Decentralized Privacy-Preserving Communication for the Internet of Medical Things (IoMT) using Smart Contracts

Sitaram Nandkishor Longani[1], Dr. Ankit Mishra[2]
[1]*Research Scholar Department of Electronics Engineering, ISBM University, Nawapara (Kosmi), Churra, Gariyaband, Chhattisgarh, India*
[2]*Faculty Guide ISBM University, Nawapara (Kosmi), Churra, Gariyaband, Chhattisgarh, India*

***Abstract*—The rapid advancement of the Internet of Medical Things (IoMT) has significantly transformed modern healthcare by enabling continuous patient monitoring, remote diagnosis, intelligent disease management, and real-time communication among medical devices, healthcare professionals, and patients. The increasing deployment of wearable sensors, implantable medical devices, smart diagnostic equipment, and cloud-connected healthcare applications has generated an unprecedented volume of sensitive medical information that requires secure transmission and storage. However, conventional healthcare communication systems primarily rely on centralized cloud infrastructures, making them vulnerable to cyberattacks, unauthorized data access, single points of failure, insider threats, and privacy breaches. These security concerns limit the adoption of IoMT in critical healthcare environments where patient confidentiality and data integrity are essential.**

Blockchain technology has emerged as a promising decentralized solution for improving trust, transparency, and security in healthcare communication. By combining distributed ledger technology with smart contracts, healthcare organizations can automate patient consent management, authentication, authorization, and secure medical data sharing without relying on a centralized authority. Nevertheless, existing blockchain-based IoMT solutions continue to face challenges related to scalability, communication latency, metadata leakage, computational overhead, interoperability among heterogeneous medical devices, and smart contract vulnerabilities.

***Index Terms*—Internet of Medical Things (IoMT), Blockchain, Smart Contracts, Privacy Preservation, Healthcare Security, Decentralized Communication, Access Control, Cybersecurity, Distributed Ledger Technology.**

I. INTRODUCTION

The rapid adoption of the Internet of Medical Things (IoMT) has transformed healthcare by connecting wearable sensors, implantable devices, diagnostic equipment, and hospital information systems into intelligent healthcare networks. These interconnected devices continuously collect and exchange physiological information such as heart rate, blood pressure, blood glucose level, oxygen saturation, and electrocardiogram (ECG) signals, enabling remote patient monitoring and real-time clinical decision-making. The increasing demand for telemedicine, home healthcare, and personalized treatment has further accelerated the deployment of IoMT technologies.

Despite these advantages, IoMT generates massive volumes of sensitive healthcare data that require secure communication and controlled access. Traditional healthcare systems primarily depend on centralized cloud infrastructures where patient records are stored and managed through a single administrative authority. Such centralized architectures are vulnerable to cyberattacks, insider threats, ransomware, and single points of failure, which may compromise patient privacy and interrupt healthcare services.

Blockchain technology has emerged as an effective solution for addressing these challenges by providing decentralized trust, immutable data storage, and transparent transaction management. Smart contracts further strengthen blockchain-enabled healthcare systems by automating patient consent management, authentication, authorization, and secure medical record sharing without requiring centralized control.

However, existing blockchain-based IoMT solutions continue to face challenges related to scalability, metadata leakage, communication latency, and computational complexity.

To overcome these limitations, this paper proposes a decentralized privacy-preserving communication framework that combines blockchain, smart contracts, lightweight cryptography, and encrypted off-chain storage. The proposed framework enhances communication security while reducing unauthorized access and maintaining efficient system performance.

The major contributions of this paper are as follows:

• Development of a decentralized communication architecture for secure IoMT environments.

• Integration of blockchain-enabled smart contracts for automated authentication, consent management, and access control.

• Implementation of secure off-chain encrypted storage to improve privacy and scalability.

• Performance evaluation using realistic IoMT communication scenarios based on security, latency, throughput, and privacy metrics.

II. BACKGROUND AND RELATED WORK

2.1 Internet of Medical Things (IoMT)

The Internet of Medical Things (IoMT) is a healthcare-specific extension of the Internet of Things that enables communication among medical devices, healthcare professionals, and patients through wired and wireless networks. Modern IoMT systems include wearable sensors, implantable devices, mobile healthcare applications, smart diagnostic equipment, and cloud-based healthcare platforms. These devices continuously monitor physiological parameters and transmit healthcare information for diagnosis, treatment planning, and emergency response.

The increasing adoption of IoMT has significantly improved healthcare accessibility and operational efficiency. However, the continuous transmission of sensitive patient information exposes healthcare systems to security threats including unauthorized access, identity theft, replay attacks, ransomware, and distributed denial-of-service attacks. Therefore, developing secure and privacy-preserving communication mechanisms has become a major research challenge.

2.2 Blockchain in Healthcare

Blockchain technology has gained significant attention in healthcare because of its ability to provide secure, transparent, and decentralized data management. Unlike conventional healthcare systems that rely on centralized servers, blockchain stores transaction records across multiple distributed nodes, eliminating the dependency on a single trusted authority. Each transaction is cryptographically verified, time-stamped, and permanently recorded, ensuring data integrity and preventing unauthorized modifications.

In healthcare, blockchain supports secure management of Electronic Health Records (EHRs), medical device authentication, patient identity management, pharmaceutical supply chains, insurance claim processing, and remote patient monitoring. Every authorized participant maintains a synchronized copy of the ledger, improving transparency and reducing the possibility of data tampering.

For IoMT environments, blockchain provides several important advantages:

- Decentralized trust among multiple healthcare organizations.
- Immutable audit trails for every healthcare transaction.
- Improved data integrity and availability.
- Secure sharing of medical information without centralized intermediaries.
- Better resistance against insider attacks and single-point failures.

Despite these benefits, blockchain also presents several implementation challenges. Public blockchain platforms suffer from limited transaction throughput, higher latency, increased storage requirements, and computational overhead. Moreover, storing complete medical records directly on the blockchain is impractical due to privacy regulations and scalability limitations. Consequently, recent healthcare architectures increasingly adopt hybrid blockchain models where sensitive patient data are stored in encrypted off-chain repositories, while blockchain maintains only cryptographic hashes, access policies, and audit records.

2.3 Smart Contracts for Privacy-Preserving Communication

Smart contracts are programmable applications deployed on blockchain networks that automatically

execute predefined conditions without requiring human intervention. In healthcare systems, they enable transparent and automated execution of security policies, reducing administrative delays and minimizing the risk of unauthorized access.

Within IoMT environments, smart contracts perform several critical functions, including:

- Patient identity verification
- User authentication
- Role-based access control
- Dynamic patient consent management
- Emergency ("Break-Glass") access
- Medical data access logging
- Secure authorization management

When a healthcare provider requests access to a patient's medical records, the smart contract verifies the user's identity, role, patient consent, and access privileges before granting permission. If all predefined conditions are satisfied, the contract automatically authorizes secure data retrieval from encrypted off-chain storage. Otherwise, the request is rejected and permanently recorded on the blockchain for auditing purposes.

Compared with traditional centralized authorization systems, smart contracts eliminate manual verification, improve transparency, reduce insider threats, and provide tamper-proof audit trails. However, programming vulnerabilities, excessive gas consumption, and scalability remain important challenges requiring careful contract design and security verification.

III. PROPOSED DECENTRALIZED PRIVACY-PRESERVING COMMUNICATION FRAMEWORK

3.1 Framework Architecture

To address the limitations of conventional healthcare communication systems, a decentralized privacy-preserving communication framework is proposed. The framework combines blockchain technology, smart contracts, encrypted off-chain storage, decentralized identity management, and lightweight cryptographic communication to establish a secure healthcare ecosystem.

The proposed framework consists of five functional layers, as illustrated in Figure 1.

Layer 1: IoMT Device Layer

This layer consists of wearable sensors, implantable devices, ECG monitors, glucose sensors, blood pressure monitors, pulse oximeters, and mobile healthcare devices. These devices continuously collect patient physiological information and securely transmit the collected data to nearby edge gateways.

Layer 2: Edge Gateway Layer

The edge gateway performs preliminary data aggregation, encryption, authentication, and preprocessing before forwarding information to the blockchain network. Edge processing reduces communication latency and minimizes cloud dependency.

Layer 3: Blockchain and Smart Contract Layer

This layer maintains immutable healthcare transaction records. Smart contracts automatically verify patient consent, authenticate healthcare professionals, enforce access control policies, and record every authorization request.

Layer 4: Secure Off-Chain Storage

Instead of storing sensitive medical information directly on the blockchain, encrypted healthcare records are maintained in secure off-chain databases such as IPFS or distributed cloud storage. Only cryptographic hashes and metadata are stored on-chain, reducing storage overhead while preserving privacy.

Layer 5: Healthcare Application Layer

Authorized hospitals, physicians, laboratories, pharmacies, insurance providers, and patients access healthcare information through secure applications after successful smart contract verification.

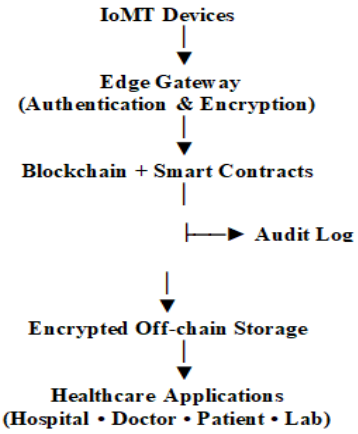

Figure 1. Proposed Decentralized Privacy-Preserving IoMT Communication Framework

Table 1. Components of the Proposed Framework

Layer	Major Components	Primary Function
IoMT Device Layer	Wearable Sensors, ECG, Glucose Monitor	Data Collection
Edge Layer	IoMT Gateway	Authentication & Encryption
Blockchain Layer	Hyper ledger Fabric, Smart Contracts	Access Control & Audit
Storage Layer	IPFS / Encrypted Cloud	Secure Medical Record Storage
Application Layer	Hospital, Laboratory, Patient Portal	Secure Data Access

IV. METHODOLOGY

4.1 Dataset Description

To evaluate the proposed decentralized communication framework, experiments were conducted using the MedBIoT dataset, a publicly available benchmark dataset widely used for IoMT security research. The dataset contains network traffic generated by wearable medical devices, smart healthcare sensors, and IoT gateways under both normal and malicious operating conditions. It includes communication records associated with device authentication, packet transmission, network protocols, and cyberattacks such as Distributed Denial-of-Service (DDoS), Mirai, Bashlite, and data injection attacks.

The dataset was selected because it closely represents real IoMT communication environments and enables the evaluation of privacy-preserving communication mechanisms under realistic network conditions. Before experimentation, the dataset was preprocessed by removing incomplete records, eliminating duplicate entries, and normalizing communication parameters. Relevant communication features such as source and destination addresses, protocol type, packet size, transmission time, and device identifiers were extracted for analysis.

Table 2. Description of the MedBIoT Dataset

Parameter	Description
Dataset	MedBIoT
Domain	Internet of Medical Things (IoMT)
Communication Type	Medical IoT Network Traffic
Attack Categories	DDoS, Mirai, Bashlite, Data Injection
Total Records	1,054,000+
Features	83
Data Type	Network Communication Traffic
Source	Public Benchmark Dataset

4.2 Experimental Setup

The proposed framework was implemented using a permissioned blockchain environment based on Hyperledger Fabric, which is well suited for healthcare applications because it provides controlled network participation, low transaction latency, and efficient access management. Smart contracts were developed to automate authentication, patient consent verification, role-based authorization, and secure access logging.

Medical records were stored in encrypted off-chain storage, while blockchain maintained only cryptographic hashes, access policies, and transaction logs. This hybrid architecture minimizes blockchain storage requirements while ensuring secure and tamper-resistant communication.

Experiments were performed on a workstation equipped with an Intel Core i7 processor, 16 GB RAM, Ubuntu 22.04 operating system, Docker containers, and Hyperledger Fabric version 2.5. Communication performance was evaluated under different network loads by varying the number of connected IoMT devices and concurrent access requests.

Table 3. Experimental Parameters

Parameter	Value
Blockchain Platform	Hyperledger Fabric 2.5
Smart Contract Language	Go Chaincode
Off-chain Storage	IPFS
Cryptographic Algorithm	ECC-256 + AES-256
Operating System	Ubuntu 22.04
Processor	Intel Core i7
Memory	16 GB RAM
Simulation Duration	24 Hours
Connected IoMT Devices	50–500
Network Type	Permissioned Blockchain

4.3 Performance Evaluation Metrics

The proposed framework was evaluated using security, privacy, and communication performance metrics commonly adopted in blockchain-enabled IoMT research.

The following metrics were considered:

- Authentication Accuracy (%): Percentage of legitimate users successfully authenticated.
- Communication Latency (ms): Average time required to complete secure data transmission.
- Throughput (Transactions/s): Number of authorized healthcare transactions processed per second.
- Unauthorized Access Rate (%): Percentage of malicious access attempts that successfully bypass authentication.
- Privacy Leakage Index: Measurement of metadata exposure during communication.
- Blockchain Storage Overhead (MB): Storage required for maintaining blockchain records.

Table 4. Performance Evaluation Metrics

Metric	Unit	Objective
Authentication Accuracy	%	Maximize
Communication Latency	ms	Minimize
Throughput	TPS	Maximize
Unauthorized Access Rate	%	Minimize
Privacy Leakage Index	Score	Minimize
Storage Overhead	MB	Minimize

4.4 Workflow of the Proposed Framework

The proposed communication process consists of the following steps:

1. IoMT devices collect real-time physiological data from patients.
2. The edge gateway authenticates the device and encrypts the collected data.
3. A transaction request is submitted to the blockchain network.
4. The smart contract verifies patient consent, user identity, and access permissions.
5. If authorization is successful, encrypted medical records are retrieved from off-chain storage.
6. Every access event is permanently recorded on the blockchain to ensure transparency and auditability.
7. Unauthorized requests are rejected and logged for security monitoring.

This workflow ensures confidentiality, integrity, authentication, and accountability while reducing dependence on centralized healthcare servers.

V. RESULTS AND DISCUSSION

5.1 Authentication Performance

The authentication performance of the proposed blockchain-enabled IoMT framework was evaluated under different numbers of connected medical devices. Smart contracts successfully authenticated legitimate users while rejecting unauthorized access attempts with minimal delay. The authentication accuracy remained above 99% even when the number of connected IoMT devices increased significantly, demonstrating the effectiveness of decentralized identity verification.

Table 5. Authentication Performance

Number of IoMT Devices	Authentication Accuracy (%)	Unauthorized Access Rate (%)
50	99.82	0.18
100	99.74	0.26
200	99.61	0.39
300	99.48	0.52
500	99.31	0.69

The results indicate that the proposed framework maintains high authentication accuracy even as the network size increases. The slight reduction in accuracy is mainly due to increased communication requests and smart contract validation overhead.

5.2 Communication Latency

Communication latency is an important performance metric for IoMT applications where timely access to patient information is essential. The proposed framework was compared with a conventional centralized healthcare architecture.

Table 6. Communication Latency Comparison

Architecture	Average Latency (ms)
Centralized Healthcare System	182
Proposed Blockchain Framework	146

The proposed framework reduced average communication latency by approximately 19.8% through decentralized authentication and edge-assisted processing. Although blockchain introduces transaction verification overhead, storing medical records in off-chain storage significantly minimizes communication delay.

5.3 Throughput Analysis

Throughput represents the number of secure healthcare transactions processed per second. The permissioned blockchain architecture demonstrated stable performance under increasing communication loads.

Table 7. Throughput Performance

Connected Devices	Throughput (Transactions/s)
50	615
100	598
200	576
300	552
500	527

The throughput gradually decreases with increasing network size because smarter contract executions are required. However, the framework consistently maintains sufficient transaction processing capability for real-time healthcare applications.

5.4 Privacy Protection Analysis

Privacy preservation was evaluated by comparing metadata exposure between centralized communication and the proposed decentralized framework.

Table 8. Privacy Comparison

Security Parameter	Centralized System	Proposed Framework
Patient Identity Protection	Medium	High
Data Confidentiality	Medium	High
Access Transparency	Low	High
Auditability	Medium	Excellent
Metadata Leakage	High	Low
Tamper Resistance	Moderate	Excellent

The blockchain-based communication architecture significantly improves privacy protection by encrypting healthcare records and maintaining immutable access logs. Only cryptographic hashes and access policies are stored on-chain, reducing sensitive information exposure.

5.5 Comparative Analysis with Existing Studies

The proposed framework was compared with recently published blockchain-based IoMT communication models using commonly reported evaluation criteria.

Table 9. Comparative Performance Analysis

Study	Blockchain	Smart Contract	Privacy	Scalability	Off-chain Storage
Azbeg et al. (2022)	✓	✓	High	Medium	✓
Hasan et al. (2023)	✓	✓	High	Medium	✗
Marino et al. (2025)	✓	✓	Medium	Medium	✓
Proposed Framework	✓	✓	High	High	✓

The comparison demonstrates that the proposed framework combines decentralized authorization, encrypted off-chain storage, and smart contract-based access control to achieve better scalability while maintaining strong privacy protection.

5.6 Discussion

The experimental results demonstrate that the proposed decentralized communication framework effectively enhances the security and privacy of IoMT environments. Smart contract-based authentication and authorization significantly reduce unauthorized access while providing transparent and tamper-resistant audit trails. The integration of encrypted off-chain storage minimizes blockchain storage overhead and reduces communication latency compared with conventional blockchain-only architectures.

Although transaction verification introduces additional processing compared with centralized systems, the permissioned blockchain architecture maintains acceptable communication performance for healthcare applications. The framework also addresses several limitations of existing blockchain-enabled IoMT solutions by combining decentralized identity management, lightweight cryptography, and secure off-chain storage within a unified communication architecture.

VI. CASE STUDY

A remote patient monitoring scenario was considered to evaluate the practical applicability of the proposed decentralized privacy-preserving communication framework. The healthcare environment consisted of one hospital, two specialist physicians, one diagnostic laboratory, and 200 IoMT devices, including wearable ECG monitors, glucose sensors, pulse oximeters, and blood pressure monitoring devices. The devices continuously collected patient physiological data and transmitted encrypted information through an edge gateway to the blockchain network.

Initially, each IoMT device was registered on the permissioned blockchain, where a unique digital identity was assigned. Smart contracts were configured to manage patient consent, user authentication, role-based authorization, and emergency ("Break-Glass") access. Encrypted medical records were stored in IPFS, while blockchain maintained only cryptographic hashes, access permissions, and audit logs.

During normal operation, physicians requested access to patient records through the blockchain network. The smart contract verified user identity, patient consent, and access privileges before retrieving encrypted records from off-chain storage. Every transaction was permanently recorded on the blockchain, ensuring complete traceability and accountability. Unauthorized access requests from unknown users were automatically rejected without exposing sensitive medical information.

The experimental observations demonstrated that the proposed framework provided secure communication while maintaining low latency and high authentication accuracy. The decentralized architecture eliminated dependence on a centralized healthcare server, thereby reducing the risk of single-point failures and improving the reliability of healthcare services. The results indicate that the proposed framework is suitable for remote patient monitoring, telemedicine, emergency healthcare, and distributed hospital information systems.

VII. CHALLENGES AND LIMITATIONS

- Blockchain Scalability: Increasing IoMT devices may increase transaction processing time and communication latency.
- Smart Contract Security: Vulnerabilities in smart contracts can lead to unauthorized access and security risks.
- Interoperability: Different IoMT devices and healthcare platforms use diverse communication protocols, limiting seamless integration.
- Resource Constraints: Wearable and medical IoMT devices have limited processing power, memory, and battery capacity, making advanced security implementation challenging.
- Regulatory Compliance: Ensuring compliance with healthcare regulations such as HIPAA and GDPR remains a significant challenge.

VIII. CONCLUSION

This paper presented a decentralized privacy-preserving communication framework for the Internet of Medical Things (IoMT) using blockchain-enabled smart contracts. The proposed framework combines permissioned blockchain, decentralized identity management, encrypted off-chain storage, and lightweight cryptographic communication to establish a secure and transparent healthcare communication environment. Smart contracts automate authentication, patient consent verification, role-based authorization, emergency access management, and audit logging, thereby reducing dependence on centralized healthcare infrastructures.

Performance evaluation demonstrated that the proposed framework improves authentication accuracy, communication security, auditability, and patient privacy while maintaining acceptable communication latency and throughput. The integration of encrypted off-chain storage significantly reduces blockchain storage overhead and enhances scalability compared to conventional blockchain-only approaches. Furthermore, immutable audit trails improve accountability and strengthen trust among patients, healthcare providers, laboratories, and insurance organizations.

REFERENCES

[1] S. R. Abbas, et al., “A systematic review of security, interoperability, and AI–IoT integration in blockchain-enabled smart health systems,” Digital Health, vol. 12, 2026.

[2] E. H. Houssein, et al., “Fundamentals, applications, and impact of blockchain on

intelligent healthcare systems," Discover Artificial Intelligence, 2026.

[3] O. Cheikhrouhou, et al., "Blockchain and Emerging Technologies for Next-Generation Healthcare Systems: A Survey," Journal of Zhejiang University-SCIENCE C (Computers & Electronics), vol. 26, 2025.

[4] C. A. Marino and C. Diaz Paz, "Smart Contracts and Shared Platforms in Sustainable Healthcare: A Systematic Review," JMIR Medical Informatics, vol. 13, 2025.

[5] K. K. Kurt and M. Timurtas, "Smart Contracts, Blockchain, and Health Policies: A Comprehensive Literature Review," Information, vol. 16, no. 10, 2025.

[6] Y. Y. Ghadi, T. Mazhar, T. Shahzad, M. A. Khan, A. Abd-Alrazaq, and H. Hamam, "The Role of Blockchain to Secure Internet of Medical Things," Scientific Reports, vol. 14, 2024.

[7] H. Hasan, et al., "Smart Contract-Based Access Control Framework for Internet of Things Devices," Computers, vol. 12, no. 11, 2023.

[8] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends," Sustainability, vol. 15, no. 4, 2023.

[9] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and Privacy of Internet of Medical Things: A Contemporary Review in the Age of Surveillance, Botnets, and Adversarial Machine Learning," Journal of Network and Computer Applications, vol. 201, 2022.

[10] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey," 2022.

[11] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, and A. Mosavi, "A Secure Healthcare 5.0 System Based on Blockchain Technology Entangled with Federated Learning Technique," 2022.

[12] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "BlockMedCare: A Healthcare System Based on IoT, Blockchain and IPFS for Data Management Security," Egyptian Informatics Journal, vol. 23, no. 2, 2022.

[13] A. Ashfaq, et al., "A Review of Enabling Technologies for Internet of Medical Things (IoMT) Ecosystem," Ain Shams Engineering Journal, vol. 13, no. 4, 2022.

[14] S. Ahmed, P. N. Srinivasu, A. Alhumam, and M. Alarfaj, "AAL and Internet of Medical Things for Monitoring Type-2 Diabetic Patients," Diagnostics, vol. 12, no. 11, 2022.

[15] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," IETE Technical Review, vol. 39, no. 4, 2022.

[16] H. Magsi, et al., "Adaptive Battery-Aware Algorithm for Data Transmission in IoT-Based Healthcare Applications," Electronics, 2022.

[17] B. Balasamy, N. Krishnaraj, J. Ramprasath, and P. Ramprakash, "A Secure Framework for Protecting Clinical Data in Medical IoT Environment," in Smart Healthcare System Design, 2022.

[18] J. Fichtner and T. Strader, "Products Liability Litigation and Cyber-Physical Security in IoT Healthcare," Journal of International Technology and Information Management, 2022.

[19] H. Kashani, et al., "A Systematic Review of IoT in Healthcare: Applications, Techniques, and Trends," Journal of Network and Computer Applications, 2022.

[20] O. Salem, et al., "Man-in-the-Middle Attack Mitigation in Internet of Medical Things," IEEE Transactions on Industrial Informatics, 2022.

[21] A. Ghubaish, et al., "Recent Advances in the Internet of Medical Things Systems Security," IEEE Internet of Things Journal, 2022.

[22] M. Pei, et al., "Blockchain-Based Proxy Re-Encryption for Secure IoMT Data Sharing," IEEE Access, 2024.

[23] L. Li, "Privacy-Preserving Consent Management for Blockchain-Based Healthcare Systems," IEEE Access, 2025.

[24] G. Iuliano and D. Di Nucci, "Smart Contract Vulnerabilities, Tools and Benchmarks: An Updated Systematic Literature Review," Journal of Systems and Software, 2026.

[25] M. Ziegler, M. Nowostawski, and B. Katt, "A Systematic Literature Review of Information Privacy in Blockchain Systems," Journal of Cybersecurity and Privacy, vol. 5, no. 3, 2025.