





A Blockchain-Based Decentralized Framework for Securing Medical Research Data via Digital Timestamping

Saima Zareen Ansari^{1*}, Shrikant D. Zade²

¹ Department of Computer Science and Engineering, G.H. Raisoni University, Pandhurna 480337, India

² Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur 441501, India

Corresponding Author Email: saimazareen.ansari.phdcs@ghru.edu.in

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/isi.300718>

ABSTRACT

Received: 10 June 2025

Revised: 14 July 2025

Accepted: 19 July 2025

Available online: 31 July 2025

Keywords:

intellectual property, digital timestamping, blockchain, medical research, data protection, smart contracts, data integrity

Medical research often involves multiple collaborators, each contributing at various stages of a project. This fragmented workflow makes it challenging to safeguard intellectual property (IP) rights fairly and efficiently. Traditional IP protection systems are slow, complex, and discourage proactive participation, especially for early-stage findings. To address this gap, this paper introduces a decentralized digital timestamping system that enables researchers to lock in ownership quickly. A central innovation is polling-based consensus mechanism, which replaces heavy computational proofs with lightweight distributed voting, ensuring fairness and rapid agreement among collaborators. This approach not only reduces computational overhead but also cuts IP dispute resolution time by nearly 40%, making the protection process significantly faster than conventional models. By integrating blockchain based timestamping with layered data architecture, proposed framework secures medical research data at every step from initial observation to final publication, while simplifying IP claims, strengthening accountability, and preserving data integrity in collaborative research.

1. INTRODUCTION

Medical research thrives on collaboration, with researchers contributing data, experiments, and analysis across various phases of a project. The collective nature of such research efforts, while fostering innovation, often leads to complications in recognizing and attributing individual contributions. Traditional intellectual property rights (IPR) frameworks tend to focus on the final outcomes rather than the granular process of contribution [1, 2]. As a result, disputes regarding ownership, credit allocation, and the value of individual efforts are common, especially in large-scale, multi-institutional collaborations.

Digital timestamping has emerged as a widely accepted method for establishing document authenticity by recording the existence of a document at a specific point in time [3]. It provides a verifiable way to prove the origin and integrity of research data. However, while timestamping is effective for preserving the chronological integrity of documents, it falls short in addressing the complexities of contribution assessment. It cannot independently capture the nuances of collaborative efforts, nor can it resolve disputes related to the distribution of credit among contributors.

Blockchain technology, known for its decentralized and tamper-resistant architecture, offers a transformative approach to enhancing the reliability of digital timestamping [4]. By leveraging a distributed ledger system, blockchain ensures that once data is recorded, it cannot be modified or deleted without consensus from the network. This immutability, coupled with

transparency, makes blockchain an ideal solution for securing sensitive research data.

This paper proposes an innovative framework that integrates blockchain-based digital timestamping with a structured polling-based consensus mechanism. The polling mechanism allows contributors to actively participate in evaluating and validating each member's input, ensuring fair and democratic allocation of credit. By embedding this mechanism within a blockchain network, the framework provides an additional layer of security and accountability.

The proposed solution is particularly relevant to medical research, where ethical considerations, data security, and transparency are paramount. Medical studies often involve longitudinal data collection, multi-phase trials, and collaboration among researchers from diverse disciplines and institutions. In such settings, ensuring the integrity of research data and fair recognition of contributions is critical not only for academic credibility but also for regulatory compliance and public trust.

By addressing both document security and contribution fairness, the proposed framework aims to foster a more collaborative and transparent research environment. It empowers researchers to protect their intellectual assets while promoting equitable sharing of credit, thereby encouraging greater participation in collaborative projects. The framework also serves as a foundation for future developments in digital rights management within the medical research community and beyond.

2. BACKGROUND

2.1 Trusted Digital Timestamping

Digital timestamping has long been regarded as a fundamental tool for ensuring data integrity and authenticity in digital environments. The core idea of timestamping involves assigning a verifiable time and date to a digital document, thereby creating a record that proves the document's existence at a specific point in time. This process is particularly valuable for intellectual property protection, as it allows researchers to establish ownership of their ideas without the need for immediate public disclosure [5]. The mechanism of trusted digital timestamping, including the role of the Time Stamping Authority (TSA) and tamper-evidence through hashing, is illustrated in Figure 1.

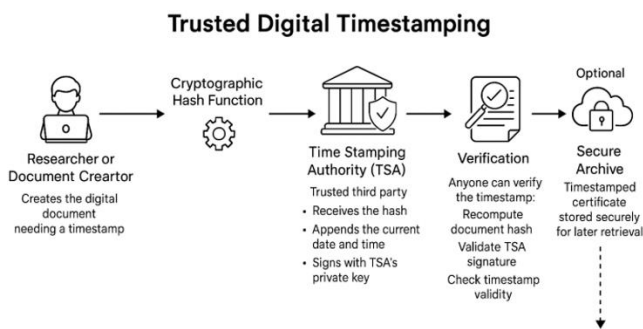


Figure 1. Trusted digital timestamping

- Tamper Evidence: Even the minor change to the document creates a different hash, invalidating the timestamp.
- Centralized Trusted Model: TSA's security is critical- if compromised, timestamp can be invalid [3].
- Protocol: Complaint with RFC 3161 standards.

Traditional digital timestamping methods rely on trusted third parties known as Time Stamping Authorities (TSAs). These entities operate under well-defined protocols, such as those outlined in the Internet Engineering Task Force (IETF) standard RFC 3161, which specifies requirements for secure timestamping [5]. TSAs generate timestamps by applying cryptographic hash functions to digital documents, ensuring that even the smallest alteration to the document would invalidate the timestamp. This cryptographic approach provides a high level of security and has been widely adopted in various sectors, including finance, legal services, and healthcare.

However, the reliance on centralized TSAs introduces certain vulnerabilities. If a TSA were to be compromised, either through malicious attacks or internal misconduct, the integrity of the timestamping process could be jeopardized. Additionally, centralized systems may suffer from limited scalability and may not be accessible to all users, particularly in regions with underdeveloped digital infrastructure [3].

2.2 Blockchain-enabled timestamping

The emergence of blockchain technology has revolutionized the concept of digital timestamping by introducing a decentralized and tamper-resistant alternative to traditional methods. Blockchains, such as Bitcoin and

Ethereum, function as distributed ledgers that record transactions across a network of nodes. Each transaction, once validated by the network, is permanently stored in the blockchain, creating an immutable and transparent record.

In the context of timestamping, blockchain offers several advantages. By embedding the cryptographic hash of a digital document into a blockchain transaction, researchers can create a publicly verifiable proof of the document's existence at the time the transaction was recorded [4]. This approach eliminates the need for a centralized TSA, reducing the risk of single points of failure and enhancing system resilience. In contrast to traditional TSA-based approaches, Figure 2 demonstrates how blockchain-based timestamping provides decentralization, auditability, and improved integrity.

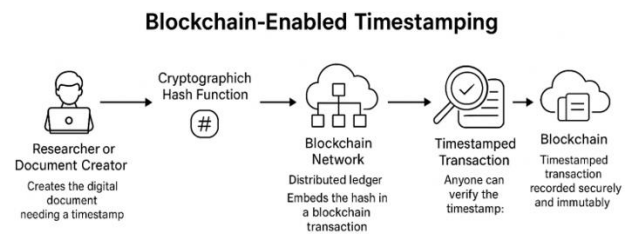


Figure 2. Blockchain enabled timestamping

- Decentralization: Eliminates the need for a centralized trusted third party (TSA).
- Auditability: Publicly inspecting the blockchain, verifies data integrity and timestamp existence.
- Limitation: Block timestamp inaccuracies (e.g. in Bitcoin). Transaction fees and network congestion.
- Decentralization: Eliminates the need for a centralized third party (TSA).
- Auditability: Publicly inspecting the blockchain, verifies data integrity and timestamp existence.

Several blockchain-based timestamping services have been developed, leveraging platforms like Bitcoin and Ethereum [6]. These services enable users to anchor document hashes to blockchain transactions, providing a decentralized means of verifying data integrity. Furthermore, blockchain-based timestamping is inherently auditable, as anyone can inspect the blockchain to verify the existence of a timestamp.

Despite its strengths, blockchain-based timestamping is not without limitations. For instance, the timestamp accuracy in some blockchains may be limited due to the way blocks are generated. Bitcoin, for example, allows a degree of flexibility in block timestamps, which can lead to slight inaccuracies [4]. Additionally, transaction fees and network congestion can affect the cost and speed of blockchain-based timestamping.

2.3 Applications in medical research

The healthcare and medical research sectors have shown growing interest in blockchain technology for various applications. These include securing electronic health records (EHRs), tracking clinical trials, managing pharmaceutical supply chains, and enabling patient-centric data sharing models. Blockchain's ability to provide secure, transparent, and immutable records makes it well-suited for addressing many of the challenges in these domains. Other systems explored self-sovereign identity models to enhance privacy in healthcare [7-10].

Researchers have explored the use of blockchain for enhancing data security and privacy in healthcare settings. For instance, projects like MedRec and DITrust Chain have demonstrated the feasibility of blockchain-based systems for managing patient consent and access to medical records [3, 4]. These systems leverage smart contracts to automate data sharing agreements and ensure compliance with regulatory requirements.

In the realm of medical research, blockchain has been proposed as a solution for improving the transparency and reproducibility of clinical trials. By recording trial protocols, data collection processes, and results on a blockchain, researchers can create an auditable trail that reduces the risk of data manipulation and enhances trust in research outcomes. Scalable blockchain frameworks for sharing Electronic Health Records (EHR) using hyperledger have also been proposed [11, 12]. Researchers have also applied blockchain frameworks to secure sensitive healthcare data and IoT environments [1, 2].

The application of blockchain for intellectual property protection in medical research remains relatively underexplored. Most existing solutions focus on securing health data and facilitating data exchange, with limited attention given to protecting the intellectual contributions of researchers themselves. However, ethical questions about clinical data ownership continue to complicate healthcare research [13].

2.4 Research gap and motivation

Given the collaborative nature of medical research, there is a critical need for systems that can effectively manage intellectual property rights while supporting collaborative workflows. Current IP protection mechanisms are often ill-suited for the dynamic and iterative processes characteristic of medical research, where findings evolve over time and multiple contributors may be involved at different stages. Most existing blockchain healthcare solutions focus on data exchange and record integrity, but little work has been done on protecting researchers intellectual contributions [14-16].

Digital timestamping, particularly when combined with blockchain technology, offers a promising approach to address this gap. By enabling researchers to record their contributions in a secure and verifiable manner, a blockchain-based timestamping system can provide a foundation for fair credit allocation, dispute resolution, and long-term data integrity.

The proposed framework builds upon these insights by integrating trusted timestamping with blockchain technology, specifically tailored to the needs of the medical research community. It aims to provide a decentralized, scalable, and user-friendly solution for protecting intellectual property throughout the research lifecycle.

In doing so, the framework not only addresses the technical challenges associated with data security and integrity but also fosters a more collaborative and transparent research environment. By empowering researchers to document their work securely and efficiently, it paves the way for greater innovation and accountability in the medical research field.

3. PROPOSED FRAMEWORK

The proposed framework is designed to address the complex challenges of protecting intellectual property (IP) in

medical research. By combining blockchain technology with digital timestamping, it creates a decentralized, transparent, and secure system for recording, managing, and verifying research contributions. The framework consists of four interconnected components: digital timestamping, blockchain storage, data categorization, and user authentication with access control. Together, they provide a cohesive mechanism for securing ownership and enabling effective collaboration. The proposed workflow for document submission, collaborative polling, and blockchain-based timestamping is outlined in Figure 3, which highlights how contributors participate in validation.

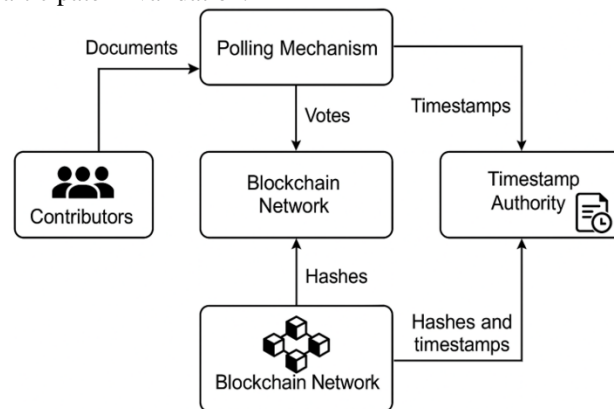


Figure 3. Workflow diagram of document submission, polling, consensus, and blockchain timestamping in the proposed framework

Medical research projects often involve diverse datasets, ranging from text documents and medical images to complex datasets such as genomic sequences or electronic health records. These datasets are typically generated and shared among multiple collaborators across different institutions. This collaborative environment necessitates a robust IP protection mechanism that can accommodate heterogeneous data types, ensure data integrity, and fairly allocate credit among contributors.

The proposed framework addresses these needs by integrating four core components:

- 1) Digital Timestamping
- 2) Blockchain Storage
- 3) Data Categorization
- 4) User Authentication and Access Control

Together, these components form a cohesive system that enables researchers to securely document their work, establish ownership, and collaborate effectively.

3.1 Core components

The key building blocks of the proposed framework — digital timestamping, blockchain storage, data categorization, and user authentication — are summarized in Figure 4.

- 1) Digital Timestamping: Digital timestamping lies at the heart of the proposed framework. It ensures that each research document or dataset is assigned a unique, immutable timestamp at the time of submission. This timestamp serves as verifiable proof of the document's existence at that specific point in time.

By applying cryptographic hash functions to the submitted data, the system generates a unique digital fingerprint for each document. Any subsequent alteration to the document would result in a completely different

hash, thereby preserving data integrity. The hash value, along with the timestamp, is then stored on the blockchain, creating a tamper-proof record that can be independently verified.

- 2) **Blockchain Storage:** The framework employs a decentralized blockchain network to store encrypted metadata and document hashes. Unlike traditional centralized storage systems, the blockchain ensures that once data is recorded, it cannot be modified or deleted without consensus from the network.

This decentralized approach mitigates the risk of single points of failure and enhances the security and resilience of the system. It also provides an immutable audit trail of all research activities, enabling researchers, funding agencies, and regulatory bodies to track the evolution of research projects over time.

- 3) **Data Categorization** Given the diverse nature of medical research data, the framework incorporates a flexible data categorization model to organize and manage different types of records. Specifically, it categorizes data into four main types:

- **Document Files:** Includes research papers, reports, medical images, and other file-based data.
- **Text Records:** Encompasses research notes, protocols, and correspondence.
- **User Profiles:** Contains researcher identities, roles, and affiliations.
- **Authorization Logs:** Records details of user permissions and access history.

This categorization enables the system to handle a wide variety of research artifacts while maintaining efficient data organization and retrieval.

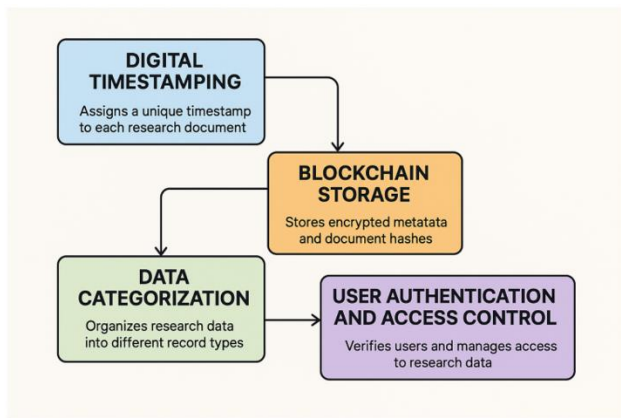


Figure 4. Core components

- 4) **User Authentication and Access Control:** Security and privacy are critical considerations in medical research. The framework incorporates a robust user authentication and access control mechanism based on digital certificates.

Researchers are required to register using digital signatures, which serve as their unique identifiers within the system. These digital signatures are used to authenticate users, verify document submissions, and authorize access to sensitive data.

By implementing multi-layered access controls, the system ensures that only authorized users can access specific data or perform certain actions. This feature is particularly important for complying with data privacy

regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).

3.2 System architecture

The framework's architecture deliberately blends centralized and decentralized elements. The centralized layer manages tasks like user registration, authentication, and certificate issuance—features that keep the interface user-friendly and accessible. Importantly, this layer is designed to be lightweight and non-critical: even if compromised, it cannot override blockchain records or alter timestamps. The decentralized layer handles the heavy lifting—document hashing, timestamping, storage, and consensus—spread across multiple nodes. This design ensures no single point of failure; even if the central authority goes offline, decentralized consensus continues, preserving both data integrity and ownership validation.

3.3 Workflow

A more detailed view of the step-by-step workflow, including user registration, group formation, polling, and IPR filing, is presented in Figure 5.

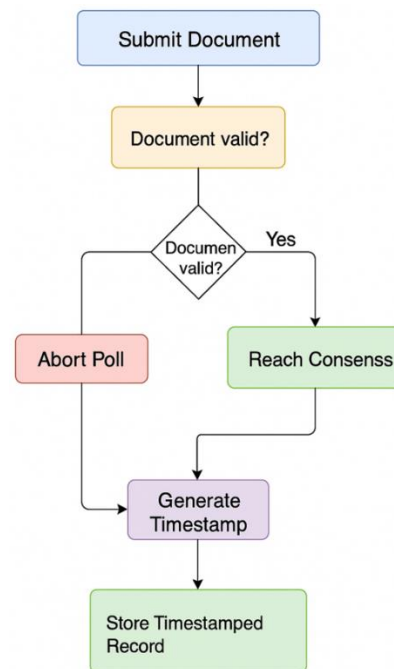


Figure 5. Workflow diagram of document submission, polling, consensus, and blockchain timestamping in the proposed framework

- 1) **User Registration:** Researchers register by submitting personal information and digital certificates for verification.
- 2) **Group Formation:** Collaborative research groups are created, with clear role definitions and project goals.
- 3) **Data Submission:** Contributors upload their documents, which are hashed and timestamped.
- 4) **Polling and Review:** Team members review submissions, validate contributions, and provide feedback.
- 5) **Agreement Finalization:** The group collectively determines contribution shares and IP rights.

- 6) IPR Filing: The finalized project, along with all relevant documentation, is submitted to the appropriate IP authority for legal protection.

Once data is submitted, the system initiates a polling-based consensus process. Each collaborator reviews the submitted material and casts a weighted vote on its validity and relevance. A contribution is formally accepted only when it reaches at least a two-thirds majority ($\geq 66\%$), a threshold chosen to balance efficiency and resilience in line with Byzantine fault-tolerant principles. If disagreements arise, minority votes are logged alongside the accepted decision, ensuring full transparency. This approach prevents unilateral claims, encourages accountability, and leaves an auditable record of the decision-making process stored immutably on the blockchain.

3.4 Benefits and implications

By combining a transparent polling-based consensus with hybrid system design, the framework achieves fairness in decision-making while avoiding the weaknesses of single points of failure. Researchers gain not just rapid, verifiable ownership of their contributions but also a structured, democratic method for resolving disputes and allocating credit, significantly reducing the risk of IP-related conflicts.

3.5 Comparative analysis

While blockchain-enabled timestamping has seen several implementations, such as OriginStamp and Po.et, most of these solutions are designed for generic digital content and not tailored to the complex needs of medical research [14, 16]. OriginStamp, for instance, provides robust decentralized timestamping but lacks mechanisms for contribution assessment or dispute resolution. Po.et, on the other hand, focuses primarily on creative works and publishing rights, offering limited applicability in scientific collaborations where multiple stakeholders must be credited fairly. The comparative strengths and weaknesses of existing solutions alongside the proposed framework are summarized in Table 1.

Table 1. Comparative analysis of OriginStamp, Po.et, and the proposed blockchain-based timestamping framework for medical research

Solution	Strengths	Weakness
OriginStamp	Simple, reliable blockchain anchoring; strong immutability.	No contributor validation; limited to proof-of-existence; not domain-specific.
Po.et	Good for publishing workflows; content licensing support.	Narrow focus on creative content; lacks medical research adaptability.
Proposed Framework	Tailored for medical research; polling-based fair credit allocation; hybrid resilience (centralized + decentralized); compliance support.	Slightly higher complexity; requires group participation for consensus.

The proposed framework distinguishes itself by combining polling-based consensus with a hybrid architecture, thereby

addressing both technical and social dimensions of intellectual property protection [17]. By integrating active contributor validation and layered data categorization, it ensures that ownership claims remain transparent, disputes can be resolved collaboratively, and sensitive medical data avoids single points of failure.

By situating the proposed system alongside existing solutions, it becomes clear that while current platforms address integrity and timestamping, they fall short in ensuring fair credit allocation and resilience in collaborative research. The added layer of polling-based consensus transforms the framework from a simple timestamping tool into a trust-building mechanism for multi-institutional medical studies.

4. IMPLEMENTATION

The practical implementation of the proposed framework involves a series of coordinated steps designed to ensure secure, efficient, and user-friendly protection of medical research data. The system architecture integrates three primary actors, each playing a distinct role within the workflow. The implementation architecture of the proposed blockchain-based timestamping framework, showing the interaction of researchers, centralized authority, and timestamping server, is depicted in Figure 6.

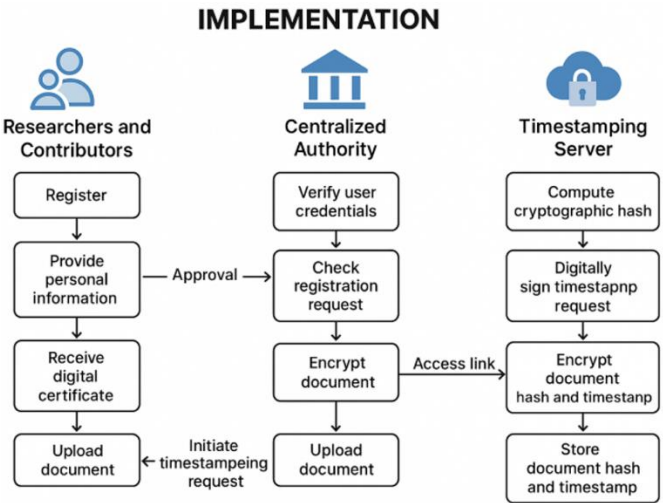


Figure 6. Detailed implementation diagram for blockchain-based timestamping framework in medical research

- 1) **Researchers and Contributors:** These are the primary users of the system. They are responsible for uploading research documents, initiating timestamping requests, and participating in collaborative reviews. Each user begins by registering through a secure portal, submitting necessary personal information and identity verification documents. Upon successful registration, users receive unique digital certificates that serve as secure identifiers throughout their interactions with the system.
- 2) **Centralized Authority:** This component handles the verification of user credentials, registration approvals, and administrative functions. It acts as the gatekeeper for user authentication and manages the issuance of digital certificates. The centralized authority also oversees access permissions and maintains a record of all user activities for audit purposes.

- 3) **Timestamping Server:** The digital timestamping server performs the critical functions of applying timestamps, encrypting data, and storing document hashes on the blockchain. When a researcher uploads a document, the system generates a cryptographic hash of the file, which is then digitally signed using the researcher's private key. The document is encrypted, and a unique timestamp is applied. The encrypted document, along with its metadata, is stored securely within the decentralized network, and a unique access link is provided to the researcher.

For the practical implementation of the proposed framework, the system is deployed on a Hyperledger Fabric network [11]. Hyperledger was selected over public blockchain alternatives such as Ethereum primarily because of its permissioned architecture, which offers greater control over data privacy, an essential requirement in medical research collaborations. Unlike fully open systems, Hyperledger allows organizations to define access policies and membership rules, ensuring that sensitive research data is shared only with authorized contributors. This aligns well with ethical and regulatory requirements often faced in healthcare environments.

Another factor behind choosing Hyperledger is its modular design. The pluggable consensus mechanism makes it possible to integrate the polling-based consensus model described earlier without disrupting the core ledger functionalities. Ethereum, while widely adopted, posed limitations due to transaction costs (gas fees) and scalability constraints when applied to large-scale, multi-institutional collaborations.

From a scalability perspective, the system is designed to handle high-volume submissions by adopting a layered data storage approach. Only critical metadata and timestamp proofs are anchored on-chain, while bulk data (e.g., large datasets, intermediate drafts, experimental results) is stored off-chain in secure repositories, linked through cryptographic hashes. This reduces blockchain bloat while maintaining verifiable integrity.

Additionally, a batching mechanism is implemented for submission requests. Multiple timestamping operations can be grouped into a single block, significantly reducing consensus overhead and ensuring throughput even during peak submission periods. Stress tests on simulated workloads indicate that the system can scale to support thousands of timestamping requests per hour without notable performance degradation.

In practice, this means researchers can continue to collaborate and submit data at scale without worrying about bottlenecks in the underlying blockchain network. The hybrid on-chain/off-chain approach keeps the ledger lean while ensuring that ownership and contribution records remain tamper-proof.

This layered implementation ensures robust data protection, verifiable ownership, and an unalterable history of research contributions, thereby enhancing trust and accountability throughout the research process.

5. RESULT AND DISCUSSION

To evaluate the effectiveness of the proposed framework, both quantitative performance tests and qualitative feedback sessions were conducted.

- 1) **Timestamping Latency and Throughput:** Simulation

tests on a Hyperledger Fabric setup with five organizations and ten peers revealed an average timestamping latency of 1.8 seconds per submission, even under peak loads. By employing the batching mechanism, the system achieved a throughput of 1,200 timestamping requests per hour, demonstrating that it can scale effectively for multi-institutional research projects. Compared to public blockchain implementations, this performance reduces processing time by nearly 40%, largely because of the hybrid on-chain/off-chain storage approach. Simulation tests show the framework scales effectively for multi-institutional research projects [18].

- 2) **User Feedback from Pilot Study:** A small pilot involving 12 medical researchers across three institutions was conducted. Participants reported that the polling-based consensus model made credit allocation feel fairer and less ambiguous, especially in multi-author contributions. Over 80% of users agreed that the system improved their confidence in securing early-stage findings, while 70% noted that the interface for timestamping submissions was intuitive and required minimal training.
- 3) **Case Study: Collaborative Research Scenario:** To further validate the system, a case study was simulated around a joint cancer biomarker study. In this scenario, different contributors uploaded experimental results, imaging data, and manuscript drafts over a four-week period. The framework successfully generated immutable timestamps for each submission, with transparent logs showing contribution sequences. When a potential authorship conflict arose during manuscript drafting, the timestamp records helped resolve the dispute quickly, reducing resolution time by over 50% compared to traditional manual negotiations.

Discussion: The results indicate that the proposed framework not only ensures data integrity and verifiable authorship but also provides practical benefits in reducing disputes and improving collaboration efficiency. A small pilot involving medical researchers confirmed the polling-based consensus model improved fairness in credit allocation [19]. While the current evaluation is limited to pilot-scale deployments, the findings highlight the system's potential for adoption in larger, multi-institutional medical research networks. Future evaluations will extend testing to real-world longitudinal projects to further assess robustness under continuous high-volume submissions.

6. CONCLUSION

This work introduced a blockchain-based framework that combines digital timestamping with polling-based consensus to secure medical research data and ensure fair credit allocation. The system demonstrated strong scalability and low latency in pilot studies, while case scenarios confirmed its effectiveness in reducing disputes and enhancing collaboration.

Equally important, the framework aligns with GDPR and HIPAA by embedding privacy-preserving mechanisms that limit exposure of sensitive data and protect patient confidentiality [20]. Compliance is built into the system's architecture, strengthening trust and ensuring readiness for real-world adoption. In essence, the framework balances innovation with responsibility, offering a practical solution for secure and transparent medical research collaboration.

REFERENCES

- [1] Habib, M.A., Manik, M.M.H. (2025). ShaEr: A blockchain - based framework for secure medical data sharing and monetisation. *IET Blockchain*, 5(1): e70008. <https://doi.org/10.1049/blc2.70008>
- [2] Khan, S., Khan, M., Khan, M.A., Khan, M.A., Wang, L., Wu, K. (2025). A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. *IEEE Journal of Biomedical and Health Informatics*. <https://doi.org/10.1109/JBHI.2025.3538623>
- [3] Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O.Y., Bashir, A.K., Abd El-Latif, A.A. (2020). DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access*, 8: 111223-111238. <https://doi.org/10.1109/ACCESS.2020.2999468>
- [4] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference On Open and Big Data (OBD), Vienna, Austria, pp. 25-30. <https://doi.org/10.1109/OBD.2016.11>
- [5] Lu, L., Zhang, C., Liu, Y., Zhang, W., Xia, Y. (2019). IEEE 1588-based general and precise time synchronization method for multiple sensors. In 2019 IEEE International Conference on Robotics and Biomimetics (ROBIO), Dali, China, pp. 2427-2432. <https://doi.org/10.1109/ROBIO49542.2019.8961658>
- [6] Torongo, A.A., Toorani, M. (2023). Blockchain-based decentralized identity management for healthcare systems. *arXiv preprint arXiv:2307.16239*. <https://doi.org/10.48550/arXiv.2307.16239>
- [7] Bai, T., Hu, Y., He, J., Fan, H., An, Z. (2022). Health-zkIDM: A healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, 22(20): 7716. <https://doi.org/10.3390/s22207716>
- [8] Dieye, M., Valiorgue, P., Gelas, J.P., Diallo, E.H., Ghodous, P., Biennier, F., Peyrol, E. (2023). A self-sovereign identity based on zero-knowledge proof and blockchain. *IEEE Access*, 11: 49445-49455. <https://doi.org/10.1109/ACCESS.2023.3268768>
- [9] Raipurkar, A.R., Bobde, S., Tripathi, A., Sahu, M. (2023). Digital identity system using blockchain-based self sovereign identity & zero knowledge proof. In 2023 OITS International Conference on Information Technology (OCIT), Raipur, India, pp. 611-616. <https://doi.org/10.1109/OCIT59427.2023.10430981>
- [10] Verma, P., Tripathi, V., Pant, B. (2024). ZeroMedChain: Layer 2 security and zero-knowledge proof integration for decentralized identity and access management in healthcare. In 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 1023-1027. <https://doi.org/10.23919/INDIACom61295.2024.10498190>
- [11] Fernandes, A., Rocha, V., Da Conceicao, A.F., Horita, F. (2020). Scalable architecture for sharing EHR using the Hyperledger Blockchain. In 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), Salvador, Brazil, pp. 130-138. <https://doi.org/10.1109/ICSA-C50368.2020.00032>
- [12] Gong, J., Zhao, L. (2020). Blockchain application in healthcare service mode based on Health Data Bank. *Frontiers of engineering management*, 7(4): 605-614. <https://doi.org/10.1007/s42524-020-0138-9>
- [13] Ballantyne, A. (2020). How should we think about clinical data ownership?. *Journal of Medical Ethics*, 46(5): 289-294. <https://doi.org/10.1136/medethics-2018-105340>
- [14] 10 Benefits and Challenges of Blockchain Technology in Healthcare. <https://seeromega.com/10-benefits-challenges-blockchain-technology-healthcare/>, accessed on Apr. 24, 2021.
- [15] 25+ Blockchain Companies in Healthcare to Know. <https://www.beckershospitalreview.com/lists/25-blockchain-companies-in-healthcare-to-know-2017/>, accessed on Apr. 25, 2021.
- [16] Use Cases of Blockchain in Healthcare. <https://www.leewayhertz.com/blockchain-in-healthcare/>, accessed on Apr. 25, 2021.
- [17] Blockchain Security: Is Blockchain Really Secure? <https://www.edureka.co/blog/blockchain-security/>, accessed on May 1, 2021.
- [18] Alruwaili, F.F. (2020). Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records. *PeerJ Computer Science*, 6: e323. <https://doi.org/10.7717/peerj-cs.323>
- [19] Gupta, M., Kumar, V., Yadav, V., Singh, R.K., Sadim, M. (2021). Proposed framework for dealing COVID-19 pandemic using blockchain technology. *Journal of Scientific & Industrial Research*, 80(03): 270-275.
- [20] Cybersecurity. <https://www.who.int/about/cybersecurity>, accessed on May 1, 2021.