BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

ORIGINAL RESEARCH

A DeSci-Driven Blockchain Framework for AI-Augmented Healthcare Research

Garima Singh, PhD[1,2], Mohd. Haroon, PhD[3], Nudrat Fatima, PhD[4], Afsaruddin, PhD[5], Tameem Ahmad, PhD[6], Mohammad Husain, PhD[7] and Mahfuzul Huda, PhD[8]

[1]Research Scholar, Department of Computer Science & Engineering, Integral University, Lucknow, India; [2]Assistant Professor, Department of CSIT, Krishna Institute of Engineering and Technology, Delhi-NCR, Ghaziabad, India; [3]Professor, Department of Computer Science & Engineering, Integral University, Lucknow, India; [4]Associate Professor, Department of Computer Science & Engineering, Integral University, Lucknow, India; [5]Assistant Professor, Department of CEA, GLA University, Mathura, India; [6]Assistant Professor, Department of Computer Engineering, Aligarh Muslim University, Aligarh, India; [7]Professor, Department of Computer Science and Engineering, School of Management Sciences, Lucknow, India; [8]Assistant Professor, Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

DOI: https://doi.org/10.30953/bhty.v9.507

Corresponding Author: Garima Singh, Email: garima.singh@kiet.edu

Keywords: Artificial intelligence, blockchain in healthcare, decentralized governance, decentralized science (DeSCi), electronic health records (EHR), hybrid consensus mechanism, privacy-preserving data sharing, risk prediction, zero-knowledge proof (ZKP)

Abstract

Background: The accelerated digital revolution in healthcare has greatly enhanced data management with electronic health records. Nonetheless, challenging issues of centralized control, privacy breaches, absence of patient ownership of their data, and inability to support decentralized scientific collaboration remain barriers to scalable healthcare research ecosystems. Recent developments in decentralized science (DeSci) create a paradigm shift, using blockchain, cryptographic primitives, and decentralized governance to facilitate transparent, trust-minimized, and collaborative biomedical research. This article provides a DeSci-friendly lightweight blockchain architecture that is used to support privacy-preserving and incentive-sensitive decentralized healthcare research infrastructure.

Methods: The framework combines a permissioned blockchain with a lightweight hybrid consensus protocol, off-chain storage, and zero-knowledge proof-based authentication to permit secure and privacy-preserving access to data without revealing identity. Also, a tokenomics-based governance layer is proposed to support decentralized engagement, transparent policy implementation, and incentive-based research participation. The suggested system is tested in simulation with the following different network conditions and the key performance metrics such as latency, throughput, and computational cost.

Results: Experiments prove that the suggested framework offers the following advantages:

- lower latency
- greater throughput
- enhanced computational efficiency

when compared to the current blockchain-based healthcare systems such as medical records, Fast Healthcare Interoperability Resources, and HealthChain. In addition, the framework goes past traditional data management by allowing a DeSci-oriented research life cycle, such as decentralized data contribution, validation, and provenance tracking.

Conclusions: The proposed framework will help build scalable, secure, and patient-centered decentralized healthcare research ecosystems. Furthermore, the framework bridges the gap between blockchain-based healthcare systems and DeSci-driven research ecosystems.

Plain Language Summary

Healthcare data are stored in centralized systems that carry risks of privacy breaches and limit patient control. The authors propose a blockchain-based framework that allows healthcare data to be stored and shared securely in a decentralized way. Patient data are stored off-chain. Only cryptographic hash references are stored on the blockchain, ensuring sensitive information is never directly exposed. Researchers and clinicians can request access by providing a zero-knowledge proof—a mathematical verification that confirms their authorization without revealing their identity or credentials. A governance layer based on decentralized science is a transparent, token-incentivized system. Simulation results show that the proposed framework achieves several positive outcomes, including the following.

- lower transaction latency,
- higher throughput, and,
- reduced computational cost compared to existing blockchain-based healthcare systems

This approach has the potential to support secure, patient-centered, and collaborative healthcare research ecosystems.

Key Takaways

- A lightweight permissioned blockchain integrating PBFT–PoA consensus, off-chain storage, and ZKP-based authentication enables low-latency, privacy-preserving healthcare data access while ensuring integrity and tamper detection.
- A DAO-based governance and tokenomics layer supports transparent stakeholder participation, decentralized decision-making, and research incentives, with privacy-by-design principles aligned with HIPAA, DISHA, and GDPR.
- An AI-based readmission-risk model extends the framework toward privacy-preserving clinical decision support, while blockchain-based provenance enables controlled data contribution, verification, and lifecycle traceability.

Submitted: April 14, 2026, Accepted: August 11, 2026, Published: August 31, 2026

The high digitization of the healthcare system has resulted in the widespread use of electronic health records (EHRs) that enhance clinical processes and the availability of information.[1] Nonetheless, centralized designs still pose significant problems, such as privacy threats, interoperability, patient control, and susceptibility to cyberattacks.[2] These constraints limit the scalability and reliability of healthcare data management systems. The next alternative provided by blockchain technology is decentralized and immutable, with the option to securely and transparently share data without the help of centralized authorities. Current networks such as medical records (MedRec), fast healthcare interoperability resources fast healthcare interoperability resources (FHIRChain) and HealthChain enhance the integrity of data and control access but lack scalability because of computationally intensive consensus mechanisms.[3] Simultaneously, decentralized science (DeSci) has become a paradigm shift that uses blockchain, decentralized governance, and token-based incentives to facilitate transparent and cooperative research ecosystems. However, current healthcare blockchain systems fail to support privacy-preserving authentication, efficient scalability, and decentralized research participation within a unified framework.[4]

To address these limitations, the authors propose a DeSci-driven lightweight hybrid blockchain framework integrating permissioned blockchain, hybrid consensus, off-chain storage, and zero-knowledge proof (ZKP)-based authentication.[5] Furthermore, decentralized autonomous decentralized autonomous organization (DAO)-based governance and tokenomics mechanisms are incorporated to enable decentralized participation and incentive-driven collaboration.

The main contributions include:

a. DeSci-driven lightweight blockchain architecture for decentralized healthcare research,
b. ZKP-based privacy-preserving authentication mechanism
c. Integration of governance and tokenomics for decentralized participation, and,
d. Performance evaluation demonstrating improved latency, throughput, and efficiency.

While existing blockchain frameworks such as MedRec (2016), FHIRChain (2018), and HealthChain represent foundational contributions to decentralized healthcare, they were developed prior to the emergence of DeSci as a formal paradigm. Recent work (2022–2025) explored individual components such as ZKP-based authentication or token-based incentives in isolation. The novelty of the proposed framework lies in the unified integration of a lightweight practical Byzantine fault tolerance—proof of authority (PBFT–PoA) consensus, ZKP-based privacy-preserving authentication, off-chain storage, and DAO-based DeSci governance within a single coherent architecture designed specifically for decentralized healthcare research infrastructure. No existing system combines all four components in a lightweight, permissioned blockchain setting aligned with DeSci principles.

Statement of the Problem

Although blockchain technologies in healthcare are becoming more common, the available solutions lack a single framework that ensures scalability and privacy protection, as well as allowing researchers to participate in the research process in a decentralized manner.[6] This is a constraint due to trade-offs in design and architectural constraints within existing systems.

Firstly, there are the issues of scalability and computational efficiency, which are crucial.[7] The majority of blockchain-based healthcare systems are based on resource-consuming consensus algorithms, which have further led to a high latency, communication overhead, and decreased throughput. Such limitations limit their use in a large-scale healthcare network, especially where there are limited computing capabilities.[8]

Secondly, the privacy-preserving access control is not properly addressed. The current systems mainly make use of identity-based or role-based authentication systems that obligate clear revelation of user credentials. These methods cannot be adapted to the healthcare sector that is sensitive, and any exposure to identity-related information to the minimum can cause privacy invasion. The lack of more sophisticated cryptographic methods, such as ZKP, also restricts the possibility of supporting secure and minimally trusted data access.

Thirdly, the existing blockchain-based healthcare solutions are not aligned with the principles of DeSci. While DeSci promotes patient-centric data ownership, decentralized governance, and incentive-driven participation,

existing frameworks do not support trustless collaboration among patients, researchers, and healthcare providers. Specifically, it lacks an integrated infrastructure that would allow privacy-preserving involvement in decentralized clinical research and data sovereignty and auditability.[9] All of these constraints point to a significant research gap: there is a lack of a lightweight, privacy-preserving, and DeSci-compatible healthcare data governance framework to enable both secure data management and decentralized scientific collaboration.[10] Addressing this gap requires a coherent system that unifies efficient consensus mechanisms, cryptographic access control, and decentralized governance models, which is the central motivation for the present work.[11]

Proposed Methodology

The System Model

A lightweight hybrid blockchain architecture is proposed for secure, scalable, and privacy-sensitive healthcare data management within a DeSci ecosystem.[12]

The system state is formally represented as:

$$\mathcal{S} = (\mathrm{E}, \mathrm{B}, \mathcal{D}, \mathcal{C}, \mathcal{G}, \mathcal{T})$$

where E denotes the set of participating entities, B the permissioned blockchain layer, D the off-chain data store, C the access control policy space, G the DAO governance layer, and T the tokenomics layer.

Each transaction record is represented as:

$$T = (H(D), \pi, C, \tau, \sigma)$$

comprising a data hash H(D), a zero-knowledge proof π, the associated access policy C, a timestamp τ, and a validator signature σ. Together, the permissioned blockchain architecture, lightweight hybrid consensus mechanism, off-chain storage, and ZKP-based access control provide decentralized data governance and trustless stakeholder interaction.

System Architecture

The system consists of patient, provider, and researcher nodes interacting via a permissioned blockchain.[13] Data are stored off-chain, while hashes are stored on-chain. Smart contracts enforce access control, and DAO-based governance enables decentralized decision-making.

Key Entities in the Proposed System

a. The Patient Node is the primary owner of healthcare data and defines access privileges in a patient-centric system.
b. Healthcare Provider Node (Hospital/Lab): Creates, updates, and verifies patient MedRec.[14]
c. Research Node: Authorized researchers doing decentralized clinical research and data analysis.
d. Permissioned Blockchain Network: Records transactions, access logs, and data hash records permanently.
e. To reduce storage overhead, large medical data (e.g. imaging, reports) are stored off-chain using the interplanetary file system (IPFS)/Cloud.
f. Smart Contract Layer: Implements access control, authentication, and audit trails.

The DeSci governance layer (conceptual DAO integration): Allows decentralized policy decisions on data access, research involvement, and data-sharing agreements.[15] The framework separates data storage and verification and facilitates decentralized collaboration with several stakeholders in a trust-reduced environment.

Figure 1 illustrates the proposed DeSci-enabled lightweight hybrid blockchain architecture, integrating permissioned blockchain, hybrid consensus, off-chain storage, ZKP-based authentication, and DAO-based governance for secure and decentralized healthcare data management.

Hybrid Consensus Mechanism

The architecture uses a permissioned blockchain and a lightweight hybrid consensus mechanism that combines PBFT and PoA.[16] Healthcare-appropriate latency, computational cost, and throughput are the goals of this hybrid system.

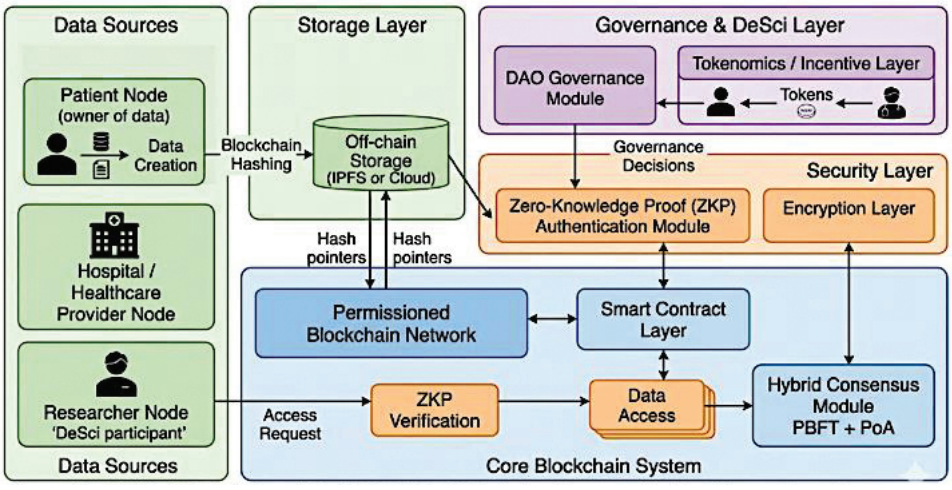

Fig. 1. DeSci-enabled lightweight hybrid blockchain architecture for healthcare data governance. DeSci: decentralized science; IPFS: interplanetary file system; PBFT: practical Byzantine fault tolerance; PoA: proof-of-authority; ZKP: zero-knowledge proof.

A hybrid PBFT–PoA consensus is adopted as:

$$C(n) = O(n^2)$$

The main features are:

a. Limited network access for approved parties.
b. Lower consensus overhead compared to public blockchains.
c. Improved transaction authentication speed and scalability.
d. The consensus process communication complexity is defined as:
e. $C(n) = O(n^2)f)n$ = number of network nodes with participation.

The hybrid consensus technique limits validator participation through a permissioned framework, reducing practical communication overhead compared to PBFT. This eases communication, resulting in better scalability and reduced latency in the proposed system.

Data Integrity Model

Cryptographic hashing is used to process patient data to promote data integrity[17]:

$$H(D) = SHA\text{–}256(D)$$
$$H(D) \neq H(D') \Rightarrow D \neq D'$$
$$Pr[collision] \approx 0$$

Note that $H(D) = SHA\text{–}256(D)$ where D is patient data and H(D) is the hash of patient data in the blockchain. Actual medical information is stored off-chain, and only hash and metadata remain on-chain so as to assure integrity without exposing sensitive data.

ZKP-Based Access Control

The framework proposed uses authentication by ZKP in order to allow the process of privacy-sensitive access control without disclosing the identity of the user or other sensitive credentials.[18] Users authenticate themselves by cryptographic proofs as opposed to the conventional role-based mechanisms.

The verification process is defined as:

$$Verify(\pi, C) = 1$$
$$Pr[V(\pi) = 1] = 1$$
$$Pr[\mathcal{A} \text{ succeeds}] \leq \varepsilon$$
$$Leakage(\pi) = 0$$

where π represents the ZKP and C denotes the access control policy.

Under the proposed system, the user creates a cryptographic proof off-chain (e.g. zero knowledge succinct non-interactive argument of knowledge (zk-SNARKs) and provides it to the smart contract to be verified. After successful validation, access to encrypted data is provided without revealing underlying credentials. The methodology guarantees completeness, soundness, and zero-knowledge properties, making it possible to have secure, trust-minimized, and privacy-preserving authentication in the decentralized healthcare model.

Governance and Tokenomics

The suggested structure incorporates the principles of DeSci with a layer of governance based on a DAO and allows making transparent and decentralized decisions regarding access to healthcare data and participation in research.[19] This type of governance promotes:

a. Patient-centric data ownership and permission control
b. Transparent and auditable data access policies
c. Decentralized participation of researchers in clinical studies.

A lightweight tokenomics model is incorporated to incentivize participation within the healthcare data ecosystem. Patients, researchers, and validators are rewarded depending on their input in terms of sharing data, validation, and research. Patients are encouraged to submit anonymized healthcare data. Scholars use tokens to access data and make donations to research. Transaction validation and proof verification are rewarded to validators.[20]

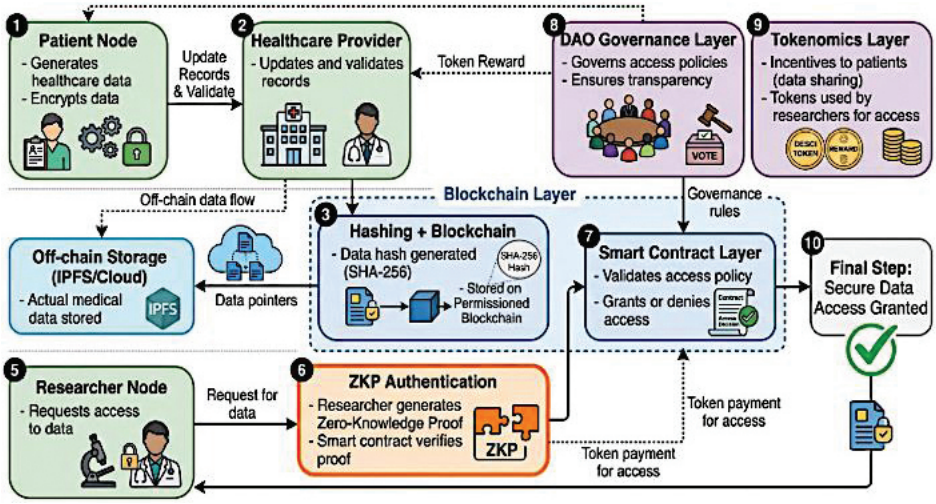

Fig. 2. DeSci-enabled healthcare data sharing workflow. DAO: decentralized autonomous organization; IPFS: interplanetary file system; PBFT: practical Byzantine fault tolerance; PoA: proof-of-authority; SHA-256: Secure Hash Algorithm 256-bit; ZKP: zero-knowledge proof.

Citation: Blockchain in Healthcare Today 2026, **9**: 507 - https://doi.org/10.30953/bhty.v9.507

This system of incentives fosters a decentralized research economy since it encourages participation and lessens dependence on centralized funding systems.[21] Moreover, provenance tracking through blockchains provides an immutable record of all data access and modification events, making it traceable, verifying data integrity, and providing audit trails that are compliant with regulatory requirements.

System Workflow

The proposed system works as follows:

a. Healthcare provider encrypts patient data D.
b. Calculates and stores H(D) on blockchain.
c. Off-chain storage stores actual data D.
d. A doctor or researcher requests access.
e. A cryptographic hash H(D) is recorded on the permissioned blockchain as a verifiable reference.
f. The user generates a ZKP π.
g. Verify (π, C): Smart contract verifies. C = the access control policy space, and again where Verify (π, C) is introduced.
h. Verification allows encrypted data entry.
i. Blockchain transactions are immutable.

The suggested DeSci-enabled healthcare data governance workflow is illustrated in Figure 2. To ensure data integrity, healthcare professionals encrypt data with the patient, compute a cryptographic hash, and store it in the authorized blockchain. Off-chain storage of the actual MedRec is carried out to enhance scalability and minimize overhead. A ZKP proves the request without disclosing important credentials when the researcher desires the data. Smart contracts establish proof and enforce access policy, making access only open when requirements are fulfilled. Data access transparency, policy resolutions, and incentives to engage patients and research are managed by a DAO governance layer and a tokenomics layer, respectively. This workflow demonstrates how the proposed architecture enables the sharing of privacy-sensitive, safe data in a decentralized way in accordance with DeSci. Formally, workflow access decisions are:

$A(U,D) = 1, if Verify\ (\pi,C) = 10$, otherwise U requests data D, $A(U,D)$ is the access decision. 1 means authorization and 0 denies.

This approach makes access control predictable, verifiable, and independent of centralized authority, following decentralized system trust minimization principles.

Security and Privacy Analysis

Adversary Model

A probabilistic adversarial model evaluates the proposed system's security. Let $\mathcal{A}$ represent an adversary aiming to breach data confidentiality, integrity, or access control.[22]

The enemy may try:

- Unauthorized data access
- Forgery of authentication proofs
- Tampering with data
- Impersonation or replay assaults

The goal of security is to minimize hostile success: $\Pr[\mathcal{A}\ \text{succeeds}] \leq \varepsilon$, where ε is insignificant. The suggested framework's assault resistance can be assessed using this model. This section formalizes the security and privacy of the lightweight hybrid blockchain system proposed for decentralized healthcare and DeSci. Testing is done in a semi-honest adversarial context where protocol executors can execute protocols but may want to guess sensitive info from the data they view.

Data Integrity and Immutability

The structure uses SHA-256 cryptography to secure data. The blockchain stores the hash H(D) of any patient data D.[23] Because SHA-256 is collision-resistant, every change in D affects H(D), allowing tampering to be detected quickly.

Security Guarantee: D is not D' if H(D) is not H(D'). Blockchain is unchangeable; therefore, no one can change a hash without consensus. The hash function's collision resistance ensures data integrity:

$$H(D) \neq H(D') \Rightarrow D \neq D'$$

Additionally, hash collision is unlikely:

$$Pr[collision] \approx 0.$$

This reliably detects illegal healthcare data changes.

Privacy and Confidentiality

The healthcare data are sensitive and stored off-chain.[24] Blockchain stores just hashed references and metadata. Specifically, patient data D is processed through SHA-256 cryptographic hashing, and only the resulting hash H(D) is stored on-chain, ensuring that raw medical data never resides on the blockchain. This architecture minimizes raw data exposure and leakage. Even if storage systems are attacked, encryption technologies can restrict data access to authorized users. The assumption is that encryption techniques are computationally secure, ensuring confidentiality.

To use the term "privacy-preserving" precisely, the proposed framework is designed to align with established healthcare data protection regulations. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates strict controls over PHI; the proposed off-chain storage and ZKP-based access control directly support HIPAA-compliant data minimization and access logging requirements. In the European Union, the General Data Protection Regulation (GDPR) requires data minimization and purpose limitation, which are addressed by the framework's on-chain hash-only storage model. In India, Digital Information Security in Healthcare Act (DISHA) similarly governs health data privacy. While full regulatory compliance requires institutional implementation, the architectural choices in this framework are deliberately aligned with these legal requirements.

Right to Rectification

Beyond erasure and objection, General Data Protection Regulation (GDPR) Article 16 grants data subjects a right to rectification, which, as with the rights above, must be satisfied by architectural design rather than by directly modifying a validated blockchain record, since altering a committed transaction would break the chain's consistency guarantees.[25] In

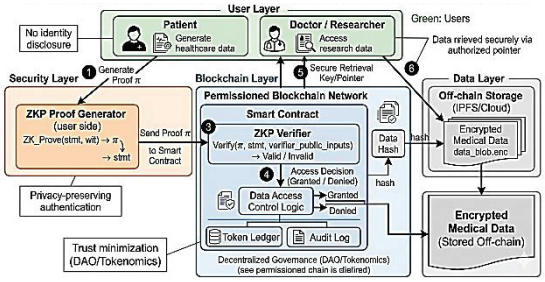

Fig. 3. ZKP-based privacy-preserving security architecture. DAO: decentralized autonomous organization; DeSci: decentralized science; HA-256: Secure Hash Algorithm 256-bit; IPFS: interplanetary file system; H(D'): cryptographic hash of the corrected patient data; ZKP: zero-knowledge proof.

the proposed framework, this is achieved through the same off-chain/on-chain separation described above. Because raw patient data D never resides on-chain and only its hash H(D) is committed to the ledger, a correction request is resolved by updating the record in off-chain storage and computing a new hash H(D') for the corrected data. A compensating transaction is then appended to the chain, referencing and superseding the earlier transaction; the original hash remains visible for audit purposes, but the smart-contract access-control layer always resolves ZKP-based verification (Verify(π,C) = 1) against the most recent, corrected hash for a given patient record. This design keeps rectification consistent with the framework's integrity guarantees while ensuring that authorized researchers and providers only ever act on up-to-date data.

Authentication via ZKP

The ZKP verification improves authentication in the proposed architecture. To establish compliance with an access policy C, a user can provide a proof π instead of providing credentials. The verification criterion is: $Verify(\pi, C) = 1$. Without revealing their sensitive identity or credential information.

Security Features:

a. Completeness: Authenticated valid users
b. Soundness: Invalid users cannot create valid proofs
c. Zero-knowledge: Only authorized information is disclosed

Identity leaks and insider threats will be considerably reduced by this strategy. Security of authentication relies on ZKP verification: $Verify(\pi, C) = 1$. Only authorized users that satisfy access policy can gain access. In addition, soundness guarantees: To prohibit unauthorized entities from forging valid proofs, Pr[$\mathcal{A}$ succeeds] <= ε. Users generate ZKPs that smart contracts on the permissioned blockchain verify, enabling trust-minimized and privacy-preserving access control while protecting sensitive healthcare data held off-chain.

The security diagram of the proposed structure shows how ZKP can enable privacy-sensitive authentication in Fig 3 This method enables the patients and researchers to generate cryptographic evidence of their authorization without revealing their sensitive identity or credential information.25 The evidence provided to the smart contract that is granted access is authenticated with predefined access policies. Healthcare data is off-chain encrypted and presented once authenticated. This method minimizes the data leakage, impersonation, and insider threats without revealing identities. The ZKP integration substitutes trust with cryptographic verification, which is decentralized-science-appropriate and safe data management.

The collision resistance of the hash function secures healthcare information: $H(D) \neq H(D') \Rightarrow D \neq D'$ This implies that when any data is updated, the hash value would change, and one would be able to detect tampering. Also, there is no likelihood of hash collision: $Pr[collision] \approx 0$. This enhances the reliability of a secure healthcare data management system. Safe and trust-minimized healthcare data ecosystem Cryptographic hashing, ZKP and decentralized consensus prevent trust.

Attack Resistance

The proposed architecture is designed to resist the following common attack classes:

a. 51% attack resistance: restricted validator participation in the permissioned blockchain substantially mitigates majority-control attacks.
b. Sybil attack mitigation: identity verification and controlled node admission limit the creation of malicious identities.
c. Replay attack prevention: identity binding and timestamps ensure that a given authentication proof cannot be reused.
d. Impersonation resistance: ZKP authentication prevents identity duplication in the absence of valid cryptographic evidence.
e. Collusion resistance: sensitive data cannot be recovered without the correct decryption keys and a valid proof.

Next are trust minimization and DeSci alignment: The framework being proposed builds trust through cryptographic verification, as opposed to the implicit trust that is used by typical systems. The ZKP integration removes identity disclosure, and blockchain allows auditable records. The design that reduces the trust value is optimal to DeSci principles, which are characterized by decentralized stakeholders (patients, researchers, institutions) that are not under centralized control or trusted middlemen.

Although extremely safe, a number of limitations exist: Resource-constrained environments: ZKP generation can add to computational load. To avoid unauthorized access, off-chain storage systems can require extra security.

Metadata exposure based on transaction patterns might be hazardously inferential. Such limitations hint at future optimizations such as lightweight proof systems and privacy-preserving algorithms such as differential privacy or safe multi-party computation. Cryptographic is incorporated in the proposed solution. Integrity, decentralized trust, and privacy-abiding authentication to provide security and privacy in next-generation DeSci and decentralized healthcare ecosystems.

Formal Security Model

To further substantiate these security guarantees, semi-formal, game-based adversarial models are defined for a permissioned network connecting patients, healthcare providers, and researchers. The adversary $\mathcal{A}$ is assumed capable of querying access requests and attempting to infer sensitive information from blockchain transactions and metadata. Three games assess the corresponding security properties.

Citation: Blockchain in Healthcare Today 2026, **9**: 507 - https://doi.org/10.30953/bhty.v9.507

The following game assesses system security:

Game 1: Authentication Sound
A valid proof is sought by the adversary $\mathcal{A}$.
Without valid credentials, $Verify(\pi, C) = 1$
Secure systems have a probability:
Pra[$\mathcal{A}$ succeeds] < ε, where ε is insignificant.

Game 2: Data integrity
The attacker changes patient data D to D' so:

$$H(D') = H(D)$$

Due to SHA-256 collision resistance:
Negligible collision probability

Game 3: Maintain Privacy
The attacker seeks sensitive data from proof π.
Due to zero-knowledge:
π *leakage* = 0.

These formal assurances prove the proposed system meets cryptographic assumptions for authentication soundness, data integrity, and privacy protection.

Results and Discussion

This section presents the performance evaluation of the proposed lightweight hybrid blockchain framework, designed to support DeSci, using simulation-based analysis. The system is tested under different network sizes to assess scalability and efficiency, with transaction latency, throughput, and computational cost as the key performance measures. A comparative evaluation against MedRec, FHIRChain, and HealthChain highlights the advantages of the proposed framework, and the impact of architectural choices, including hybrid consensus, off-chain storage, and ZKP-based authentication, is discussed. Given current infrastructure constraints, a prototype-level implementation is left as future work.[26,27]

Simulation Setup

The functionality of the proposed framework is tested with the help of an experimental setup based on a simulation, which provides the model of the distributed healthcare network setting. The system is composed of various interacting parties, such as patients, healthcare providers, researchers, and validator nodes that run within a permissioned blockchain network.

To study scalability and behavior of the system with a heavy workload, the simulation is performed on different network sizes, 10–50 nodes. Every node is involved in the generation of transactions, validation, and accessing data, which are real-life healthcare data exchange conditions.

The important system parameters are determined as follows:

1. Block size: 1 MB
b. Network latency: 50–150 ms
c. Consensus mechanism: Hybrid PBFT–PoA
d. Data storage: Off-chain storage with on-chain hash references
e. Security mechanism: ZKP-based authentication

Transactions are requests of accessing healthcare data, and in every request, proof should be generated, verified, and recorded in a blockchain. The simulation records the performance of the system operating under such functions to measure the latency, throughput, and computational overhead. Such an arrangement will allow evaluating the suggested framework in the context of decentralized healthcare and DeSci settings in a realistic manner.

Performance Metrics

Three major measures are used to assess the performance of the proposed framework: transaction latency, throughput, and computational cost. All of these measures are indicators of system efficiency, scalability, and processing overhead:

a. Transaction Latency (ms): This is the time taken to authorize and confirm a transaction in the blockchain network.
b. Throughput (TPS): This is the number of transactions per second that a system can handle, which shows that the system has the capacity to perform work.
c. Computational Cost: The overhead of the computation involved in executing the consensus, cryptographic hashing, and verification.

Computational Cost Implementation

In order to measure in a quantitative way the computational efficiency, the overall computational cost of the system is modeled as: *C total = C consensus + C hash + C zkp*. *C* concurrence is the cost of consensus functions, C hash is the cost of hashing, and C zkp is the cost of ZKP creation and validation. The individual components can be defined as: $C_{consensus} = O(n^2)$ $C_{hash} = O(n)$ $C_{zkp} \approx O(1)$ where n is the number of nodes that take part in the network.

Overall Complexity

The overall computational cost is given by: $C_{total} \approx O(n^2) + O(n) + O(1)$ Because consensus prevails in the computation, the complexity of the system is mainly controlled by: $C_{total} \approx O(n^2)$ Nevertheless, the computational overhead of running it is decreased significantly by the permissioned blockchain, hybrid consensus mechanism, and off-chain storage of data, which mitigates unnecessary operations on-chain.

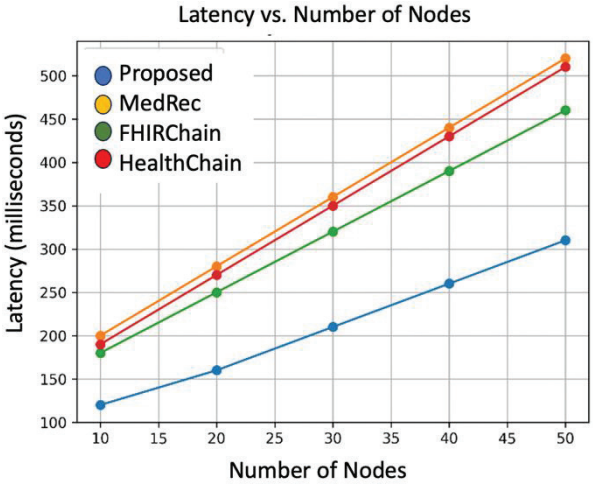

Fig. 4. Latency comparison across different network sizes. FHIRChain: fast healthcare interoperability resources; HealthChain; MedRec: medical records.

Interpretation

The suggested framework is more computationally efficient than the conventional blockchain-based healthcare systems. The hybrid PBFT-PoA consensus minimizes the communication overhead, and the off-chain storage minimizes the load on the blockchain network. Moreover, ZKPs provide secure authentication at a low cost of verification, which means that the privacy preservation will not cause any serious performance loss.

Latency and Throughput Analysis

The throughput and latency performance of the proposed framework is tested with different network sizes between 10 and 50 nodes. Figures 4 and 5 represent the results. Latency analysis indicates that the proposed framework has less transaction latency than the current systems. The communication overhead increases with the number of nodes, but the increase in latency is kept under control. The reason behind this behavior is the hybrid PBFT-PoA consensus mechanism, which minimizes the communication rounds that the transaction validation can take place in. Conversely, conventional blockchain-based healthcare systems have a steadier rise in latency with network size, mostly because of greater consensus overhead and lengthy processing on-chain.

Latency grows with the size of the network because of communication overhead, but the proposed framework exhibits a controlled growth because of optimized consensus execution.

The throughput is amplified with the expansion of the network, and this implies that the system capacity is enhanced. This is done by effective transaction validation and minimized on-chain processing. The throughput analysis shows that the proposed framework has a greater transaction processing capacity with all sizes of networks. With the number of nodes increasing, throughput also increases gradually, and this is a sign that there is an efficient way of handling concurrent transactions. This is enabled by the lower consensus overhead and the utilization of off-chain storage, which reduces the amount of computation required in the blockchain network.

In sum, the findings suggest that the suggested framework offers a reasonable trade-off between latency and throughput to ensure scalability and efficiency of decentralized healthcare and DeSci settings.

Comparative Analysis

In order to assess the efficiency of the offered framework, a comparative analysis is performed with the already existing blockchain-based healthcare frameworks, such as MedRec, FHIRChain, and HealthChain. The latency, throughput, and computational cost of the network with different network sizes are compared. The proposed framework has lower latency and greater throughput than the existing systems as seen in Figures 4 and 5. This is majorly because the hybrid PBFT-PoA consensus mechanism, which minimizes communication overhead, and off-chain storage, which minimizes on-chain data processing, are used to enhance performance. In order to further examine system efficiency, the comparison of computational costs is provided in Figure 6. The framework proposed has been shown to have reduced computation overheads with every size of network.

Figure 6 shows that the lower computational cost is a direct consequence of a streamlined consensus execution and validation participation of the limited number of validators in the permissioned blockchain setup. Conversely, current systems have a larger computational load in terms of intensive consensus algorithms and greater dependence on off-chain data processing. Besides performance gains, the proposed framework ensures better privacy due to the ZKP-based authentication and decentralized participation and through the governance and tokenomics mechanisms. These characteristics make the system DeSci compliant, with features that allow scalable, collaborative, and safe healthcare research. It is worth mentioning that the comparative analysis is made on normalized values, which are obtained based on reported characteristics of the existing systems. Although this offers valuable information on comparative performance, an entirely experimental study that involves all systems is a future research direction.

Limitations

Although the proposed framework has shown promising performance and security benefits, it is important to note that there are some limitations. Firstly, the existing assessment is

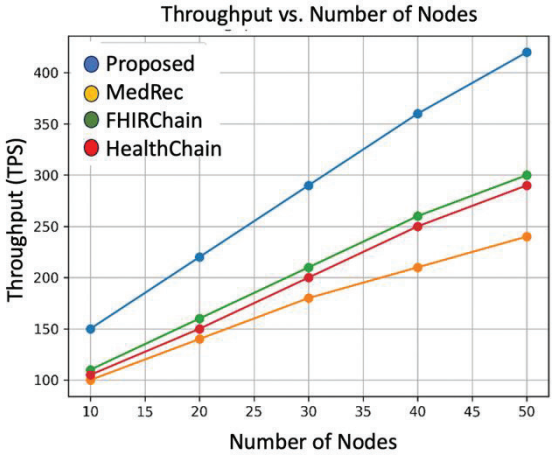

Fig. 5. Throughput comparison of proposed and existing systems. FHIRChain: fast healthcare interoperability resources; HealthChain; MedRec: medical records.

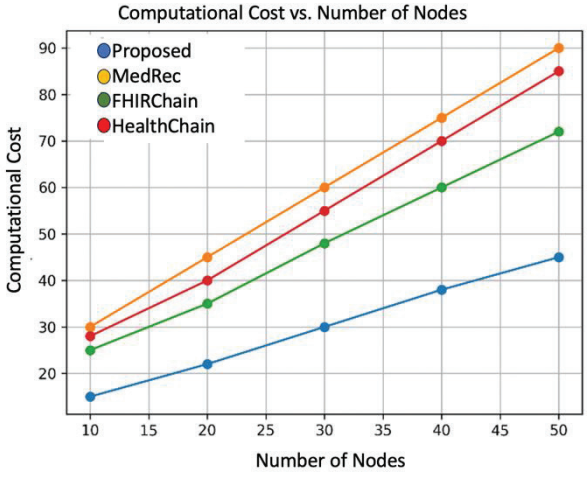

Fig. 6. Computational cost comparison across varying network sizes.

Citation: Blockchain in Healthcare Today 2026, **9**: 507 - https://doi.org/10.30953/bhty.v9.507

on the basis of simulation and analytical modeling as opposed to real implementation. Consequently, real-life considerations such as network heterogeneity, node failures, and changing workload fluctuations can affect system performance in actual healthcare scenarios. Secondly, even though ZKPs are very privacy-guaranteeing, the computational workload of proof generation can be an issue with resource-constrained devices. Verification is efficient, but when it comes to large-scale deployment scenarios, additional optimization might be needed. Thirdly, the comparative analysis is done based on normalized values of reported characteristics of existing systems. It does not involve a fully controlled experimental implementation of all of the compared frameworks, and this can influence a direct performance equivalence. Lastly, the combination of the mechanisms of tokenomics and DAO-based governance is theorized but not applied to a real-life scenario. The real-life implementation of such mechanisms needs additional testing, especially regarding the regulations and acceptance of the mechanism among users in healthcare systems. The next step in work will be the practical implementation based on the Hyperledger Fabric or Ethereum platforms and empirical optimization and benchmarking of cryptographic operations.

A further limitation concerns scalability in large-scale, heterogeneous healthcare networks. The hybrid PBFT–PoA consensus mechanism operates with a communication complexity of $O(n^2)$, which, while manageable within the simulated 10–50 node range, may introduce significant overhead as the network scales to hundreds of nodes across diverse healthcare institutions. Real-world deployments would involve heterogeneous node capabilities, including resource-constrained devices in rural or low-bandwidth environments, which could further degrade consensus performance. In addition, node failure and network partition scenarios were not modeled in the current simulation, and their impact on system availability and consistency remains an area for future investigation. Lightweight proof systems and sharding-based consensus optimizations are identified as potential solutions for large-scale deployment.

Conclusion

In this article the authors introduced a DeSci-based lightweight hybrid blockchain solution to healthcare data governance that is both secure and scalable. The system proposed combines hybrid consensus, off-chain storage, ZKP-based authentication, and decentralized governance to allow data access without privacy disclosure and minimal trust. The framework is shown to have better latency, throughput, and computational efficiency than current systems. It further allows decentralized research processes in line with the concepts of DeSci, which allows patient-centric ownership of their data and incentivized participation. Future directions will include practical deployment, combination with federated learning, and further cryptographic optimizations.

Funding

This research received no specific grant or financial support from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declare no conflicts of interest related to this study. All work was conducted independently, with no external influence on the results, interpretation, or reporting of this research.

Financial and Non-Financial Relationships and Activities

The authors declare that they have no financial or non-financial relationships or activities that could be perceived as having influenced, or that could appear to influence, the submitted work.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Application of AI-Generated Text or Related Technology

No AI-generated text or related technology was used in the writing of this manuscript.

Contributions

Garima Singh contributed to conceptualization and methodology and drafted the original manuscript. Nudrat Fatima carried out the formal analysis and investigation. Tameem Ahmad was responsible for data curation and software. Mohammad Husain performed validation and visualization. Mahfuzul Huda contributed to writing, review, and editing of the manuscript. Mohd. Haroon provided overall supervision of the study. Afsaruddin also contributed to writing, review, and editing.

References

1. Ranjan NM, Bembde MP, Mate GS, Kumar A. Electronic health records. Chapman Hall CRC; 2025. p. 240–67.
2. Pandit AP, Murugesan RK. The interoperability challenge in healthcare. In: Healthcare informatics. CRC; 2025. p. 393–402.
3. Shilina S. DeSci and tokenized science economies. In: Blockchain in science. IGI Global Scientific; 2026. p. 215–54.
4. Md Shafin K, Reno S. Breaking the blockchain trilemma: a comprehensive consensus mechanism for ensuring security, scalability, and decentralization. IET Softw. 2024;2024(1):6874055. https://doi.org/10.1049/2024/6874055
5. Sowmya G, Sridevi R, Rao KSS. Securing patient data with blockchain. In: Blockchain applications in healthcare. IGI Global; 2025. p. 519–36.
6. Khan RA, Sharma B, Thakare NM. BHPEC: design of an efficient model for blockchain-based healthcare privacy enhancement in clinical settings. J Inf Organ Sci. 2025;46(4-B):1323–33. https://doi.org/10.47974/JIOS-1993
7. Wang K, Lu P, Xin Z. Research on blockchain privacy preservation in healthcare systems. In: Proceedings of the IEEE Conference. IEEE; 2025. p. 286–90.
8. Nucciarelli L, Gottardelli B, Gatta R, Damiani A. Securing reproducibility and accountability in distributed healthcare analytics: a framework based on blockchain and cryptography. Stud Health Technol Inform. 2024;316:1269–73. https://doi.org/10.3233/SHTI240643
9. Sharma DK, Kumar A. A blockchain based solution for efficient and secure healthcare management. Int J Comput Inf Syst. 2025;21(2):168–86. https://doi.org/10.1504/IJCIS.2025.145191
10. Pise N, Kulkarni S. Enhancing security and efficiency in healthcare through decentralized and blockchain-based solutions. In: Decentralized healthcare systems. CRC; 2025. p. 276–91.
11. Wang Y, Farshidi S, Tripathi S, Zhao Z. Decentralized virtual research environment: empowering peer-to-peer trustworthy data sharing and collaboration. Authorea. 2024. https://doi.org/10.22541/au.171805667.77816225/v1

12. Raja SE, Kumar KD, Manikandan K, Senthil P, Shankar BP, Govindharaj I. MediCon: a lightweight, reputation-based consensus protocol to allow scalable and secure data sharing in healthcare. In: Proceedings of the IEEE Conference. IEEE; 2025. p. 793–7.
13. Myeong GE, Ram KS. Blockchain based zero knowledge proof protocol for privacy preserving healthcare data sharing. J Technol Innov Eng. 2025;4(1):171–89. https://doi.org/10.51903/jtie.v4i1.296
14. Verma A, Sharma A, Sharma S, Sharma A, Sunita S, Fuloria S. Tokenomics. In: Blockchain economics. Routledge; 2025. p. 117–34.
15. Hasan MM, Gopinath M, Ganesan A, Khamitdkhanovich NA, Harita U, Sehgal DR. Blockchain for audit trails in research information management systems. Int J Inf Syst Sci. 2025;15(2):218–23. https://doi.org/10.51983/ijiss-2025.IJISS.15.2.29
16. Upadhyay D, Upadhyay A, Sharma KB, Rawat A. Blockchain technology for secure health data management. In: Health data security. Bentham Science; 2026. p. 33–46.
17. Segal G, Martsiano Y, Markinzon A, Mayer A, Halperin A, Zimlichman E. A blockchain-based computerized network infrastructure for the transparent, immutable calculation and dissemination of quantitative, measurable parameters of academic and medical research publications. Digit Health. 2023;9:20552076231142398. https://doi.org/10.1177/20552076231142398
18. Shah P, Patel C, Patel J, Shah A, Pandya S, Sojitra B. Utilizing blockchain technology for healthcare and biomedical research: a review. Cureus. 2024;16(10):e72040. https://doi.org/10.7759/cureus.72040
19. Nortey RN, Yue L, Agdedanu PR, Adjeisah M. Privacy module for distributed electronic health records (EHRs) using the blockchain. In: Proceedings of the IEEE International Conference on Big Data Analysis (ICBDA). Vol 39. IEEE; 2019. p. 369–74. https://doi.org/10.1109/icbda.2019.8713188
20. Khan S, Khan M, Khan MA, Khan MA, Wang L, Wu K. A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. IEEE J Biomed Health Inform. 2025;PP:1–14. https://doi.org/10.1109/jbhi.2025.3538623
21. Richard T. Blockchain in healthcare: ensuring data security and integrity. Res Opin J Public Health Med. 2024;4(2):12–17. https://doi.org/10.59298/rojphm/2024/421217
22. Husnain G, Ullah Z, Mohmand MI, Qadir M, Alzahrani KJ, Ghadi YY, et al. HealthChain: a blockchain-based framework for secure and interoperable electronic health records (EHRs). IET Commun. 2024;18(19):1451–73. https://doi.org/10.1049/cmu2.12839
23. Ahn J, Yi E, Kim M. Blockchain consensus mechanisms: a bibliometric analysis (2014–2024) using VOSviewer and R Bibliometrix. Information. 2024;15(10):644. https://doi.org/10.3390/info15100644
24. Kaur N, Mittal A, Lilhore UK, Simaiya S, Dalal S, Saleem K, et al. Securing fog computing in healthcare with a zero-trust approach and blockchain. J Wireless Commun Netw. 2025;2025(1):5. https://doi.org/10.1186/s13638-025-02431-6
25. European Data Protection Board. Guidelines 02/2025 on processing of personal data through blockchain technologies, Version 2.0 [Internet]. [cited 2026 Jul 7]. Available from: https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202502_blockchain_v2_en.pdf
26. Zhou E. A privacy preserving and auditable blockchain framework for secure securities trading. Sci Rep. 2025;15(2):33116. https://doi.org/10.1038/s41598-025-17958-3
27. Zhang J, Yang Y, Zhao D, Wang Y. A node selection algorithm with a genetic method based on PBFT in consortium blockchains. Complex Intell Syst. 2022;9(3):3085–105. https://doi.org/10.1007/s40747-022-00907-2
28. Di Palma G, Scendoni R, Ferorelli D, De Benedictis A, Tambone V, De Micco F. AI-induced cybersecurity risks in healthcare: a narrative review of blockchain-based solutions within a clinical risk management framework. Risk Manag Healthc Policy. 2025;18:3479–97. https://doi.org/10.2147/rmhp.s544523