventive medical services and safe, high-quality health information, a differentiated strategy is necessary to revitalize the PHR industry and enhance competitiveness (Clauson et al., 2018; Castaldo and Cinque 2018).

To ensure the quality and application of exponentially growing medical information, international standards related to blockchain technology and security have been implemented. This enables the international exchange and sharing of medical information among various institutions such as hospitals, medical research institutions, and national medical institutions. As interest in the medical environment has intensified, so has the demand for medical services. Consequently, the development of medical services has become a focal point, pushing for the advancement of medical information sharing systems (Patel 2019; Shen et al., 2019; Zhang et al., 2020).

Interest in blockchain technology has been steadily increasing, and research in blockchain-related fields has expanded extensively. Although initially devised for the financial sector, blockchain has extended its reach into various domains such as manufacturing, distribution, healthcare, content, and public services. It is expected to bring about significant industry-wide changes through a new paradigm of decentralization. Blockchain, in conjunction with core technologies of the fourth industrial revolution such as the Internet of Things (IoT), Big Data, and artificial intelligence, is anticipated to revolutionize society and industries as a whole (Ali et al., 2018; Fouka and Mantzourou 2021).

Blockchain is not limited to the financial industry but is spreading throughout multiple sectors, necessitating measures such as technology standardization and legal frameworks. To invigorate blockchain, deregulation and supportive policies are required to transition from the current centralized management system to a distributed open system. As a result, blockchain and distributed ledger technology have been standardized by various organizations and consortiums, including the International Organization for Standardization (ISO).

If medical data is distributed over the cloud infrastructure of medical institutions like hospitals, it can pose serious risks. Unauthorized access or infringement can jeopardize patient safety and have negative implications for patients, scientific research, and all stakeholders involved. To address this issue, this paper proposes a blockchain-based data sharing framework to tackle access control challenges related to sensitive data stored in the cloud.

The proposed system leverages the immutability of blockchain and incorporates built-in autonomy. It utilizes a permissioned blockchain, allowing access only to authorized users. This approach ensures additional authentication for users. The system operates within a blockchain environment, enabling efficient, extensive, and lightweight utilization.

In summary, the proposed framework aims to mitigate the risks associated with cloud-based medical data distribution by implementing a secure and decentralized blockchain solution. By ensuring access control and maintaining data integrity, it provides enhanced security and privacy for sensitive medical information.

2. Related Works

One of the definite advantages of blockchain technology is its potential for broad application in various fields such as finance, logistics, healthcare, and education. Blockchain technology is being utilized to address trust issues and preserve value, and its applications are expanding in the market. Particularly, investors and entrepreneurs are leveraging blockchain technology due to the ongoing changes driven by the proliferation of digital technologies like FinTech in the financial sector. Blockchain technology serves as a novel tool for facilitating value and capital exchange without the need for a central institution, thereby effectively addressing trust issues (Hepp et al., 2018; Dubovitskaya et al., 2020; Kyun et al., 2021).

Many observers believe that blockchain will emerge as a mainstream financial technology. In the future, access to limited financial services will be restricted to a new blockchain-based automated form of P2P lending. These services will only be available to individuals with certified financial records (Kyun et al., 2021; Wu and Kim 2022).

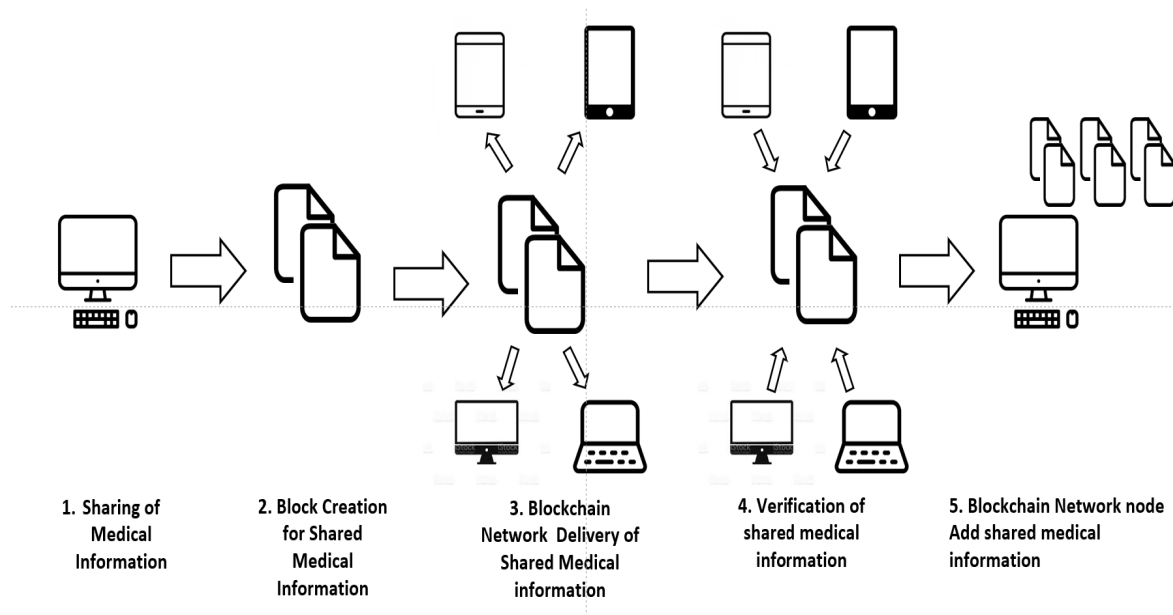


Fig. 1: Blockchain medical application mechanism

In fact, blockchain technology is considered one of the most successful applications that reduces information asymmetry and lowers transaction costs. In the current development of blockchain-based financial applications, there is a growing interest in health and the proliferation of smart devices, leading to the creation and distribution of health information by non-medical personnel after converting medical information into Electronic Medical Records (EMR). Even in the medical field, decentralization is important, and numerous application examples have emerged in this regard. The reliable exchange of data and information between doctors and patients in hospitals holds significant importance across various fields. From this perspective, blockchain applications should be further developed, and many related studies are actively underway (Wu and Kim 2022; Kyun et al., 2021; Lee 2020; Xiang et al., 2022).

In any field that involves the utilization of information, value, or goods, blockchain requires a central institution to delegate transactions and facilitate transactions between parties. It can enhance the security and traceability of products within the supply chain and aid in certification.

3. Technique of Blockchain-based System

Blockchain is a distributed database that contains an ordered list of interconnected records called blocks. It operates as a constantly growing, decentralized, and immutable ledger, particularly useful for transactions like financial transactions. Systems built on blockchain technology often rely on verifying transactions through a network of nodes. For instance, when client "A" transfers an asset to client "B," the asset is verified by a set of nodes, and the ownership of the asset is then assigned to client "A."

Clients transmit assets by assigning ownership to the new owner, such as client "B," and these transactions, verifications, and ownership changes are recorded in a public database for future reference and transactions. If any malicious activity is detected, verification nodes track the record properties and resolve the issue. To support such a system, highly immutable and stable databases are required. In summary, there is a need for a system that ensures secure transactions between parties who may not know each other's identities.

Blockchain technology is well-suited to address trust and data change-related problems. It offers highly decentralized cloud storage, with records of every client and every valid transaction guaranteed by the blockchain system. Overall, the properties of blockchain include secure data sharing, immutability, and the ability to conduct trustless transactions securely.

The structure of a blockchain network consists of individual blocks that are chained together, with events progressing from the first block to the current or next block. Detailed information about each event is stored in the connected blocks, forming a chain that can be modified, updated, or removed. This enables data forensics and improves data traceability in events. It is particularly useful when a user violates the group's data policy or if a malicious threat is detected. Essentially, the blockchain network acts as an immutable ledger, allowing only authorized individuals to broadcast processed and approved blocks.

Encryption keys play a crucial role in the proposed blockchain-based system for security-related tasks. These keys include:

Membership issuing key: Sent to a user requesting data sharing or participation, granting access to the membership verification key and enabling the creation of transaction private and public keys using appropriate parameters. Without the membership key, a user cannot sign up for the system.

Membership verification key: Used to authenticate the validity of a user in the system, granting access to the membership private key and verifying membership.

Membership private key: Used to create a request that will later be transformed into a block. Users cannot create requests without access to the membership private key.

Transaction private key: Used to digitally sign requests created using the membership private key.

Transaction public key: Used to verify the signature of a block.

The proposed system design utilizes a data sharing mechanism applied to blockchain-driven medical data sharing, essentially functioning as an electronic medical record system. It includes user and system management sections.

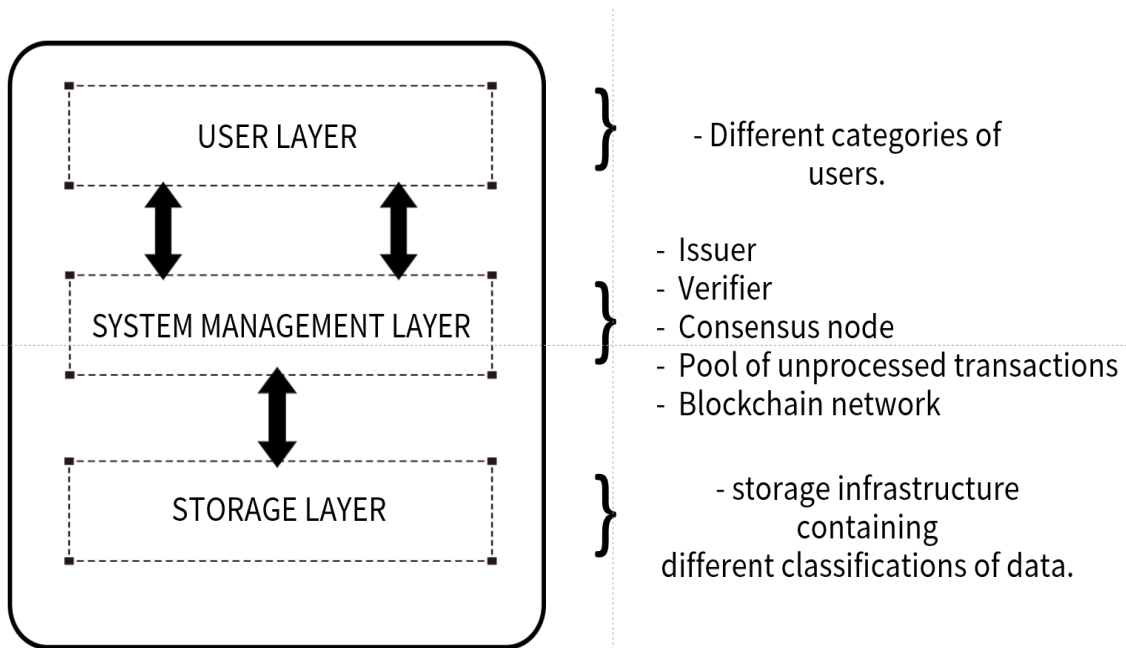


Fig. 2: Proposed system design

Users: Users refer to individuals or organizations, such as hospitals and research institutes, who seek access to or provide data within the system. **System Management:** System Management comprises interconnected entities responsible for security settings, efficient operation, and system optimization.

The different entities involved in system administration are as follows:

Issuer: The issuer configures the data manager layer of the group through authentication. When a user requests to join a group based on specific criteria, the issuer verifies the necessary details and accepts the user into the group.

Verifiers: Verifiers play a role in further authenticating users to become part of the data manager

layer. They receive the user's transaction key stored in the private database and validate the blocks signed by the user. Verifiers utilize the user's membership private key to create blocks, which form part of the blockchain within the system.

Consensus Nodes: Consensus nodes retrieve unprocessed blocks from the unprocessed pool and process and verify the details within those blocks. Once processed, the block is broadcast to the blockchain by consensus nodes.

Storage: The storage layer encompasses cloud-based data storage and processing infrastructure. It maintains data for various purposes, including referencing existing shared data stored in cloud storage or accessing data in the cloud storage for correction or analysis.

Overall, these entities and layers within the system administration ensure secure data management, authentication, and efficient operation of the system.

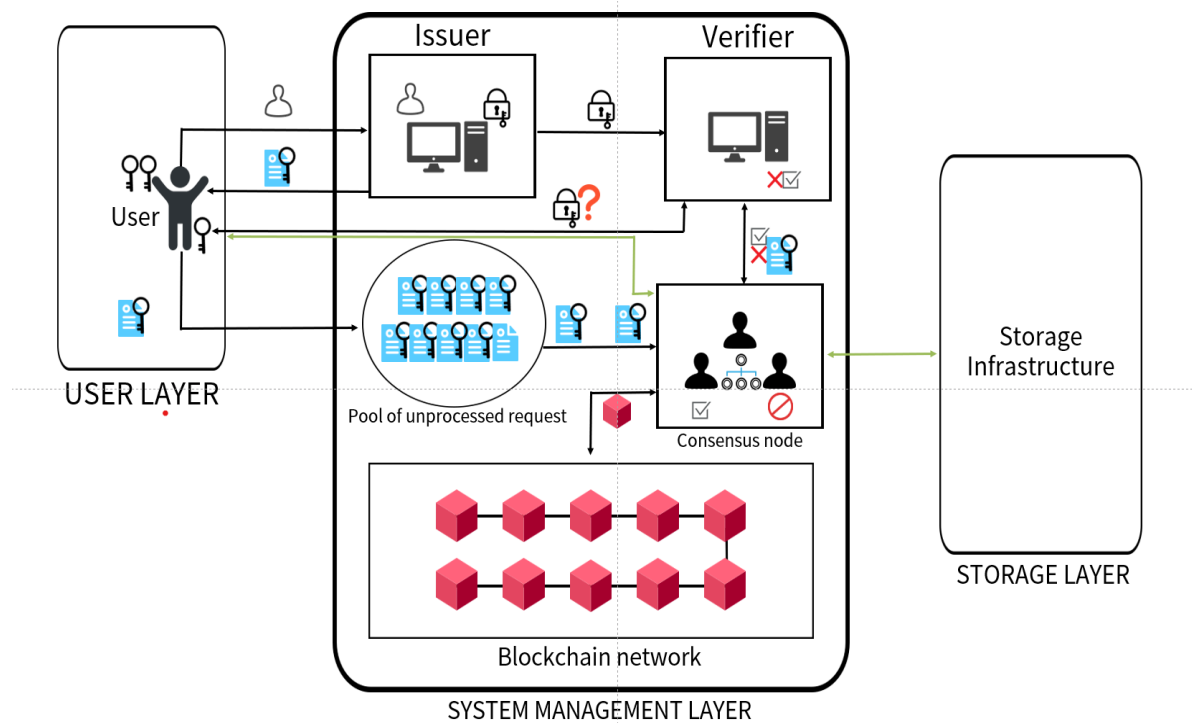


Fig. 3: Proposed system architecture

4. System Implementation

In this chapter, a shared framework is introduced and implemented to facilitate data sharing. Figure 3 illustrates the security structure that has been implemented for this purpose.

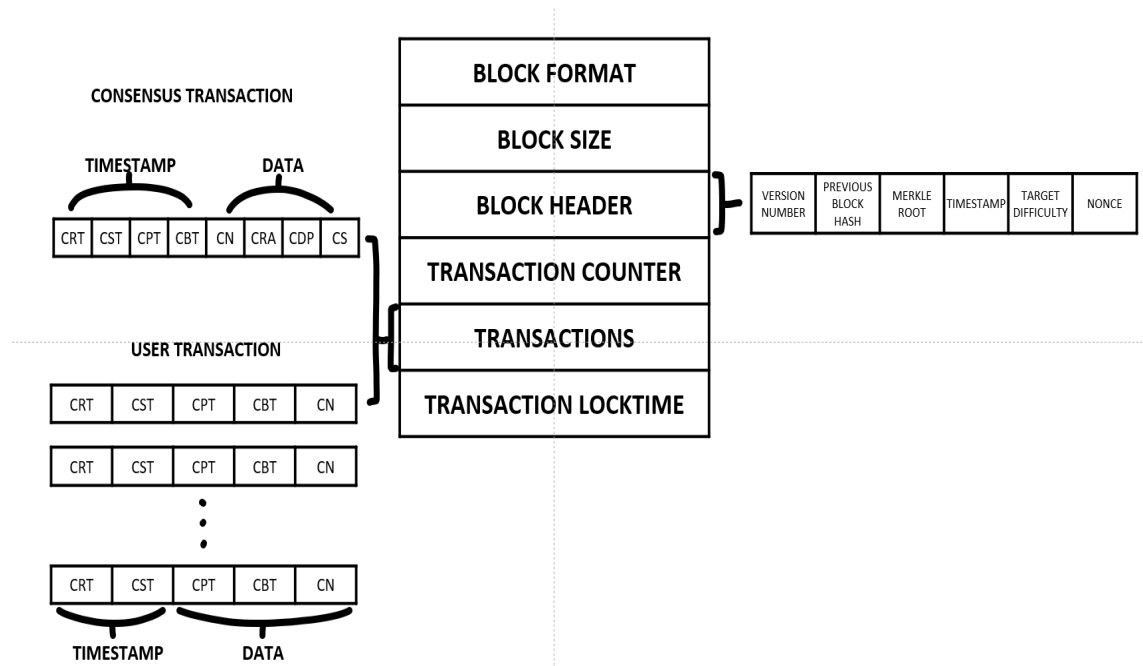


Fig. 4: Block structure

In the depicted figure, the issuer is responsible for generating the membership issuing key and a set of membership authentication keys. The issuer shares the membership verification key with the verifier. When a user intends to join an authorized group, they send a request to the issuer. The issuer then authenticates the user and decides whether to accept or deny their entry into the group. If accepted, the issuer sends the user a membership issuance key to complete the process.

Subsequently, the user performs the following steps:

The user verifies the issuer's key by transmitting the membership key along with the generated key to the issuer.

Upon entering the group, the issuer checks if the key is correctly configured and sends the verification key to the user along with other parameters.

Using the received parameters, the user creates transaction private and public keys.

The user sends their membership to the verifier and requests confirmation of their membership.

The verifier, upon receiving the user's membership, verifies their membership within the group. If the verification is successful, the verifier sends the user their membership in private. Additionally, the verifier generates membership private keys from the verification key and parameters.

Finally, the user sends the transaction private key to the verifier, and the verifier keeps the transaction open. These steps demonstrate the process of membership authentication, verification, and key generation within the shared framework as depicted in Figure 3. Figure 4. Block Structure

The request file contains information provided by the user who either wants to provide data or request access to data within the system. It is generated using the membership private key obtained during the membership authentication process from the verifier.

When sending a message, a block is created. The user utilizes the membership private key to create a block (request) and signs the request. Subsequently, the user includes the transaction private key and sends it to the outstanding request pool. The outstanding request pool consists of blocks that have not yet been processed by the consensus nodes. To transform a block into a request, the user needs to obtain valid consensus from the pool and prepare it for validation.

Each block represents a single event, with the event persisting from the moment the request is created until the block is broadcasted to the blockchain. If authorized institutions require it, requests can be sent to identify any abnormalities in the system, and access will be granted accordingly.

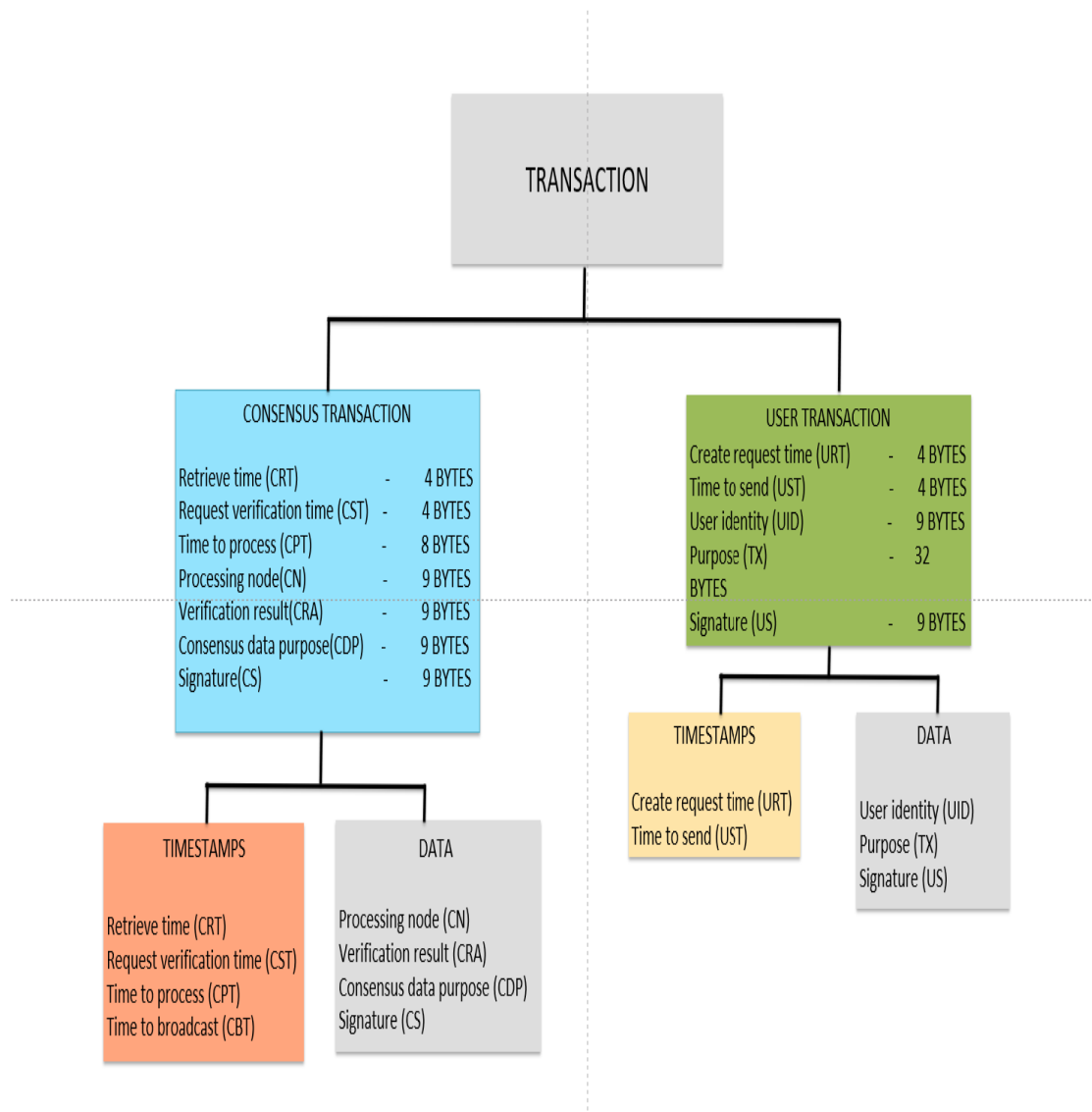


Fig. 5: Transaction structure

The final component that defines the entire block structure is the block locktime, which is a timestamp. It records the timestamp of the last transaction within the block, indicating the end of the block. Once all the requirements are met, the block is ready to be broadcasted to the blockchain network.

In general, block time refers to the moment when a block becomes part of the blockchain. Once a block enters the blockchain, it is added to the block height, representing its position within the chain.

When another block is created after a particular block in the system, it retrieves the header hash of the previous block and includes it in the header of the newly created block. This process continues, forming a chain of blocks. Figure 6 illustrates the entire process.

Overall, the block locktime, along with the block time and the connection between blocks, plays a crucial role in the structure and integrity of the blockchain system.

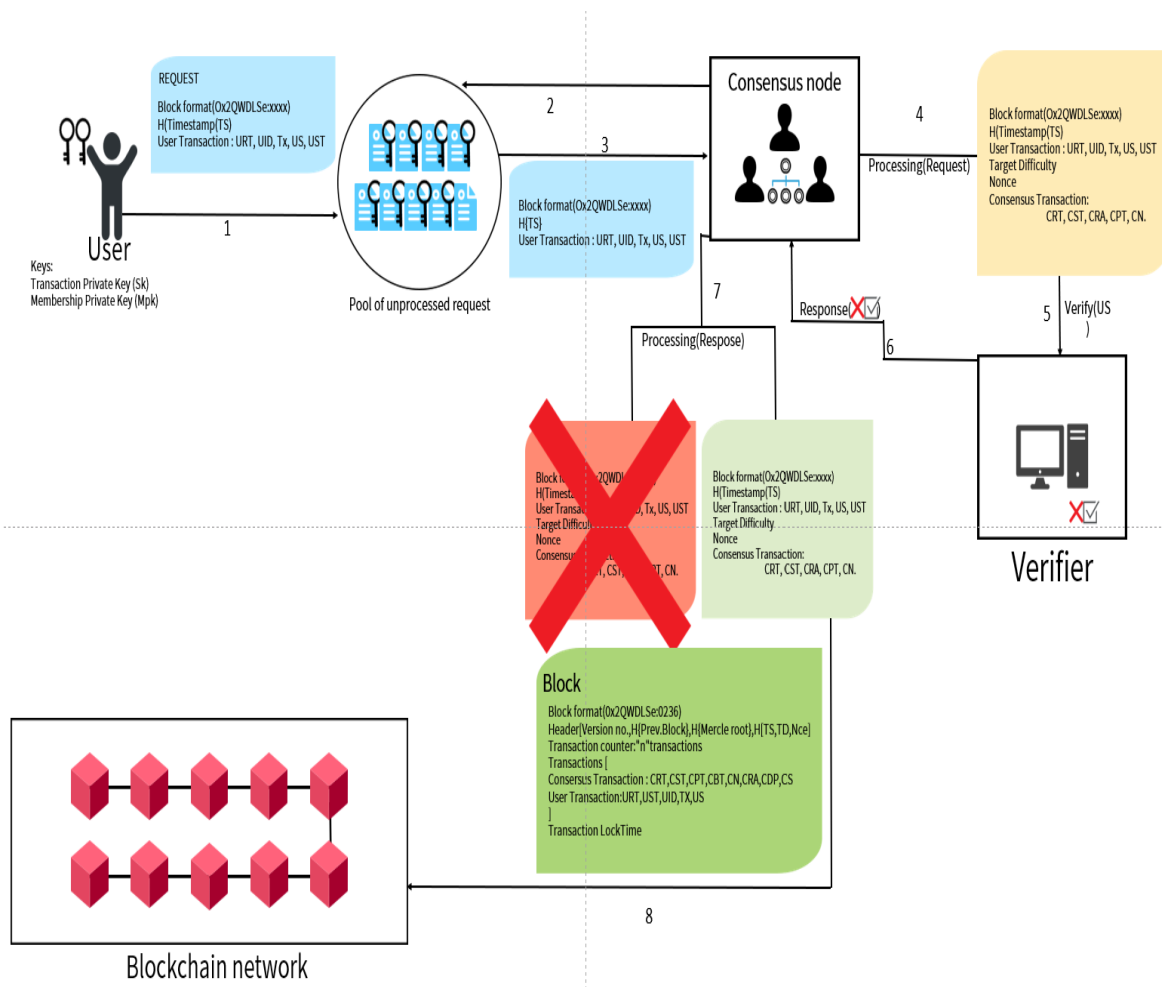


Fig. 6: Proposed BBDS system logic

The user verification protocol can be summarized as follows:

The user initiates the membership verification process by requesting verification from the verifier. The verifier responds by sending the membership issuance key, which is concatenated with a randomly generated number.

The user verifies the authenticity of the verifier by using the random number and responds to the verifier. The response is signed by the user using the membership verification key. Essentially, the user sends the random number to validate the verifier's identity as per the request.

The verifier compares the received signature and verification with the shared confirmation key stored in memory to ensure the authenticity of the user. Upon successful verification, the verifier sends the membership credentials and a random hash to the user.

The user further verifies the identity of the verifier and sends the transaction public key to the verifier. The verifier, upon receiving the transaction public key, stores it in a private database.

Additionally, the verifier verifies the membership private key using the verifier membership authentication key, ensuring the integrity of the membership verification process.

5. Conclusions

In conclusion, the paper proposes a novel blockchain-based architecture for decentralized, tamper-proof sharing of electronic health records among medical institutions. The system leverages cryptographic

access controls, distributed consensus, and blockchain immutability to enable secure, auditable PHR data exchange without centralized intermediaries. While conceptual, further inquiry is warranted to assess network scalability, adoption feasibility, and real-world performance.

Acknowledgements

Funding for this paper was provided by Namseoul University

References

- Abel, G. A., Mendonca, S. C., McPhail, S., Zhou, Y., Elliss-Brookes, L. & Lyratzopoulos, G. (2017). Emergency diagnosis of cancer and previous general practice consultations: Insights from linked patient survey data. *Br. J. Gen. Pract.* 67, e377–e387.
- Ali, S., Wang, G., White, B. & Cottrell, R. L. (2018). A blockchain-based decentralized data storage and access framework for PingER. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August, 1303–1308.
- Azaria, A., Ekblaw, A., Vieira, T. & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, 25–30.
- Castaldo, L. & Cinque, V. (2018). Blockchain-based logging for the cross-border exchange of ehealth data in Europe. In *Informatics and Intelligent Applications; Springer: Cham, Switzerland*, 46-56.
- Clauson, K. A., Breeden, E. A., Davidson, C. & Mackey, T. K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain Health Today*, 1, 1–12.
- Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P.S., Swaminathan, A., Jahangir, M., Chowdhry, K., Lachhani, R. & Idnani, N. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *J. Med. Internet Res.* 22, e13598.
- Fouka, G. & Mantzorou, M. (2011). What are the major ethical issues in conducting research? Is there a conflict between the research ethics and the nature of nursing? *Health Sci. J.* 5, 3.
- Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A. & Gipp, B., On-chain vs. off-chain storage for supply- and blockchain integration. *It-Inf. Technol.* 60, 283–291.
- Kyun, S., Yi, J. & Jang, J. (2021). A decentralized approach to education powered by blockchain technology. *Asia-pacific Journal of Convergent Research Interchange*, FuCoS, ISSN: 2508-9080 (Print); 2671-5325 (Online), 7(7), 131-141. DOI:<http://dx.doi.org/10.47116/apjcri.2021.07.13>.
- Lee, S. Y. (2020). Cloud-based blockchain technology for personal health. *International Journal of Advanced Nursing Education and Research*, 5(3), 47-54. DOI: <http://dx.doi.org/10.21742/IJANER.2020.5.3.05>.
- Maslove, D. M., Klein, J., Brohman, K. & Martin, P. (2018). using blockchain technology to manage clinical trials data: A proof-of-concept study. *JMIR Med. Inform*, 6, e11949.
- Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform.*, 25, 1398–1411.
- Roehrs, A.; da Costa, C. A. & Righi, R. D. R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *J. Biomed. Inform.* 71, 70–81.

Shapiro, J. S., Kannry, J., Lipton, M., Goldberg, E., Conocenti, P., Stuard, S., Wyatt, B. M. & Kuperman, G. (2006). Approaches to patient health information exchange and their impact on emergency medicine. *Ann. Emerg. Med*, 48, 426–432.

Shen, B., Guo, J. & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* 9, 1207.

Wong, D. R., Bhattacharya, S. & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nat. Commun.* 10, 1–8.

Wu, Y. –F. & Kim, H. –H. (2022). Research on the application of blockchain technology in the comprehensive health industry. *Asia-pacific Journal of Convergent Research Interchange*, FuCoS, ISSN: 2508-9080 (Print); 2671-5325 (Online), 8(3), 15-26. DOI:<http://dx.doi.org/10.47116/apjcri.2022.03.02>.

Wu, Y. F. & Kim, H. –H. (2022). Vocational education system architecture based on blockchain technology. *Asia-pacific Journal of Convergent Research Interchange*, FuCoS, ISSN: 2508-9080 (Print); 2671-5325 (Online), 8(6), 1-12. DOI:<http://dx.doi.org/10.47116/apjcri.2022.06.01>.

Xiang, Y., Kong, H., Li, M., Shen, B. & Tian, L. (2022). A new consortium blockchain for multi-center clinical data sharing. *Journal of Medical Internet Research*, 24(8), e38578.

Zhang, P., White, J., Schmidt, D. C., Lenz, G. & Rosenbloom, S. T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol*, 16, 267–278.

Zhang, R., Xue, R. & Liu, L. (2020). Security and privacy on blockchain. *ACM Comput. Surv.* 52, 1–34.