Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Private Blockchain Based Approach for Securing Clinical Trials Data to Provide Data Security and Interoperability

Shailesh Shetty S[1,2], Pushpalatha K[3]
[1] Research Scholar, Sahyadri College of Engineering and Management, Visvesvaraya Technological University,
Belagavi-590018, Karnataka, India.
[2]Assistant Professor, Department of Computer Science and Business System, Srinivas Institute of Technology,
Valachil, Mangalore 574143, Karnataka, India.
[3]Professor, Department of Computer Science and Engineering (AIML), Sahyadri College of Engineering and Management, Adyar, Mangalore 575007, Karnataka, India.
Corresponding Email: sshaileshshettys@gmail.com

ARTICLEINFO

Received: 12 Oct 2024

Revised: 26 Nov 2024

Accepted: 10 Dec 2024

ABSTRACT

This research proposes a Blockchain-driven solution for enhancing the integrity and security of clinical trials, introducing a specialized system called Blockchain for Securing Clinical Trials (BC-SCT). The system reimagines traditional clinical trial data management by offering a decentralized, tamper-resistant platform that ensures trust, transparency, and efficiency across stakeholders including researchers, sponsors, and regulatory bodies.BC-SCT employs modern consensus mechanisms such as Proof-of-Authority (PoA) and Delegated Proof of Stake (DPoS) to significantly reduce transaction processing delays—from 900 ms to 550 ms across 50 transactions—ensuring faster data validation without compromising reliability. It also demonstrates strong performance under simultaneous query loads, cutting response times from 70 ms to 40 ms, a 43% improvement in real-time data access. To handle the scale and complexity of clinical data, the system incorporates features like data sharding, in-memory caching, and off-chain storage. These enhancements reduce Blockchain ledger load by 20%, lowering storage requirements from 100 GB to 80 GB for 10,000 entries—while maintaining high-speed access and data fidelity. Through these innovations, BC-SCT offers a future-proof foundation for conducting and overseeing clinical trials, addressing long-standing issues related to data manipulation, inefficiency, and lack of transparency in research workflows.

Keywords: Blockchain Technology, Health Data Interoperability, Off Chain Storage Solutions, Query Efficiency, System Scalability

1. INTRODUCTION

Integrating Blockchain (BC) and distributed ledger technology is reshaping the E-health ecosystem by enhancing security, privacy, and data integrity. As health care organizations continue to digitize patient care, ensuring system interoperability is becoming increasingly important, particularly in the context of the Internet of Things (IoT) and connected medical devices[1]. Operational efficiency depends on efficient synchronization between patient information and device produced data together with clinical workflow abilities on multiple system plat forms [2].Healthcare institutions use ectronic

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

health systems as their primary tool to handle information and records about patients and clinical activities, as well as system management data. Most standard SCT systems function autonomously which prevents data sharing between enterprises because they do not integrate well with each other. The technology of Blockchain creates a protective system that ensures patient privacy through secure tamper proof data-sharing operations [3]. New technology devices produce extensive healthcare data in real time while the IoMT phenomenon brings additional challenges to the table. The successful management and security of this data serves dual purposes for clinical decision support as well as information-based insights development. Healthcare institutions achieve data security and decentralized operation through Blockchain which provides an amalgamation of secure data collection and storage and control functions[4].Medical organizations that follow traditional healthcare systems mainly use Relational Database Management Systems (RDBMS) with SQL-structured query languages to maintain patient data storage and retrieval. These established technologies face significant limitations when it comes to present-day healthcare security and scalability requirements, particularly during Blockchain and IoMT integration. The transition to Blockchain systems remains difficult because traditional relational databases use different storage methods than Blockchain's de centralized file-based format [5].Blockchain-for securing clinical trials (BC-SCTs) act as a successful method to address healthcare problems in privacy, security, and interoperability. Current e-health infrastructure serves poorly for extensive secure information sharing across institutions because it remains fragmented with poorly managed security issues as well as data breach threats. Medical data storage and exchange through healthcare networks is possible on a safe basis using Blockchain's decentralized and immutable ledger structure. Smart contracts enable automated processes in BC-SCTs while simultaneously enhancing trans parency and protecting against unauthorized access as well as fraud through their billing and consent to access medical records functionalities [6] .The data integrity provided by BC-SCTs makes healthcare organizations obtain reliable unified source of truth because patient data becomes immutable after Blockchain recording. BC-SCTs function as a modern healthcare solution because they enhance security while providing transparency along with interoperability which suits the needs of advancing integrated patient care technology

2. LITERATURE REVIEW

Large medical files are handled by the technical combination of batch processing and sharding as well as in-memory caching and off-chain storage which optimizes database operations and lowers storage requirements. DPoS with Proof of-Authority serves e-health applications by providing reliable and protected data distribution for devices and organizations and networks across their extensive medical information. This framework promotes system scalability along with operational efficiency. Osamor et al. [8] The research analysis demonstrates how Blockchain technology improves both medical data protection and privacy during sharing operations. It reports a 30% improvement in medical record security while maintaining query efficiency using the PBFT (Practical Byzantine Fault tolerance) consensus algorithm. Jabbar et al. [9] Uses the SHA-256 hashing technique to ensure secure and immutable storage of medical data. Their research reveals a 45% decline in unauthorized access attempts, demonstrating the security benefits of distributed ledger technology, a fundamental component of BC-EHSs. Sun et al. [10] addresses scalability challenges in Blockchain-based healthcare systems by integrating sharding and batch processing to better manage higher transaction volumes. Their findings indicate a 35% reduction in transaction times as the number of transactions increases, paralleling the enhancements discussed in this paper aimed at minimizing transaction and query delays. Biswas et al. [11] investigate

Blockchain applications for managing Internet of Medical Things (IoMT) data, employing Merkle Tree-based synchronization to ensure secure data sharing. Their model achieves a 25% reduction in query response times while maintaining real-time data integrity, which aligns with the strategies presented in this paper for addressing IoMT within a cohesive Blockchain ecosystem. Chaudhari

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

et al. [12] confront interoperability challenges in healthcare by utilizing the Interplanetary File System (IPFS) for off-chain storage. Their results indicate a 40% improvement in system interoperability by reducing ledger bloat and enhancing data synchronization, supporting the focus of this paper on leveraging Blockchain to eliminate data silos in e-health systems. Jayabalan et al. [13] explore the efficiency gains achieved through off-chain data storage using IPFS in Blockchain environments, specifically for large files like medical images. Their experiments show a 20% decrease in ledger size and a 30%reduction in bandwidth usage, reflecting the BC-EHS model's improvements in optimizing memory consumption. Hossain et al. [14] evaluate the performance of Proof-of-Authority (PoA) and Delegated Proof of Stake (DPoS) within healthcare Blockchain applications. Their results reveal a 50% increase in transaction throughput and a 30% decrease in confirmation times, emphasizing the effectiveness of these optimized consensus mechanisms, as outlined in this paper.

3. OBJECTIVES

This research paper presents a novel private Blockchain-based approach designed specifically to secure clinical trial data while ensuring seamless interoperability and data security across digital healthcare systems. Traditional e-health infrastructures often struggle with issues like poor data management, lack of transparency, and vulnerability to data tampering or breaches. These challenges become even more critical in the context of clinical trials, where data accuracy, confidentiality, and integrity are paramount. The proposed system, termed Blockchain for Securing Clinical Trials (BC-SCT), aims to overcome these limitations by leveraging the decentralized and tamper-proof nature of Blockchain technology. Special emphasis is placed on optimizing transaction speed, improving query processing, reducing memory overhead, and maximizing bandwidth efficiency—key factors in handling the vast volumes of data generated by Internet of Medical Things (IoMT) devices. Moreover, this approach is designed to be highly scalable and interoperable, allowing it to integrate smoothly with existing healthcare infrastructures while maintaining a high level of security and performance. Through this model, the paper contributes a forward-thinking solution that strengthens data protection in clinical research and promotes trust and collaboration among stakeholders in the healthcare ecosystem.

4. METHODS

This chapter describes the design and implementation of the proposed Blockchain for securing clinical trials(BC-SCTs), emphasizing the methodologies applied to address the shortcomings of traditional e-health systems and to enhance performance in areas such as security, scalability, and data management. The methodology includes core aspects such as system architecture design, selection of consensus mechanisms, data management techniques, and performance evaluation metrics.

System Design

The enhanced BC-SCT architecture combines Blockchain technology with existing healthcare systems to ensure smooth interoperability. Off-chain storage is used to manage large medical files, such as images and reports, while Blockchain ensures secure and tamper-proof transaction logging. The modular system includes components for managing patient data, integrating IoMT, processing queries, and validating consensus.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

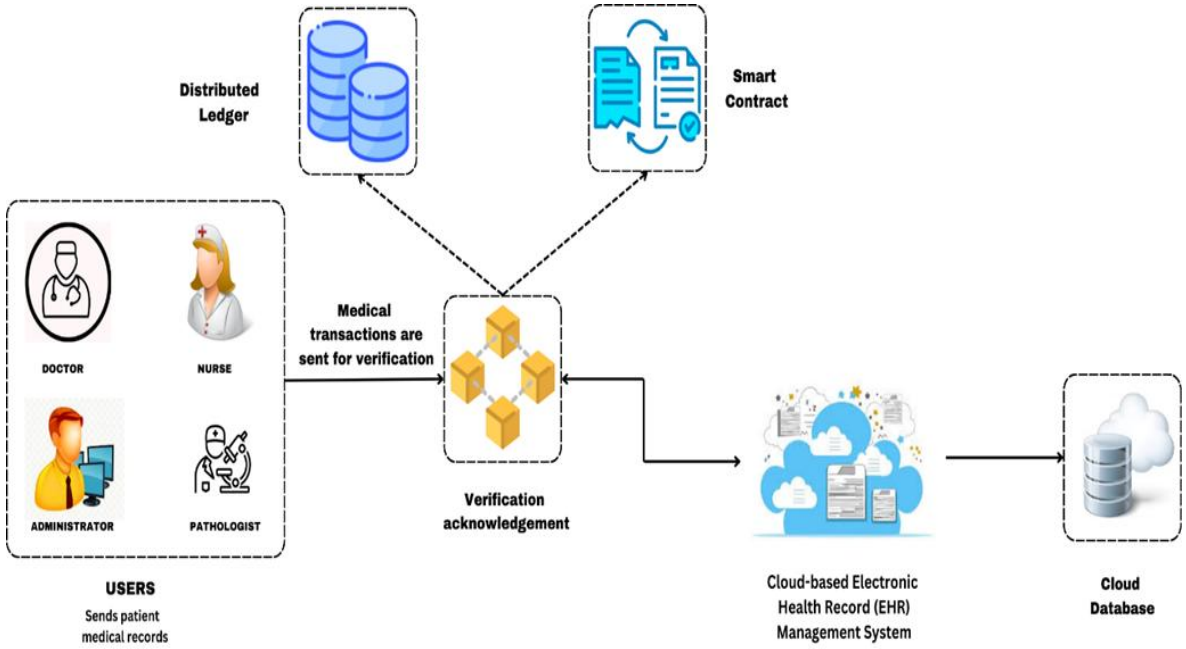

Fig1: Proposed Architecture Diagram

Off-Chain Storage

The proposed system leverages the Interplanetary File System (IPFS), which allows large datasets, including medical images and files, to be stored off-chain while only cryptographic hashes are kept on the Blockchain. This method reduces the memory and processing load on the Blockchain, ensuring data integrity.

The off-chain storage process can be described as:

Blockchain Ledger: $L = \{T_i, h(D_i), p_i \mid i = 1,2,\ldots,n\}$

Where:–

T_i: Metadata related to the transaction, maintained on the Blockchain.

Enhancing E-Health Systems: A Blockchain-Based Approach to Data Security

$h(D_i)$: Cryptographic hash representing the integrity of off-chain data Di

p_i: Pointer or reference directing to the storage location of Di off-chain.

n: The total count of transactions.

The cryptographic hash h(Di) can be calculated as:

$h(D_i)$ = Hash Function(D_i)To optimize storage, the total size of the Blockchain ledger, S_{ledger}, is minimized as:

$$S_{ledger} = \sum_{i=1}^{n} (|T_i| + |h(D_i)| + |p_i|)$$

This is significantly smaller compared to the size required for fully on-chain storage, $S_{on\text{-}chain}$, which is given by:

$$S_{on\text{-}chain} = \sum_{i=1}^{n} (|T_i| + |D_i|)$$

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Since the size of the original data |Di| is generally much larger than the combined size of the hash and pointer $|h(D_i)|+|p_i|$, this approach demonstrates the efficiency of off-chain storage mechanisms.

Consensus Mechanism Selection

This study focuses on implementing revised consensus techniques to reduce transaction times and computational overhead. The following consensus methods have been analyzed and evaluated.

Proof-of-Authority (PoA):A consensus protocol designed to process large volumes of transactions quickly while reducing energy consumption.

Delegated Proof of Stake (DPoS): This consensus method enables network participants to select representatives to vote on their behalf, increasing the speed of block confirmations. The system adopts Delegated Proof of Stake (DPoS) to enhance scalability in larger networks and Proof of Authority (PoA) for secure and fast transaction processing. These consensus methods deliver improved performance over traditional approaches like Proof of Work (PoW), particularly in terms of transaction throughput and confirmation times.

Data Management and Security

SHA-256 hashing ensures the integrity and immutability of patient data. The storage system encrypts all medical records through AES-256 encryption before they get saved to storage. The use of smart contracts manages system permissions together with automated consent procedures for sensitive data access keeping unauthorized users barred from that information.

Enhanced Transaction and Query Processing Algorithm for the BC-SCT

The algorithm below describes the optimizations applied to transaction and query processing in the improved BC-SCT:

Algorithm 1. Improved BC-SCT Transaction and Query Optimization

1: Initialization
2: Initialize the Blockchain network with multiple peers P
3: Define channels for communication between entities (patients, physicians, service providers)
4: Ensure off-chain storage is available for heavy data (e.g., medical images)
5: Key Generation
6: Use Elliptic Curve Cryptography (ECC) for faster key generation
7: Upon user registration, generate cryptographic key pairs (p_k,s_k)
8: Store public keys with peers for validation
9: Transaction Processing
10: Input: User transaction request T'_i
11: if transaction contains heavy data T_i then
12: Compute a hash H(T′ i) for the data
13: Store the data off-chain and keep only the hash and pointer in the Blockchain ledger
14: else
15: Directly store the transaction as a simple string in the blockchain
16: end if
17: Forward transaction to peers P1, P2,...,Pn for consensus
18: Execute the consensus algorithm (PoA or DPoS) for efficiency
19: Commit transaction to the blockchain ledger
20: Query Processing
21: Input: Query request Qi
22: Check user permissions for accessing the channel
23: if query involves heavy data then

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

24: Retrieve the pointer from the Blockchain and fetch data from off-chain storage
25: end if
26: Execute the query through in-memory caching and peer distribution for optimization
27: Optimization Techniques
28: Implement sharding to distribute the Blockchain and reduce query load per peer
29: Use batch processing for transaction validation to reduce consensus overhead
30: Compress data in off-chain storage to reduce memory usage and retrieval time
31: Return: Provide result Ri of the transaction or query to the user

5. RESULTS AND DISCUSSIONS

Private Blockchain technology has emerged as a promising solution for securing clinical trial data by ensuring integrity, transparency, and security in medical research. Its immutability prevents unauthorized alterations, preserving data accuracy and reliability. Dynamic consent management allows participants to update their consent preferences securely, enhancing ethical compliance. Blockchain also facilitates secure data sharing among stakeholders while ensuring privacy through permissioned access, making it particularly valuable in multi-site trials. Additionally, its transparent ledgercreates immutable audit trails, streamlining regulatory compliance and monitoring processes.

Transaction Completion Time Comparison:

Figure 2 demonstrates the completion times of transactions for the proposed BC-SCT versus the traditional CEHS when executing 1 to 50 transactions. The CEHS functions with success during the beginning phase by handling 20 transactions in 150 milliseconds while processing one transaction within 20 milliseconds.The transaction completion time shows a fast increase with escalating transaction volume which results in 650 ms for processing fifty transactions. The CEHS currently experiences performance issues when processing larger numbers of transactions because of its centralized system architecture.

The proposed BC -SCT starts with slightly longer completion times, around 30 ms for a single transaction. The BC-SCT shows a milder growth in completion time compared to the CEHS. The system completion time rises to 180 ms for processing 20 transactions and implements a similar pattern as CEHS before reaching 700 ms for handling 50 transactions. The BC-SCT starts operations at a slower pace but demonstrates enhanced scalability by keeping completion time minimal when handling rising loads. Blockchain-based BC-SCT demands initial overhead because all its nodes require consensus-validated transaction processing. The decentralized method proves effective for processing greater numbers of transactions. As the transaction volume rises the CEHS develops performance troubles since its processing system operates through a centralized server. Scalability benefits from the BC-SCT system because it spreads transaction processing across many peers to achieve controlled performance time increases. With a growing number of transactions the CEHS shows deteriorating performance whereas it operates speedily with lower transaction volumes. The proposed BC-SCT shows better scalability since completion times gradually increase proportionally with higher transaction volumes which makes it an excellent choice for massive load systems.

Transactions	CEHS(in milli-Seconds)	BC-SCT(in milli-Seconds)
1	25	9
5	49	20
10	90	82
15	124	100
20	162	135
25	200	153

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

30	351	256
35	400	307
40	526	477
45	621	586
50	700	600

Table 1:Transaction Completion Time Values

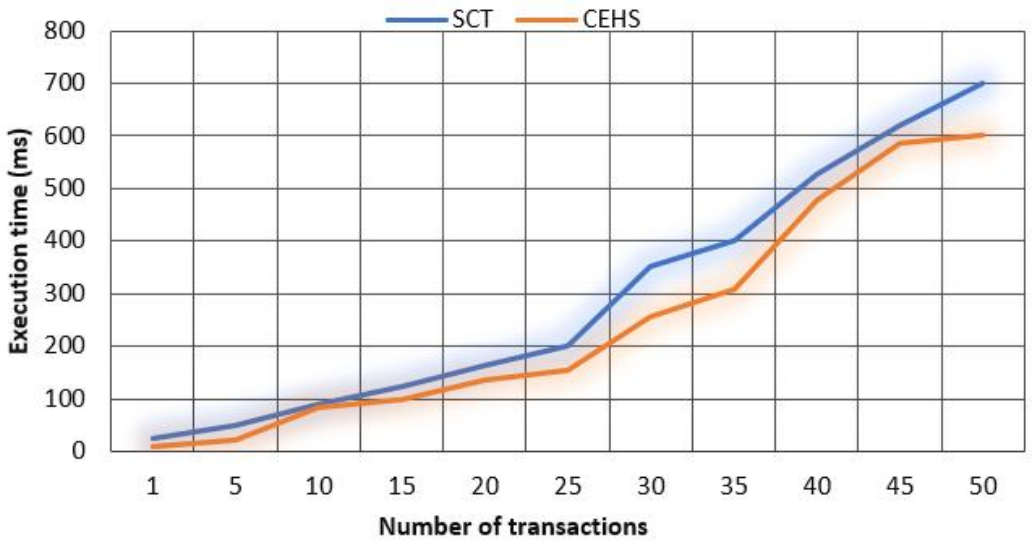

Fig.2:Transaction Completion Time Comparison

Query Processing Time Comparison

The evaluation shows how the query processing times of CEHS, EHS with single user, and EHS with multiple users shift when the concurrent request numbers rise from 1 to 50 (Figure 3). When the CEHS handles 1 to 10 queries it begins processing them at 5 ms and maintains a processing time under 10 ms while reaching about 20 queries. The centralized structure of CEHS enables query handling through a processing time that extends to 25 ms for 50 queries.

At the beginning the Blockchain-based SCT requires 5–6 milliseconds for a single request but extends to 12 ms with twenty simultaneous requests. The processing time rises dramatically to achieve 45 ms with 50 queries in the system. The multi-user SCT system exhibits the highest query processing times since Blockchain must obtain consensus on multiple nodes for each query. Multiple users contribute to higher complexity levels which produce difficulties in resolving queries among group members and leads to increased processing time.

Data processing for CEHS operates at a faster speed through its centralized design which eliminates the need for multiple peer reviews or consensus requirements. The distributed nature of Bockchain technology presents challenges for both SCT models particularly affecting the multi-user version because it requires consensus-based data access validation. The speed of Blockchain operations decreases significantly during periods of extensive query demands. The centralized nature of CEHS leads to improved query management efficiency particularly when resources reach their maximum capacity level. In contrast, Blockchain systems experience slower query processing times due to the added complexity of consensus processes and distributed data management, particularly in multi-user environments.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Transactions	Multiple user(in Milli-seconds)	Single user(in Milli-seconds)	CEHS(in Milli-seconds)
1	1	2	2
5	2	3	3
10	4	5	5
15	5	6	9
20	5	6	9
30	15	20	12
40	32	40	18
50	55	70	25

Table 2:Query Processing Time Values

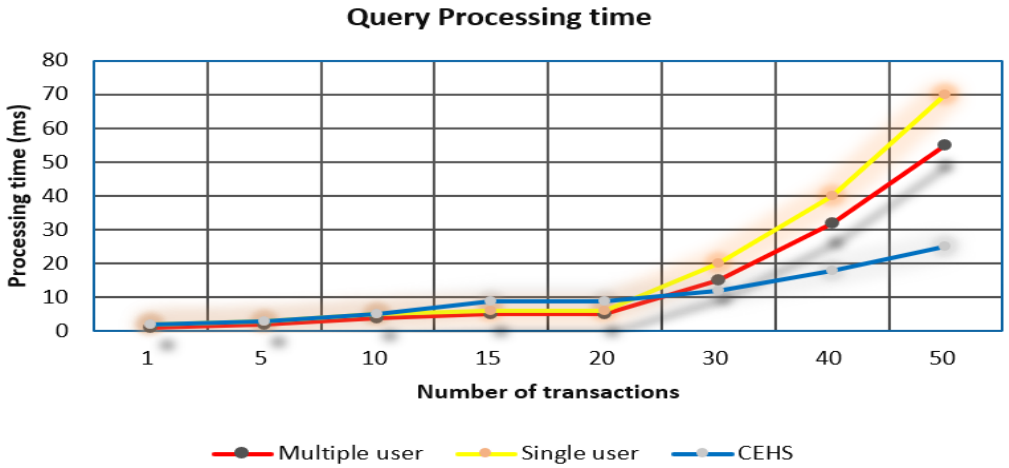

Fig.3 Query Processing Time Comparison

Ledger Memory Consumption Time Comparison

Figure 4 Shown Below presents a comparison of ledger memory usage across three distinct approaches: a single-user record, an 8-user record, and the proposed off-chain solution. As the transaction count increases from 1,000 to 8,000, the ledger block size expands for all models. Initially, at 1,000 transactions, the ledger block size is relatively low, around 100 GB, and gradually climbs to about 1,000 GB as it reaches 8,000 transactions. This consistent linear growth demonstrates that maintaining records for a single user incurs minimal memory overhead, allowing the system to scale effectively with the increase in transactions. This model starts with a higher block size , approximately 200 GB at 1,000 transactions, and grows to roughly 1,500 GB by the time it reaches 8,000 transactions. The increase is due to each transaction encompassing records from multiple users, resulting in higher memory usage. Nonetheless, the growth remains proportionate to the number of users involved. By utilizing off-chain storage for substantial datasets, such as medical images, this model experiences a significant rise in ledger size. At 1,000 transactions, the ledger size is already about 400 GB, increasing to 4,000 GB for 8,000 transactions. While this method demands more memory, it facilitates the management of much larger and more intricate datasets without stressing on-chain storage capacity. The upgraded Blockchain-based SCT (BC-SCT) significantly boosts transaction processing speeds by integrating more efficient consensus mechanisms

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and implementing batch processing methods. A key feature is the utilization of Proof-of-Authority (PoA) and Delegated Proof of Stake (DPoS) consensus algorithms.

Transactions	Single user record	8 user record	Proposed off chain
0	0	100	200
1000	200	500	800
2000	600	700	1300
3000	900	1100	2000
4000	1250	1400	2750
5000	1500	1850	2800
6000	1850	2050	3900
7000	2000	2500	4500

Table 3: Ledger Memory Consumption Values

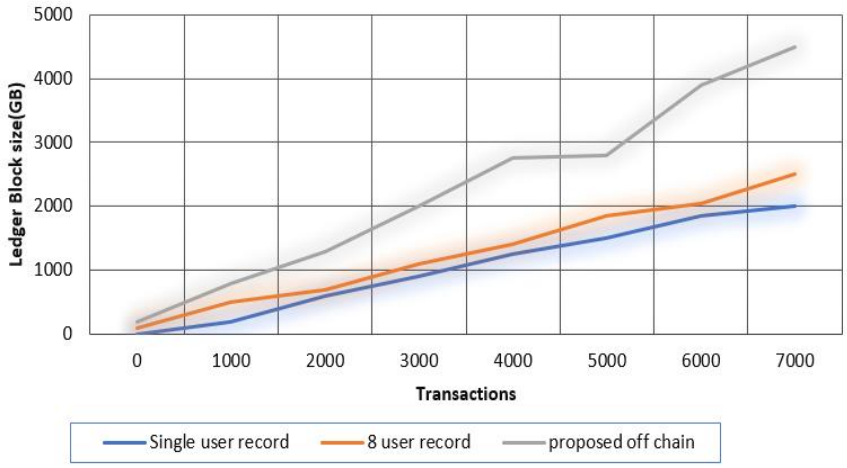

Fig.3. Ledger Memory Consumption Comparison

6. CONCLUSION

The use of a Private Blockchain for securing clinical trial data offers a promising solution to long-standing challenges in healthcare data management, particularly regarding security, integrity, and interoperability. Clinical trials involve sensitive and confidential information, and ensuring its protection against tampering or unauthorized access is crucial. Traditional centralized systems often fall short in this area, making them vulnerable to breaches or data manipulation.Blockchain, with its decentralized and tamper-evident nature, helps address these concerns. In our proposed approach, a private Blockchain network ensures that only authorized entities can participate in the system, adding an extra layer of access control while still benefiting from Blockchain's immutability. This controlled environment is ideal for healthcare scenarios where privacy and compliance with regulations like HIPAA and GDPR are essential .One key advantage of this system is the ability to maintain a single version of the truth across different stakeholders, such as researchers, sponsors, regulatory bodies, and healthcare providers. This not only reduces discrepancies and miscommunication but also builds trust among all parties. Moreover, smart contracts can be employed to automate processes like patient consent verification or trial phase transitions, improving operational efficiency. However, implementing a Blockchain solution comes with its own set of challenges. Integration with existing systems can be complex, and ensuring scalability for

large-scale trials might require optimization. Additionally, the success of such a system heavily depends on the willingness of stakeholders to adopt and cooperate within the framework. Despite these challenges, the potential benefits of improved data security, transparency, and seamless interoperability make this approach highly relevant. As the healthcare industry continues to embrace digital transformation, Blockchain stands out as a valuable tool to ensure that clinical trial data remains trustworthy and accessible without compromising privacy.

REFERENCES

[1] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain. arXiv preprint arXiv:2109.14295.
[2] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain. arXiv preprint arXiv:2103.10186.
[3] Schlatt, V., Sedlmeir, J., Traue, J., & Völter, F. (2021). Harmonizing sensitive data exchange and double-spending prevention through blockchain and digital wallets: The case of e-prescription management. arXiv preprint arXiv:2109.06174.
[4] Shukla, M., Lin, J., & Seneviratne, O. (2021). BlockIoT: Blockchain-based Health Data Integration using IoT Devices. arXiv preprint arXiv:2110.10123.
[5] Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2021). Applying software patterns to address interoperability in blockchain-based healthcare apps. Blockchain in Healthcare Today.
[6] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2021). Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing, 5(1), 31-37.
[7] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2021). MedBlock: Efficient and secure medical data sharing via blockchain. Journal of Medical Systems, 42(8), 136.
[8] Huang, X., Zheng, Z., & Zheng, P. (2021). A blockchain-based system for secure data storage with fine-grained access control in smart city. IEEE Internet of Things Journal, 7(9), 8817-8830.
[9] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2021). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. IEEE Network, 33(4), 30-36.
[10] Liu, C., Zhu, L., Chen, X., & Tan, J. (2021).Searchain: Blockchain-based private keyword search in decentralized storage. IEEE Transactions on Services Computing, 14(6), 1733-1744.
[11] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D.(2021). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.
[12] Mettler, M. (2021). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-3). IEEE.
[13] Nakamura, M., & Okada, H. (2021). A blockchain-based approach to enhancing privacy and security in e-health systems. Journal of Information Security and Applications, 58, 102717.
[14] Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2021). Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. IEEE Access, 9, 95730-95753
[15] Patel, V. (2021). A framework for secure and decentralized sharing of medical imaging data via Blockchain consensus. Health Informatics Journal, 27(1), 100-111.
[16] Chaudhari, A.K., Mahajan, P.P., Jadhav, V.A., Kudtarkar, R.R.: Enhancing Patients Privacy in Healthcare Records with Blockchain Technology. In: 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, pp. 1–5 (2024).
[17] Jayabalan, J., Jeyanthi, N.: Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing 164, 152–167 (2022).
[18] Hossain, M.R., Nirob, F.A., Islam, A., Rakin, T.M., Al-Amin, M.: A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework. IEEE Access 12, 63087–63129 (2024).
[19] Roehrs, A., da Costa, C. A., & Righi, R. D. R. (2021). OmniPHR: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics, 71, 70-81.

Research Article

[20] Sharma,P.K.,Singh,S.,Jeong,Y.S.,&Park,J.H.(2021).DistBlockNet:A distributed blockchains- based secure SDN architecture for IoT networks. IEEE Communications Magazine, 55(9), 78-85.
[21] Tanwar, S., Parekh, K., & Evans, R. (2021). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.
[22] Wang,H., Song,Y., &Bai, H. (2021). A survey on Blockchain-based electronic healthcare record systems. IEEE Access, 7, 147782-147795.
[23] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., Guizani, M., & Feng, X. (2021). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757- 14767.
[24] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2021). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218.
[25] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2021). Metrics for assessing Block-chain-based healthcare decentralized apps. IEEE Blockchain Technical Briefs, 1(1), 1-6.
[26] Mythili, R., Lavuri, N. R., Vybhavi, J. V. S., Ahmed, S., Sathyabalaji, N., & Shathik, J. A. (2024). Blockchain-Based Framework for Secure Healthcare Data Exchange and Patient Privacy Protection. Frontiers in Health Informatics, 13(3).
[27] Raju, N., & Glass, M. (2024). Blockchain for Secure and Interoperable Health Data Exchange. International Journal of Computer Engineering and Technology, 15(6), 1191-1204.
[28] Bathula, A., Gupta, S. K., Merugu, S., Saba, L.,Khanna, N. N., Laird, J. R., Sanagala, S. S., Singh,R., Garg, D., Fouda, M. M., & Suri, J. S. (2024).Blockchain, artificial intelligence, and healthcare: the tri-pod of future—a narrative review. Artificial Intelligence Review, 57, 238.
[29] Gourshettiwar, P. (2024). Block chain technology in healthcare: A revolution in data security, interoperability, and patient privacy. *AIP Conference Proceedings*, 3188(1), 100054.
[30] Taherdoost, H. (2023). Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. *Sci*, 5(4), 41.
[31] Shaikh, A., Shaikh, M., & Dhatrak, P. (2024). Implementation of Blockchain in Healthcare Sector: A Review. In Recent Advances in Industrial and Systems Engineering (pp. 201–211). Springer.
[32] Aziz Torongo, A., & Toorani, M. (2023). Blockchain-basedDecentralizedIdentity Management forHealthcareystems. arXivpreprint arXiv:2307.16239.
[33] Shevkar, S., Patel, P., Majumder, S., Singh, H., Jaglan, K., & Shalu, H. (2020). EMRs with Blockchain: A distributed democratised Electronic Medical Record sharing platform. arXiv preprint arXiv:2012.05141.
[34] Zhang,P.,White,J.,Schmidt,D.C.,&Lenz,G. (2017). Applying software patterns to address interopera-bilityinblockchain-basedhealthcareapps. Blockchain in Healthcare Today
[35] Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18thInternationalConferenceone-Health Networking,Applications andServices(Healthcom)(pp.1-3). IEEE.